ISBN 978-81-924867-3-4

Vol. 2

ICRIET 2014

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

19th - 20th December 2014

Organised by

Department of Electronics & Communication Engineering

Sponsored by

ISTE | PTU Jalandhar

AUTONOMOUS* UNDER UGC ACT 1956 [2(F AND 12 B)] NBA Accredited NAAC Accredited

AMRITSAR COLLEGE OF ENGINEERING & TECHNOLOGY

Approved by AICTE, New Delhi & Affiliated to PTU, Jalandhar

Editors

Dr. V.K. Banga

Dr. Tanu Preet Singh

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

19th - 20th December 2014

ICRIET 2014

Sponsored by

PTU | ISTE

EDITORS

Dr. V. K. Banga

Dr. Tanu Preet Singh

Organised by

Department of Electronics & Communication Engineering

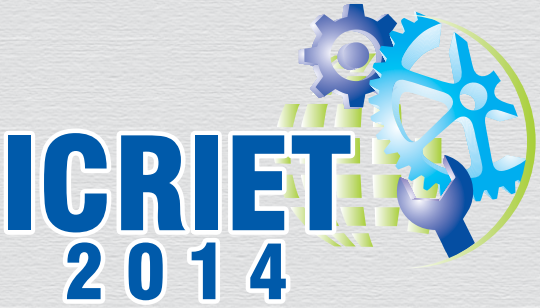
AUTONOMOUS* UNDER UGC ACT 1956 [2(F AND 12 B)] NBA Accredited NAAC Accredited

AMRITSAR COLLEGE OF ENGINEERING & TECHNOLOGY

Approved by AICTE, New Delhi & Affiliated to PTU, Jalandhar

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY



19th - 20th December 2014

CHIEF PATRON

Sh. Amit Sharma (Chairman & CEO, ACET Amritsar)

PATRONS

Ms. Ragini Sharma, Director (Finance)

Dr. O. K. Harsh, Group Director

CONFERENCE CHAIR

Dr. V. K. Banga, Principal

ORGANIZING SECRETARY

Dr. Tanu Preet Singh, Prof. & HOD ECE

CONVENOR

Mr. Sandeep Kaushal, Assoc. Prof. ECE

COORDINATOR

Mr. Narinder Sharma, HOD EE

CO-CONVENOR

Mr. Atul Mahajan, Assoc. Prof. ECE

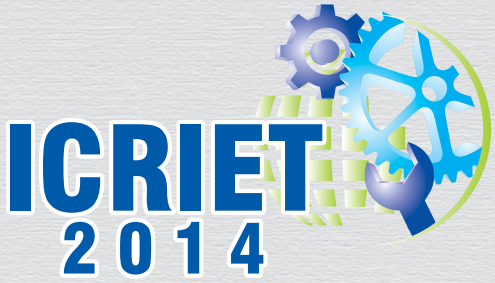
AUTONOMOUS* UNDER UGC ACT 1956 [2(F AND 12 B)] NBA Accredited NAAC Accredited

AMRITSAR COLLEGE OF ENGINEERING & TECHNOLOGY

Approved by AICTE, New Delhi & Affiliated to PTU, Jalandhar

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY



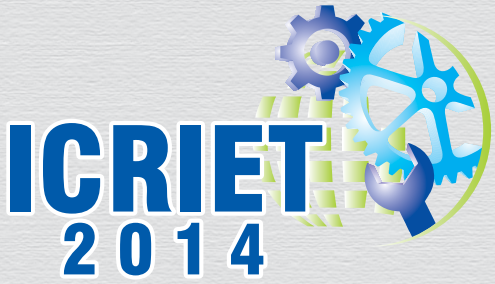
19th - 20th December 2014

INTERNATIONAL ADVISORY COMMITTEE

Dr. Sunil Kumar	Coating Mantra Science & Technology Consulting, Australia
Dr. D.P. Sharma	The University of West Indies, West Indies
Dr. Masashi Kotobuki	Hakodate National College of Technology, Hokkaido, Japan
Dr. Venkatachalam Ramaswamy	Princeton University (Forrestal Campus) New Jersey, USA
Dr. Thae Maung Maung	Aerospace Engineering University, Meikhtilar, Myanmar
Dr. Salam Amir Hoshang	Head of MIs department, Thailand
Dr. Narasimhaiah Gorla	American University of Sharjah, UAE
Dr. Mazdak Zamani	Advanced Informatics School, University Teknologi Malaysia, Malaysia
Dr. Michael Sega Gumelar	Universitas Multimedia Nusantara, Indonesia
Mr. Geetesh Madan	Q.A. Consultant with Tesco Bank, Newcastle, UK
Dr. Jack Ajowi	Jaramogi Oginga Odinga University of Sci. & Tech., Kenya
Dr. Srinivas Sampalli	Dalhousie University, Halifax, Canada
Dr. Hong Guo	3rd Research Institute of Ministry of Public Security, China
Mr. Aryya Bhattacharyya	Enterprise Domain Architect, Xerox Services, US
Dr. M.M. Schiraldi	Tor Vergata University of Rome, Italy
Dr. Md. Rizwan Alam	Amity University, Dubai
Dr. Naufal Bin Manso	School of Mechatronic, University Malaysia Perlis, Malaysia

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY



19th - 20th December 2014

NATIONAL ADVISORY COMMITTEE

Dr. Rajneesh Arora	VC PTU Jalandhar
Dr. R.S. Bawa	VC CU Punjab
Dr. G.K. Singh	IIT Roorkee
Dr. K.K. Pant	IIT Delhi
Dr. S.N. Singh	IIT Kanpur
Dr. S.S. Pattnaik	NITTTR Chandigarh
Dr. P.S. Bhimbhra	TU Patiala
Dr. Yaduvir Singh	ITBTI Kanpur
Dr. Rajesh Kumar	TU Patiala
Dr. Dilbag Singh	NIT Jalandhar
Dr. B.S. Saini	NIT Jalandhar
Dr. M.L. Singh	GNDU Amritsar
Dr. Sandeep Yadav	IIT Rajasthan
Dr. R.N. Yadav	MANIT Bhopal
Dr. Ajay K. Saxena	DEI Agra
Dr. Dharmendra Singh	IIT Roorkee
Dr. R.K. Singh	UTU Dehradun
Dr. H.S. Saini	MD GNI Hyderabad
Dr. S.K. Gupta	IIT Delhi
Dr. V. Sundarapandian	VTDRSRTU Chennai
Dr. Harish Kumar	ITS Ghaziabad
Dr. Kawaljit Singh	Punjabi University, Patiala
Dr. Deepak Garg	Thapar University, Patiala
Dr. Vishal Sharma	IIT Roorkee

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

ICRIET 2014

19th - 20th December 2014

EXECUTIVE COMMITTEE MEMBERS

Dr. V.K. Banga	Principal ACET Amritsar
Dr. Harinder Singh Gill	Principal (ACHMT)
Mr. Manoj Kumar	Registrar
Mr. Paramjit Singh Sidhu	Dean Academic Affairs & HOD (CE)
Col. (Retd.) Gurmukh Singh	Dean Student Affairs & HOD (CSE)
Mr. Gaurav Tejpal	Dean-Admission-Head ME
Mr. Rakesh Jaitly	Dean Placement
Dr. Amit Sareen	HOD (AS Group A)
Mr. Sandeep Kad	HOD (IT)
Mr. Ajay Sharma	HOD (AS Group B)
Dr. Maninder Singh Gill	HOD (MBA)
Ms. Deepti Malhotra	HOD (MCA)
Mr. Harinder Singh Sarkaria	HOD-Librarian
Mr. Jayant Vats	Incharge, Admission

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

AUTONOMOUS* UNDER UGC ACT 1956 [2(F AND 12 B)] NBA Accredited NAAC Accredited

AMRITSAR COLLEGE OF ENGINEERING & TECHNOLOGY

Approved by AICTE, New Delhi & Affiliated to PTU, Jalandhar

Department of Electronics & Communication Engineering Organizing Committee

Editorial Committee
1. Dr. V.K. Banga
2. Dr. Tanupreet Singh
3. Er. Sandeep Kaushal
4. Er. Narinder Sharma
5. Er. Atul Mahajan
6. Mr. Harminder Singh (Student)

Registration and Reception Committee
1. Er. Guneet Kaur
2. Er. Jagdeep Singh
3. Er. Reetu Pathania
4. Er. Vanita Kumari

Publication Committee
1. Er. Sandeep Kaushal
2. Er. Gaurav Soni
3. Er. Atul Mahajan
4. Er. Jayant Vats

Hospitality Committee
1. Er. Narinder Sharma
2. Er. Gurjeet Singh
3. Er. Kamaljit Kaur
4. Er. Bharti Sharma
5. Er. Madhvi
6. Er. Harsimran Kaur
7. Er. Gurpartap Singh

Media/Publicity Committee
1. Er. Narinder Sharma
2. Er. Jayant Vats
3. Er. Satish Pawar
4. Er. Bharti Sharma
5. Er. Chetan Verma

Prize Distribution Committee
1. Er. Neha Sharma
2. Er. Kamaldeep Kaur

Tour & Transportation Committee
1. Er. Gurjeet Singh
2. Er. Jagdeep Singh
3. Er. Chetan Verma
4. Er. Gurpartap Singh

Accommodation Committee
1. Er. Rakesh Jaitly
2. Er. Gurjeet Singh
3. Er. Chetan Verma

Financial/ Accounts Committee
1. Dr. Tanupreet Singh
2. Mr. Ashish Arora
3. Er. Atul Mahajan
4. Er. Jagdeep Singh

Arrangements/ Decoration Committee
1. Er. Satish Pawar
2. Er. Reetu Pathania
3. Er. Kamaljit Kaur
4. Er. Vanita Kumari
5. Er. Neha Sharma

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

ICRIET 2014

19th - 20th December 2014

OUR PUBLICATION PARTNERS

Cyber Times International Journal of Technology & Management	CTIJTM
International Journal of Computing Technologies	Journal of Computing Technologies
International Journal of research in Engineering & Technology	IJRET International Journal of Research in Engineering and Technology e-ISSN 2319 - 1163 p-ISSN 2321 - 7308 eSAT
ACET Journal of new horizon	NEW HORIZON

ISBN: 978-81-924867-3-4

INTERNATIONAL CONFERENCE ON RESEARCH AND INNOVATIONS IN ENGINEERING & TECHNOLOGY

ICRIET 2014

19th - 20th December 2014

KEYNOTE SPEAKERS

Professor Pang Leang Hiew
Educationist, Technologist and Experienced Leader
Selangor, Malaysia

Prof. Yaduvir Singh
Prof. & Head, Electrical & Engineering Dept.
HBTI Kanpur

Dr. Sunil Kumar
Adelaide, Australia

Dr. Anup Girdhar
CEO & Founder
Sedulity Solutions and Technologies

Communiqué

It is a matter of immense contentment to know that the "International Conference on Research and Innovations in Engineering and Technology" is being organized by Department of Electronics and Communication Engineering of Amritsar College of Engineering and Technology.

The conference is a timely step in sharing new innovations and transmitting the same to its consumers at a very fast pace. Research includes any gathering of data, information and facts for the advancement of knowledge and such conferences unveil the treasure of innovative ideas. It creates the talent, creativeness and professional skills of an individual.

Technology in the world is going through a tremendous flux. The Conference aims at bringing together Researchers, Scientists, Academicians and many others to interact and exchange their ideas & experiences, which in turn would help the students and faculty to gain immensely at the professional front. I believe that the conference will serve its objectives and will provide the necessary impetus in setting forth a dynamic process of continuous interaction among the researchers, teachers and professionals throughout the globe.

I also take the opportunity to thank the Electronics and Communication Engineering Department for organizing this event and convey my greetings to the organizers and wish grand success in the endeavor for the event.

Dr. Rajneesh Arora
Vice Chancellor
Punjab Technical University
Kapurthala

Communiqué

It fills my soul with immense pleasure to witness a major milestone for us all – the publication of the Proceedings of the "International Conference on Research and Innovations in Engineering and Technology" organized by the Department of Electronics and Communication Engineering at Amritsar College of Engineering and Technology, Amritsar.

Research is to see what everybody else has seen and to think what nobody else has thought and research in all the fields of Engineering and Technology has to be undertaken earnestly, with the objective of original findings in new realms. I am particularly happy to know that Department of Electronics and Communication Engineering of ACET, Amritsar is carrying forward the legacy of PTU by organizing such an event with a strong agenda for researches to provide solutions to the myriad problems in the field of Science, Engineering and Management that continue afflicting the Industries & Society.

I am sure that this conference will pave the way for providing a forum to the researchers, academicians and students to express their innovative and creative research skills. This event will spread the enormous light of awareness about the latest and upcoming fields and research areas in Engineering and Technology.

I compliment the organizer of ICRIET-2014 for holding this event and wish all success to the conference.

Advocate Amit Sharma
Chairman & CEO
ACET, Amritsar

Communiqué

It is a matter of great pleasure for me that Department of Electronics and Communication Engineering of our college is organizing an "International Conference on Research and Innovations in Engineering and Technology" on December 19-20, 2014.

It is an outcome of extraordinary endeavour put by the organizers in planned manner within a limited period of time. This conference is an attainment to meet the modern technological challenges in topical themes and areas of Science and Engineering, which is an essential need for current global development. The Conference will provide the ideal forum to stimulate ideas and establish collaborations and to initiate intense discussions about latest development in the area of technological research.

The Conference is being held in Amritsar, which is the palace of spiritual importance in Punjab and I hope the delegates will have a comfortable stay and they will enjoy the traditional hospitality offered by the Institution. It is not an easy job for the organizers of this international conference of such a magnitude, and I would like to thank all the members of the organizing committee for their hard work.

I wish the conference a substantial success.

Ragini Sharma
Director (Finance)
ACET, Amritsar

Communiqué

I am delighted to note that the "International Conference on Research and Innovations in Engineering and Technology" is being organized by Department of Electronics and Communication Engineering, Amritsar College of Engineering and Technology during December 19-20, 2014.

Research has been creating continuously new knowledge and this Conference will spread the light of awareness about the latest and upcoming areas in Engineering and Technology. While praying for the institute to accomplish its mission, I send my best wishes and congratulate the students and the staff of the department for organizing this event.

I am sure that the Conference will not only provide a useful forum to the participants to share their expertise in their respective fields but will also be professionally beneficial to them.

On this prestigious day, on behalf of Amritsar College of Engineering and Technology, Amritsar, I wish all academicians and professionals for further fruitful interaction and future direction in this significant field. I congratulate the Electronics and Communication Engineering Department for organizing this Conference.

Dr. Om Kumar Harsh
Group Director
ACET, Amritsar

Communiqué

I am extremely thankful to the Management of Amritsar College of Engineering and Technology, Amritsar especially Honb'le Chairman & CEO Sh. Amit Sharma for their full support and motivation to organise the first International Conference on Research and Innovation in Engineering & Technology-ICRIET2014.

Organizing an international conference is always a big challenge, but looking at the efforts and the effective planning put up by the organizers, I am confident that this conference will live up to the expectations of the participants and the academic community in general.

ICRIET2014 aims at exploring the ideas through enlightened deliberations and their fruitful implementation both in industry as well as academics. I am sure that sharing of research ideas by the eminent keynote speakers would add to the professional skills of the conference delegates.

It would be a matter of great satisfaction, not only to the organizers but the whole research community, if some useful thoughts and directions for prospective development can come out of the deliberations of this conference.

I once again complement the entire organizing team and congratulate them for their remarkable effort in making this conference a great success.

Dr. V. K. Banga
Principal
ACET, Amritsar
Conference chair
ICRIET-2014

Communiqué

I am pleased to have the opportunity to witness and attend this "International Conference on Research and Innovations in Engineering and Technology" organized by the Department of Electronics and Communication Engineering at Amritsar College of Engineering and Technology, Amritsar.

Different spheres of Engineering and Technology starting from makers and suppliers around the world increasingly rely on research and experimental studies, for both component and systems level analysis. This gathering serves the urge that looks for advancements in every domain of Science, Engineering and Technology.

The "International Conference on Research and Innovations in Engineering and Technology" is a platform where research scientists and practicing engineers can share their experiences and ideas. This plenary session incorporating presentations and discussions by experts will certainly create awareness of the intricacies of the subject among the professionals, technologists' and research scholars.

I know that the success of the conference depends ultimately on the many people who have worked in planning and organizing the technical event with full dedication and commitment. So I congratulate the Electronics and Communication Engineering Department for organizing this conference successfully.

Dr. H. S. Gill
Principal ACHMT
ACET, Amritsar

Communiqué

I am exuberant that the department of Electronics and Communication Engineering is organizing the "International Conference on Research and Innovations in Engineering and Technology (ICRIET-2014)" on December 19-20, 2014.

In today's era new developments are occurring almost on daily basis. These developments are changing the shape of the society. Considering the fast pace of globalization and dynamic nature of Trends in Science, Engineering and Technology, the need of the hour is to provide a platform where experts on respective subjects may share the latest development and research.

I believe that organizing such event is must for enabling professionals, scientists, scholars and educators to analyse the future needs and keep themselves updated with latest advances in the field of science and technology. This event too is an effort to meet the surging technological challenges in Research & Development area, which is very important for Global development.

The conference received an overwhelming response from various professionals across the globe. We have received around 350 papers covering several areas of Science, Technology and Engineering and other related topics. The papers received in this conference have been reviewed by reviewer committee and editorial board depending upon the subject matter of the paper. After the review process, the submitted papers were selected on the basis of originality, significance, clarity for the objective of the conference.

I hope that the sincere efforts, zeal and vigour of the members of Electronics and Communication Engineering Department of ACET would be prolific enough in making this event a grand success.

Best Wishes

Dr. Tanu Preet Singh
Head, ECE
ACET, Amritsar
Organising Secretary
ICRIET-2014

Communiqué

It is my privilege and honor to welcome you to the FIRST 'International Conference on Research and Innovations in Engineering and Technology' which is held/organized at Amritsar College of Engineering and Technology, Amritsar from 19 – 20 December, 2014.

This conference provides an excellent opportunity to showcase your research work and share your expertise, so we as an Engineering Institution can move towards developing national and international priorities for research and development in the field of Science, Engineering and Technology which ultimately results in/leads to social wellbeing. This interdisciplinary conference will bring together academicians, researchers, administrators, industry representatives and students from various esteemed organizations from all over the globe to share and enhance knowledge on latest innovations in Engineering and Technology.

As you all know that organizing a conference is a task of massive responsibility. I have been able to accomplish this with the will and cooperation of numerous colleagues and seniors of ACET. I would like to express my gratitude to all those who have contributed towards this. I am thankful to all the authors whose papers are accommodated in the proceedings of the conference and also to those who could not find the space. I hope they will understand my predicament.

I excitedly look forward to your participation in the FIRST 'International Conference on Research and Innovations in Engineering and Technology' and with great pleasure I welcome you once again to this holy city of Amritsar.

Er. Sandeep Kaushal
Convener
ICRIET-2014

Communiqué

On the behalf of organizing committee, we feel privilege and welcome your active participation in International Conference on Research and Innovation in Engineering and Technology (ICRIET-14) at Amritsar College of Engineering and Technology, Amritsar, which literally means, a pool of nectar, a city of Golden Temple.

The ICRIET-14, a premier international conference is the vehicle to challenge and shift attitude towards very best research results, problem solutions, and insight on new challenges facing the field of Communication Systems, Network Security, VLSI, Computational Techniques, Algorithms and Protocols or Digital Communication.

ICRIET-14 Committee will provide an interactive stimulating and creative environment for you to enjoy, participate learn and share the advancements in this technological era. The conference sessions will enable conference participants to leave with a strong sense of insight and ways of providing leadership.

We are grateful to our main sponsors for their assistance and guidelines. We are confident that the conference becomes an occasion for researchers, academicians, professionals and students to acquire latest knowledge in the field of Engineering and Technology.

I wish this conference a great success.

Narinder Sharma
Co-ordinator
ICRIET-2014

Communiqué

It is a matter of great privelege for me that our department is organizing a “International conference on Research and Innovation in Engineering and Technology (ICRIET-14) on 19th -20th December 2014.This conference is going to be an important platform for the technical experts from different engineering streams.

This conference aims at exploring the ideas through enlightened minds and their fruitful implementations both in industries and academic research activities. International and National experts from various centres will deliver keynote lectures during the conference for enlightenment of professional skills in conference delegates.

It is my firm believe that by organizing such events we provide a platform for professionals, scientists, scholars and educators to analyze the future needs and updation with the latest advances in the field of science and technology. Moreover this event provides an effort to meet the surging technological challenges in Research and Development areas, which is very important for nation development.

For this special event, I take the opportunity to thank the Management, Director, Principal and staff of ACET for their encouragement and continous support without which this event would not have taken shape.

With Best Wishes.

Atul Mahajan
Associate Professor
ECE Department
Co-Convenor
ICRIET-2014

INDEX
International Conference on
Research and Innovations in Engineering and Technology – ICRIET 2014
December 19-20, 2014

PART III – Network Security and Privacy

PART IV – Management and E-Governance

PART V – Image and Signal Processing

PART VI – Mechanical and Automobile Engineering

PART VII – Electrical Engineering and Renewable Resources

Survey Of various Routing Protocol-A Review

Gagandeep kaur
Student, Dept. ofCSE
Amritsar College of Engineering & Technology
PTU, Jalandhar, Punjab
gagan11.cse@gmail.com

Dr. Tanu Preet Singh
Professor and HOD, Dept. of ECE
Amritsar College of Engineering and Technology,
PTU, Jalandhar, Punjab
tanupreet.singh@gmail.com

ABSTRACT

A Mobile ad hoc network is a collection of wireless mobile nodes forming a temporary network without the aid of any centralized administration. Mobile Ad hoc network are self-configuring and self-organizingand also wireless nodes that can dynamically form a network to exchange information without use any existing fixed network infrastructure It is a system in which mobile nodes connected by wireless links and free to be move dynamically .it means network configuration may change any time In this paper we have studied various routing protocols .The main objective of routing protocol is to have an efficient route establishment between pair of nodes , so that message can be delivered in timely manner .in this paper we studied various routing protocols

Keywords—MANET, ROUTING, PROACTIVE, REACTIVE, HYBRID

1. Introduction

A Mobile ad hoc network is a group wireless mobile node that transfers the packet from source to destination by using the transitional nodes. The nodes in the network act as routers for transferring the packets. As nodes in the network are highly mobile, this causes the topology to be highly dynamic in nature. Routing in the mobile ad hoc network is a challenge in this type of network where topology is getting change highly. The MANET is a collection of self-configuring nodes which does not depend on any infrastructure . The property of MANET is its easy exploitation. Due to this property it can be used in military and emergency areas. Many routing protocols are proposed in MANET like AODV, DSR and DSDV [1]. MANETs possess certain characteristics like Bandwidth-constrained, variable capacity links, Energy- constrained Operation, Limited Physical Security, Dynamic network topology, Frequent routing updates. Ad hoc network can be used in areas where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Some applications of ad-hoc network are student using laptop to participate in an interactive lecture , business associates sharing information during a meeting, soldier relaying information about situation awareness in a battlefield. Ad hoc network are created ,for example when a group of people come together and use wireless communication for some computer based collaborative activities ;this is also called spontaneous networking [4]. Mobile Ad-hoc Network usually has a dynamic shape and a limited bandwidth. Ad hoc radio networks have various implementation areas. Some areas to be mentioned are military, emergency, conferencing and sensor applications [3].

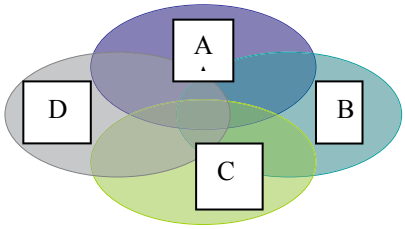


Figure 1 A Mobile Ad Hoc Network with 4 Nodes

2. Routing in MANETs

A Mobile Ad Hoc Network or spontaneous network is an infrastructure less, self-organized and multi-hop network with rapidly changing topology causing the wireless links to be broken and reestablished on the fly. A key issue is the necessity that the Routing Protocol must be able to respond rapidly to the topological changes in the network. In these networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and destination may have to communicate via intermediate nodes [2].

Routing in MANETs has been an active area of research and in recent years numerous protocols have been introduced for addressing the problems of routing. The routing protocol overhead traffic is not allowed to drive the network to congestion nor is a local change in link not allowed to cause a massive control traffic storm throughout the network.Traditional routing protocols used for wired networks cannot be directly applied to most wireless networks because some
common assumptions are not valid in this kind of dynamic network. For example, one assumption is that a node can receive any broad- cast message sent by others in the same

subnet. However, this may not be true for nodes in a wireless mobile network. The band- width in this kind of network is usually limited. Thus, this network model introduces great challenges for routing protocols [3].The energy efficient routing may be the most important design criteria for MANETs, since mobile nodes will be powered by batteries with limited capacity. Power failure of a mobile node not only affects the node itself but also its ability to forward packets on behalf of others and thus the overall network lifetime. This paper surveys and classifies numerous energy-efficient routing mechanisms proposed for MANETs. A mobile node consumes its battery energy not only when it actively sends or receives packets, but also when it stays idle listening to the wireless medium for any possible communication requests from other nodes. Thus, energy- efficient routing protocols minimize either the active communication energy required to transmit and receive data packets or the energy during inactive periods. The transmission power control approach can be extended todetermine the optimal routing path that minimizes the total transmission energy required to deliver data packets to the destination. For protocols that belong to the latter category, each node can save the inactivity energy by switching its mode of operation into sleep/power-down mode or simply turns it off when there is no data to transmit or receive. [5].

2. ROUTING PROTOCOLS IN MANET

We will discuss the classification of existing wireless ad hoc routing protocols. The Routing Protocols for ad hoc wireless networks can be divided into two categories based on the routing information update mechanism. They could be Reactive (On-demand), Proactive (Table-driven) [15]. Figure 2 shows the two categories of Ad hoc RPs and various proposed Protocols under each category:

1. Proactive routing protocols.
2. Reactive routing protocols.

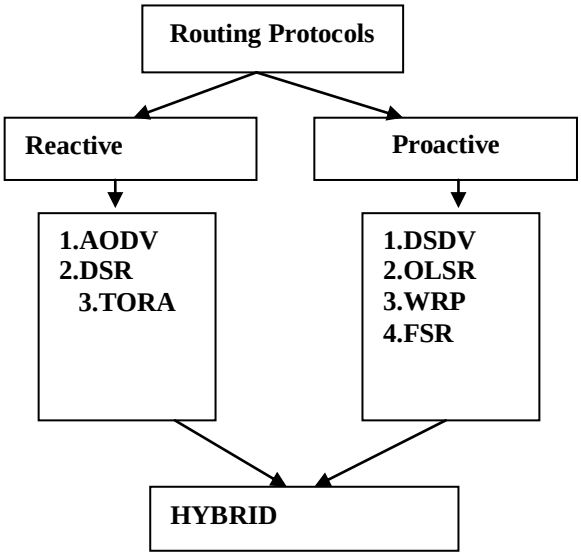


Figure 2 Basic Category of Routing Protocols.

3. Proactive Routing Protocols

In Proactive, nodes maintain one or more routing tables about nodes in the network. These routing protocols update the routing table information either periodically or in response to change in the network topology. The advantage of these protocols is that a source node does not need route-discovery procedures to find a route to a destination node. On the other hand the drawback of these protocols is that maintaining a consistent and up-to-date routing table requires substantial messaging overhead, which consumes bandwidth and power, and decreases throughput, especially in the case of a large number of high node mobility. These protocols always maintain up-to-date information of routes from each node to every other node in the network. These protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. Different protocols keep track of different routing state information [2]. These protocols require each node to maintain one or more tables to store up to date routing information and to propagate updates throughout the network. As such, these protocols are often also referred to as table-driven. These protocols try and maintain valid routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table driven ad hoc routing protocolsThere are various types of Table Driven Protocols: Destination Sequenced Distance Vector routing (DSDV), Wireless routing protocol (WRP), Fish eye State Routing protocol (FSR), Optimized Link State Routing protocol (OLSR)[1].

3.1Distance Sequenced Distance Vector

Distance sequenced Distance Vector (DSDV) is a table driven routing protocols which promote the packets from one node to another node using routing table. The routing table usually contains the next hop information and sequence number DSDV routing protocol depends on a well recognized algorithm Bellman-Ford algorithm where each device maintain the shortest path to the next device in the network of devices [10]. DSDV routing protocols is a proactive routing protocol that solves the major setback of wired network which is count to infinity problem by introducing the distance sequence number [4]. The major use of sequence number used in DSDV routing protocol is to check freshness of route. The node with the greater entry is used to forward the packet as it will contain a new fresh route. The sequence number is also used to discriminate the stale route from new one [5].It is a destination based distance vector routing protocol in which every node maintains a routing table. This routing table contains all available destinations, the next node to reach to destination, and the no of hops between it. Whenever any node changes its position it broadcast the routing updates to the other nodes. Sequence number is used to avoid loop freeness. Keeping the simplicity of distance vector protocol it guarantees loop freeness it reacts immediately on topology changes. Since the route for destination is always available at the routing table of

each node so there is no latency caused by route discovery.The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last updates communicated earlier. So, the updates are both time-driven and event-driven. The routing table updates can be circulated in two ways: a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental updated packet, then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent[10].

3.2 Optimized link state protocol(OLSR)

Optimized Link State Routing (OLRS) is a topology- based, neighbor selection protocol, in which each node only maintains a subset of network topology information. OLRS is a proactive protocol, because it exchanges the topology information with other nodes regularly to maintain information required for routing. OLRS reduces the cost of distributing network-scale link-state information by two ways. First, it uses multi- point relays (MRP) to reduce redundant re- broadcasting during flooding operation [4]. That is the key concept of the protocol. MRPs are selected nodes, which forward broadcast messages during the flooding process**.**. The main advantage of OLSR protocol was that it was good for dense network which was not supported by AODV protocol. In OLSR each node periodically broadcast hello messages to learn topology up to 2 hops. Based on this hello messages each node select its set of MPR's. The problem in this type of protocol is to select a minimal set of MPR each time the topology changes which is a NP hard problem. However in this paper we are concerning on the energy efficient protocols the traditional OLSR protocol was not suitable for the viewpoint of energy efficiency which is a critical issue in case of mobile ad-hoc network. Several enhancements have been done by the professionals for making it energy efficient which is as follows OLSR protocol does not take energy saving techniques into account proposed a new energy efficient unicast routing protocol EOLSR which made it energy efficient. EOLSR increases the network lifetime by selecting the path having minimum cost where the cost is calculated on the basis of residual energy of each traversed node and the energy conserved on this path**[**10**].** OLSR is based on the following three mechanisms: neighbor sensing, efficient flooding and computation of an optimal route using the shortest-path algorithm. Neighbor sensing is the detection of changes in the neighborhood of node. Each node determines an optimal route to every known destination using this topology information andstores this information in a routingtable**.** The shortest path algorithm is then applied for computing the optimal path. Routes to every destination are immediately available when data transmission begins and remain valid for a specific period of time till the information is expired[5].

3.2 Wireless Routing protocol (WRP)

The Wireless Routing Protocol (WRP) is a proactive, destination-based protocol. WRP belong to the class of path finding algorithms. The typical feature for these algorithms is that they utilize information about distance and second-to-last hop (predecessor) along the path to each destination. Path-finding algorithms eliminate the counting-to-infinity problem of distributed Bellman- Ford-algorithms by using that predecessor information, which can be used to infer an implicit path to a destination and thus detect routing loops.In WRP nodes exchange routing-table update messages only from a node to its neighbors. An update message contains such components as an update list. An update list entry specifies a destination, a distance to the destination and a predecessor to the destination. When a link fails or a link-cost changes, node recomputed the distances and predecessors to all affected destinations, and sends to all its neighbors an update message for all destinations whose distance or predecessor have changed [6].The Wireless Routing Protocol (WRP)is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list(MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor [6, 7].

.3.3Fish-eye Source Routing (FSR)

Fisheye Source Routing (FSR) is based on a method to divide each node's neighborhood to blurred zones so that the information details and accuracy is better for nodes to be near. The name's basis is on the phenomenon of fish eye's ability to see objects the better the nearer they are. In FSR zones are classified according to the distance, measured by hops, from the node[6].FSR is a protocol to be built on top of another protocol. It can be applied to work together with some link-state protocols as GSR. In GSR link state packets are not flooded but nodes maintain a link state table based on the up-

to-date information received from neighboring nodes and periodically exchange it with their local neighbors.Fisheye State Routing (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from node increases. Figure 1 defines the scope of fisheye for the center (red) node**.** The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctlybecause the route information becomes more and more accurate as the packet moves closer to the destination. FSR scaleswell to large networks as the overhead is controlled in this scheme.

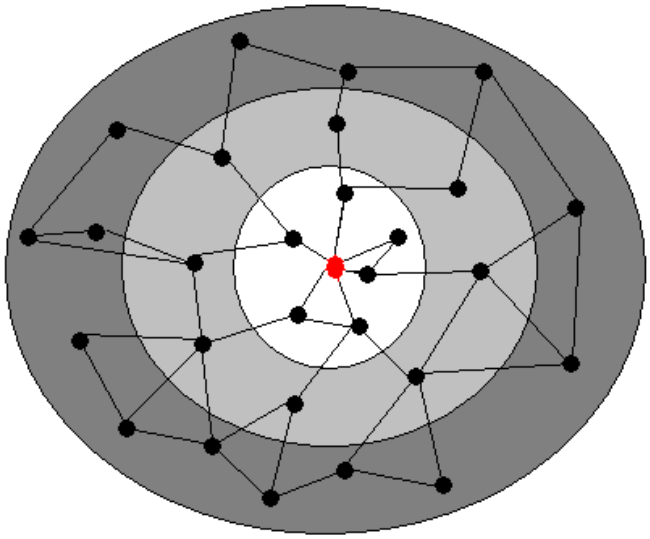


Figure 3 Accuracy of information in FSR [5]

4. Reactive Routing Protocols

Reactive routing is also known as on-demand routing protocol these protocols have no routing information at the network nodes if there is no communication. These protocols take a lazy approach to routing [3]. They do not maintain or constantly update their route tables with the latest route topology. If a node wants to send a packet to another node then this protocol searches for the route and establishes the connection in order to transmit and receive the packet.such protocols are often also referred to as on demand. The common element in reactive protocols is the mechanism used for discovering routes. The source node emits a request message, requesting a route to the destination node. This message is flooded, i.e. relayed by all nodes in the network, until it reaches the destination. The path followed by the request message is recorded in the message, and returned to the sender by the destination, or by intermediate nodes with sufficient topological information, in a reply message.

4.1 ADHOC on-Demand Routing Protocol

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self- starting, and scales to large numbers of mobile nodes.

AODV is a reactive or source initiated routing protocol which is based on the concept of DSDV. AODV mostly consists of two phases [6]:

Route Discovery stage

Route maintenance stage

Route Discovery phase

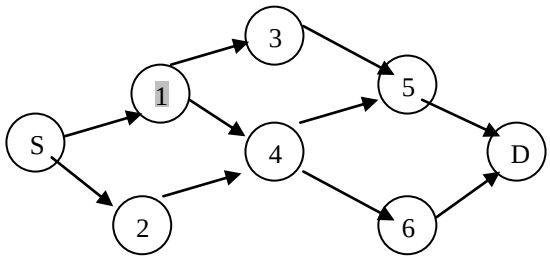
AODV is a source initiated routing protocol in which source broadcast the route request packet (RREQ) to all the neighbors. The neighbors in turn broadcast the packets to other neighbors until one of the node send the route reply (RREP) packet or the RREQ packet reaches to destination node. There are three types of control packets used in AODV [6]

Route request (RREQ)

Route Reply (RREP)

Route Error (RRER)

RRER control messages are used when the link between the two nodes break then the consulting node send the RRER control message to the source node so that route discovery can be initiated again. The node that has the path to the destination node or the node itself sends the reverse path to the source n ode.

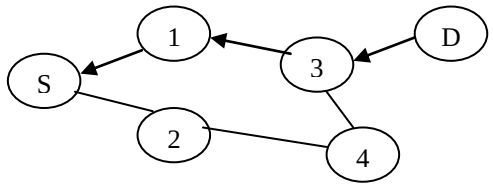


RREQ ⟶

Figure 4Route discovery Process in AODV.

Route Maintenance Phase

As the nodes in the mobile ad hoc network are mobile, there are chances of breaking of route between the nodes. In this case route maintenance comes into action. Whenever the path between the two nodes breaks it send the route error control message to the source node [6].



RREP

Figure 5 Propagation of route reply in AODV.

4.2 Distance Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. It is similar to AODV in that it forms a route on- demand when a transmitting computer requests one. Except that each intermediate node that broadcasts a route request packet

Distance Source Routing(DSR) is a source initiated routing protocol. In DSR, the sender knows the complete hop- by-hop route to the destination. These routes are stored in a route cache [6]. When a sender wants to transmit the source packet to another node, which is not in the range of that node, send an information packet to all the neighboring nodes. This process is called route discovery process. Detection of the appropriate route is done with the help of propagation of RREQ packet. There is a flooding of route request packets to all the nodes in the network until the destination node reaches [7].

The Route request packet carries the entire information about the route to be traverse by the node. The destination node replies with the entire route to the source in the reverse direction.

The main task of the sender is to transmit the route request packet to all the neighbors for propagation of RREQ packet until the destination node met. If the node is not the destination node then it broadcast the packet to the neighboring node. Then the destination node send the reverse path bask to the source node [7].

Now the feature of DSR protocol is route maintenance. Each node which is transmitting the packets is responsible for confirming the packets sent by it has been successfully received by the destination node. If it is not happening then it is the responsibility that a route error packet should be transmitted to back to the source node. So that the source can again initiate the route discovery process. This process is called route maintenance [7].

TheDSRprotocoliscomposedoftwomechanismsthatworktogether toallowthediscoveryandmaintenance of source routes in the ad hoc network:

Route Discoveryis the mechanism by which a node S wishing to send a packetto a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.

4.3 Temporally Ordered Routing Algorithm (TORA)

TORA is another source-initiated on-demand routing protocol Built on the concept of link reversal of the Directed Acylic Graph(DAG).In addition of being loop-free and bandwidth efficient .TORA has being highly adaptive amd quick in route repair during link failure ,while providing multiple routes for any desired source/destination pair.these properties make it especially for large highly,dynamic,mobile ad hoc environment With dense nodes populations[4]. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. In comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks. TORA involves four major functions: creating, maintaining, erasing and optimizing routes. Since every node must have a height, any node which does not have a height is considered as an erased node and its height is considered as null. Sometimes the nodes are given new heights to improve the linking structure. This function is called optimization of routes.

4.3 Hybrid Routing Protocol (HARP)

HARP - hybrid ad hoc routing protocol. HARP is a hybrid scheme combining reactive and proactive approaches. The routing is performed on two levels: intra-zone and inter- zone, depending on whether the destination belongs to the same zone as the forwarding node.In HARP, each node maintains only routing information of those nodes that are within its zone, and its neighboring zones. The routing is performed on two levels: intra-zone and inter-zone, depending on whether the destination belongs to the same zone as the forwarding node. Intra-zone routing relies on an existing proactive mechanism, and HARP includes reactive mechanism for the inter-zone

routing. Zone creation and proactive behavior in relation to network properties are provided by DDR - dis- tribute dynamic routing [11]. On the other hand, HARP is responsible for discovering and maintaining paths to satisfy application requirements. HARP aims at establishing the most stable path from a source to a destination in order to improve delay performance due to path failure. HARP applies the path discovery mechanism between zones that intends to limit flooding in the network, and that filters the candidate paths as soon as possible according to the stability criteria. As stability is the most desired parameter, HARP offers different mechanisms to anticipate path failure along with path maintenance procedure whose complexity is reduced by the proactive nature of the routing algorithm within a zone. These procedures reduce the delay that stems from a path failure during data transmission.There is a trade-off between proactive and reactive protocols. Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So a Hybrid protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols. Hybrid routing protocol is combination of both proactive and reactive routing protocol. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Hybrid protocol is suitable for large networks where large numbers of nodes are present. In this large network is divided into set of zones where routing inside the zone is performed by using reactive approach and outside the zone routing is done using reactive approach [14].

An adaptive hybrid routing protocol requires the following three properties for successful deployment [13].

Adaptive: The protocol should be applicable to a wide range of network characteristics. It should automatically adjust its behavior to achieve target goals in the face of changes in traffic patterns, node mobility and other network characteristics.

Flexible: The protocol should enable applications to optimize for different application-specific metrics at the routing layer. These optimization goals should not be set by the network designer, but be placed un- der the control of the network participants.

Efficient: and Practical: The protocol should achieve better performance than pure, non-hybrid, strategies without invoking costly low-level primitives such as those for distributed agreement or re- liable broadcast.

References

1.TanuPreet Singh, Shivani andVikrant Das"Energy-Efficient Routing Protocols In Mobile Ad-HocNetworks",International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE) volume 2,Issue 1,January 2012.

2. Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma "Review of Various Routing Protocols for MANETs",International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.

3.Thakare,p.p joshi M.A nadRaur A.D"A Review paper on routing protocols of wireless ad hoc network technology "International Journal of Networking, Volume 2, Issue 1, 2012.

4.Geetajayakumar and G.Gopinath,"Ad Hoc Mobile wireless Networks Routing Protocols-A Review",journal computer science and application,October 2007.

5.Shiva parkash,J.p saini"A review of Energy Efficient Routing Protocols for Mobile Ad Hoc Wireless Networks", International Journal of Computer Information Systems, Vol. 1, No. 4, 2010.

6.PetteriKuosmanen "Classification of Adhoc routing protocol", 2012.

7. Limin Meng; Wanxia Wu, ―Dynamic Source Routing Protocol Based on Link Stability Arithmetic‖ IEEE publications, December 2008.

8.Hong Jiang, "Performance comparison of three routing protocols for ad hoc networks", IEEE conference publications, August 20011.

9. C.Siva Rammurty and B.S. Manoj , "Ad hoc wireless network architectures and protocols" ISBN 978-81-317- 0688-6, 2011.

10.Surya Kant, Dr. Krishan Kumar,"Performance Analysis Of Dynamic Source Routing Protocol In Wireless Mobile Ad Hoc NetworkInternational Journal of Engineering Research &Technology(IJERT) Vol. 1 Issue 10, December- 2012 .

11. Bhabani Sankar Gouda, Ashish Kumar Dass,LakshmiNarayan "A Comprehensive Performance Analysis of Energy Efficient Routing Protocols in different traffic based Mobile Ad-hoc Networks",IEEE 2013

12. Geethu Mohandas, Dr.Salaja Silas, Shini Sam," Survey onRouting Protocols in Mobile Ad Hoc Network", IEEE 2013.

13 Dr.S.S.Dhenakaran, A.Parvathavarthini "An Overview of Routing Protocols in Mobile Ad-Hoc Network",International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),volume 3 ,issue 2 ,February 2012

14 Manish Sharma1 , Gurpadam Singh "Evaluation of Proactive, Reactive and Hybrid Ad hoc Routing Protocol for various Battery models in VANET using Qualnet "October 2013

An Account Of Clustering Schemes In VANETs

Manverpreet Kaur
Research Scholar, M.Tech (CSE)
Deptt. Of CSE, ACET Amritsar
Amritsar, India
manverpreet05@gmail.

Er.Amarpreet Singh
Associate Professor
Deptt. Of CSE, ACET Amritsar
Amritsar, India
comamarmandeep@yahoo.com

Abstract- : **VANETs is a special type of MANETs which uses vehicles as a mobile node. It uses the intelligent transportation system in which vehicles can communicate with each other to avoid large number of increasing accidents on roads . The communication between the vehicles is at greater risk because the messages are broadcasted by wireless channel and vehicles move with high mobility. With dissemination of messages, vehicles can change their position and direction which causes communication gap between the vehicles. To overcome such situation and achieve efficient communication among these vehicles clustering algorithms are used. Cluster formation in the VANETs is more challenging because vehicles are highly mobile. This paper focus on the survey of clustering algorithms proposed for stable cluster formation and more efficient communication.**

***Index Terms*—Transportation System, VANETs, Wireless Channel, Clustering**

I.INTRODUCTION OF VANETs

Vehicular Ad Hoc networks develops a vehicular communication system to enable fast and efficient distribution of data for the safety and comfort. VANETs defines two modes of communication V2V and V2R as shown in fig.1 .[1] V2V means vehicle to vehicle communication. V2R means vehicle to Road Side Unit. VANETs has less infrastructure, self-organize and autonomous network where vehicles can freely move within the network. VANETs turns every participating vehicle into wireless router or node , allowing vehicles approximately 100 to 300 meters of each other to connect and create a network with wide range VANETs.[2]

Vehicles send messages in network regarding road information, unnatural activities on road and their personal information to other vehicles of the network. These communications are donethrough the wireless medium. In VANETs communication are done through the wireless medium. In VANETs, communication can be done by using three ways which are Inter –Vehicular communication (IVC), Inter-Road Side Unit communication (IRC), and Road Side Unit to Vehicle communication (RVC). Thus, due to dynamic nature of VANETs, it likely to face stale entries and congestion. In order to overcome these kind of problems many Solutions have been proposed of which clustering is one of the solution technique. Clustering decreases the messages count and increase the connectivity in the network.

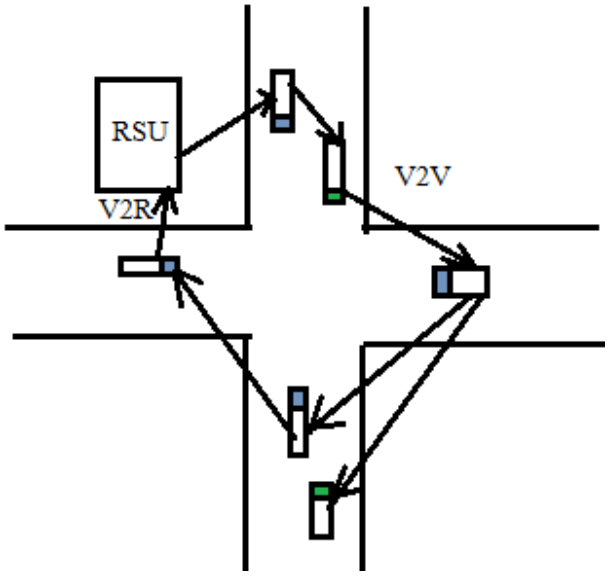


Figure no. 1

II.CLUSTER

Clustering is a technique for grouping nodes in geographical area together, making the network more robust and scalable**.** The process of grouping nodes i.e. mobile devices, sensors, vehicles etc. together according to some rules and divides the network into interconnected substructures called clusters These rules differ from one algorithm to another and are the key factor to build stable clusters. [3] Clusters are a kind of virtual groups that have been formed by a clustering algorithm. Each cluster contains atleast one cluster Head and two or more cluster members. Cluster head is selected by these members byusing some techniques. The size of the cluster depends upon the transmission range of the wireless communication that each node contains. However, some filter prevents the nodes to join a cluster byusing someclustering algorithm. For instance, one of the most frequently used is the movement direction filter i.e. a cluster nodes could not join the cluster whose cluster Head moves an opposite direction.

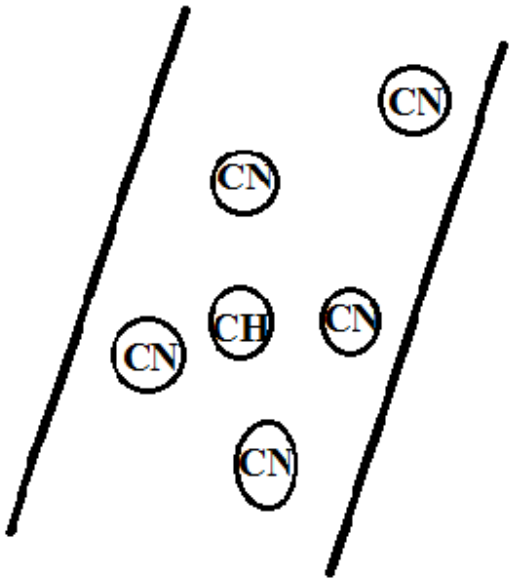


Figure no.2

In VANETs cluster is represented by set of mobile vehicles that are moving on the Highway scenario and urban scenario . The figure No.2 depicts the Highway scenario where cluster Head is in the Center and cluster nodes are move around it . Each cluster node can communicate directly with Cluster Headand two Cluster nodes can communicate with each other in worse case i.e. by cluster Head.

III.IMPORTANCE OF CLUSTER

The basic idea is that of grouping network nodes that are in physical locality. The subsequent backbone uses the induced hierarchy to form a communication infrastructure that is functional in providing desirable properties such as minimizing communication overhead, increasing the probability of aggregating redundant data, choosing data aggregation points, and so on. An accident happens in a highway at a point in time where traffic is more, and in VANETs the vehicles approaching the place of accident are able to “detect” the accident. The accident effects in the highway being blocked. In such a situation density of vehicles increases dramatically and a clustering method is necessary for the appropriate dissemination of safety messages.

IV. ADVANTAGES OF CLUSTERING

The dynamic VANETtopology produces many challenges for communication and networking. In traditional Mobile Ad hoc Network (MANET) research, these difficulties were often overwhelmed by a clustered topology. As a result, clustering has become a common topic in the VANET research community. These problems were often overcome by a clustered topology. [15]

1. HandleDynamic Network -The Stable Clustered networkhandles Dynamic network topology, resulting from the high mobility and high node-density of vehicles. This dynamic topology causes routing problems as well as congestion from floodingand because of densenetwork the hidden node problems are arise.

2. Stable Network-: A clustered structure can make the network appear smaller and more stable in the view of each node [17], [18].

3. Improved Congestion-: Clustering handle "broadcast storm problem" which calls the congestion by re- broadcasts and flooding. The dynamic topology of VANETs demand a high frequency of broadcast messages to keep the surrounding vehicles updated on position and safety information. All of this flooding leads to severe congestion, which can be improved by a clustered topology [14], [15].

4. Reduces Broadcast-: In the clustered network, only the cluster head participates in handing routes, which greatly reduces the number of necessary broadcasts.

V.CLUSTERING PROTOCOLS FOR VANETs

Researchers proposed many clustering schemes for VANET. Although, VANETS has their own clustering schemes but it also uses clustering schemes of MANET for cluster formation. Hence, this paper describes these schemes according to the parameters that they possess. Classification of the clustering schemes in vehicular network is summarized below:-

A. Mobility based Clustering schemes

In this categorythe protocols consider only mobility characteristics of vehicles as one of the parameter for selecting clusters and cluster heads in the network .The mobility based clustering schemes is further classified into two types :-

1. Direction based on clustering schemes [6]

This clustering scheme is based on direction of vehicles for selective effective clusters in the vehicular network. The direction based clustering algorithm is suitable for urban area .In this scheme, clusters are formed before road intersection point and the vehicles that take the same turn are cluster together.The Direction Based Clustering is further divided into -:

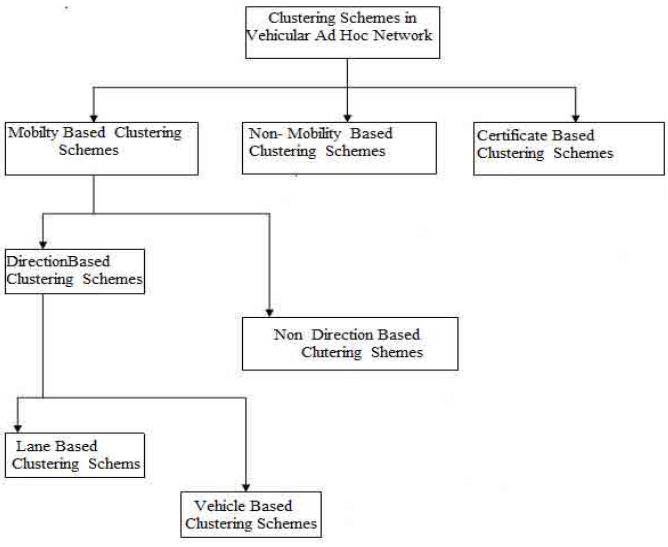


Figure No. 3

a) Lane based clustering scheme

The lane clustering schemes consider the direction of traffic on road as one of the parameters for calculating efficient and comparatively stable clusters in VANETS. In this technique cluster head is selected based on lane having the maximum traffic flow. Each vehicle has knowledge of a lane of traffic and broadcast this information to nearby vehicles. Every vehicle computes their cluster head levels by using lane weight,average distance level, network connectivity level and average velocity level of the traffic [4].

b) Vehicle based clustering scheme

In which protocols using the direction of vehicles for selection of clusters and cluster head. These protocol are-:

LORA –DCBF- : (Direction Cluster Based Flooding): It is a routing algorithm based on position of vehicle. It uses direction of vehicles and GPS for cluster formation. This global positioning scheme allows two or more cluster head for the same cluster, provided that the cluster head in opposite directions. In this hop to hop fashion, node uses the most recent location information of the neighboring nodesfor packetrouting in the network. To control traffic onto the network only selected nodes are used i.e. gateway nodes for dissemination of messages. Although, there are different direction nodes have different cluster Heads but this strategy is more effective and results in more stable clusters.

AMACAD- :(Adaptable Mobility Aware Clustering Algorithm) [8] This algorithm is proposed to represent the Behavior of vehicles and their mobility patterns in groups for vehicular network. AMACAD uses mobility pattern of the network to increase the lifetime of clusters. It reduces the global overhead, decreases thecluster re - affiliation and also avoid group re - clustering. The metrics consideredfor stable cluster formation are current location, speed, relative destination and final destination of vehicles in the network. This scheme transmittedmessages by groups which causes increasing the Communication delay, low data delivery, reliability congestion issues.

VWCA- : (Vehicular Weighted Clustering Algorithm) [13] It is an effective clustering algorithm using a complex metric for more stable clusters and increased connectivity in the network. It is a weighted clustering algorithm proposed for highway scenarios for improved stability and connectivity of VANET. This metric is used for stable cluster formation by using the number of neighbors, the direction of vehicles, the entropy, and the distrust value parameters. Stability and connectivity can be enhanced and overhead can be reduced by considering these parameters for cluster formation in the network. For electing cluster head, this algorithm uses weighted clustering value, which has weighted sum of distrust value of a vehicle, entropy value of a vehicle, number of neighbors of a vehicle and direction measure of a vehicle. Vehicle having the minimum weighted clustering value is elected as the cluster head. If vehicle cannot identify any cluster head in its neighborhood, it simply declares itself as a cluster head. But if there is more than onevehicle with same minimum weighted clustering value, the vehicle holding higher entropy or lower distrust value is selected as the new cluster head.

2. Non-direction based clustering schemes

These protocols using mobility without specify direction as the metric for selecting cluster and cluster Heads known as Non-direction based schemes. The protocols of this Scheme are- :

VMaSc-: (Vehicular Multi Hop algorithm for stable clustering) [10] The key metric of this technique is relative speed. In this clustering technique a cluster Head is selected by considering the least mobility function. The least mobile node can be defined by using the speed difference between the neighboring nodes in the networks. Clustering is based upon changes in relative mobility of vehicles by calculating average of relative speed of all the neighboring nodes moving in the same direction. The connection between Head member pair is weaker than the multi - hop clustering member election is based on cluster information reception.

KCLS Protocol [11]- : (K –Hop Clustering Structure) It is a location service protocol which combines both Connectivity and mobility of vehicles. Thus, this technique can be selected cluster formation with trade – off betweencommunication overheads and vehicle locations. Cluster formation in KCLS protocol are quite stable as the mobility of vehicles is considered as per the average link expiration time. It can increase the life time upto 50 percent than other clustering techniques of VANETs . During a creation of new cluster in the network, a cluster state message been broadcasted by cluster Head. Depending upon the received cluster state packets, the cluster Head updates the location information of cluster and establish location service table in the network. The cluster state packet contain the corresponding cluster ID, the cluster Heads co- ordinates , cluster member list and neighboring cluster list.

ASPIRE- : (Adaptive Service Provide Infrastructure) is a Clustering scheme proposedfor vehicular ad hocnetwork where clustering is done in a distributed manner. [12] This scheme helps in generating largeclusters and also providing high network connectivity. The technique lowers cluster head durations and increases the number of cluster head changes. It reduces the infrastructure costs in the network by using mere vehicles on roads. ASPIRE architecture consists of vehicles that form clusters with relatively lower mobility. In these clusters some nodes act as Cluster Members (CM) while the other acts as Cluster Heads (CH). Every cluster has a single cluster head. These clusters in turn form Mobile Network, each with a Mobile Router. ASPIRE provides caching potentials between clusters formed by vehicles and NEMOs, reducing the overhead and cost of accessing the fixed service provider network for each vehicle request or binding update due to a topology change.

B. Non Mobility Based Schemes

The Non Mobility based schemes of vehicular ad hoc network do not uses the mobility one of its metric. One of the Protocols of this technique is- :

CBLR (cluster based location routing) This technique is discussed by R.A. Santos et al. It uses a multi hop network and implement clustering technique in evaluating inter- vehicular traffic of data on a motor way . To distributes states the nodes in the vehicular networkuses HELLOmessage. when a new node entering into the network either it joins the existing cluster or create the new cluster by acting as a new cluster Head. Thus to do this each node must know the position and location of others nodes in the cluster. In which each cluster Head contain the member list to contain the address and geographic locations of its member nodes and also maintain the cluster head neighbor table to contain the information about its nearest cluster Head.

C. Certificate Based ClusteringSchemes

In certificate based schemes protocols use clustering scheme for certificate generation or revocation. The following are few protocols which fall under this category - :

Tahani Gazdar et al. [14] discuss a dynamic public key infrastructure for VANETs that aims to allocate the role of the central certification authority among a set of dynamic chosen Certificate Authorities (CA). Election of dynamic CAs is based on a clustering scheme where cluster heads perform the role of certificate authorities. The dynamic demilitarized zone (DDMZ) formed by confident nodes which are located at 1-hop distance from cluster head of the same cluster. These confident nodes are intended to perform as the registration authorities (RA).

Ghassan Samara et al. discuss a new security mechanism that attains secure certificate revocation. Revoking some or all the certificates of the complex vehicles is called as certificate revocation. This allows other vehicles to avoid any information from those vehicles that can cause problems. Certificate re-vocation is done in circumstances where any misbehaving vehicle having valid certificate (VC) is discovered, or where an RSU replaces old valid certificate with new invalid certificate. Generally, an RSU changes VC with an invalid certificate. This is done in order to inform other vehicles about avoiding this vehicle. This happens when more than one vehicle inform to RSU with the same VC and broadcasts wrong data.

VI. CONCLUSION

VANETs have high mobility featuresthan MANETs. So, Traditional clustering algorithms developed forMobile ad – Hoc network are difficult to implement for Vehicular ad hoc networks due to high mobility feature involved. So, to provide the solution, a brief overview about various clustering algorithm are discussedand are classified based on the parameters used to form stable and effective clusters in the networks that increases the connectivity between the vehicles.

REFERENCES

[1 International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-3, January2011 Implementation and Performance Analysis of AOD Routing Protocol in VANETs

[2] International Journal of Computer Engineering an Applications, Volume VI, Issue III, June 14 ISSN 23213469AODV ROUTING PROTOCOL FOR IMPROVING EFFICIENCY IN VANETPrerana Deshmukh1, Prof. Shrikan Sonekar

[3] Communications and Network, 2013, 5, 8-14 doi:10.4236/cn.2013.52B002 published Online May 2013 Survey of Clustering Schemes in Mobile Ad hoc Networks Abdelhak Bentaleb

[4] A Survey on Clustering Algorithms forVehicular Ad-Hoc NetworksSamo Vodopivec, Janez Bešter, and Andrej Kos

[5]A SURVEY ON CLUSTERING TECHNIQUES USED IN VEHICULARAD HOC NETWORK1TADIPARTHI PRIYANKAP. Basu, N. Khan, and T.D.C. Little. "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks,"ICDCSW, 2001, pp. 413-418

[6] N. Maslekar. (2011, July). A stable clustering algorithm forefficiencyapplications in VANETs. 7th International Wireless Communications andMobile ComputingConference (IWCMC). pp. 1188 – 1193

[7] Mohammad S. Almalag and Michele C. Weigle, "Using TrafficFlow for Cluster Formation in Vehicular Ad-hocNetworks", IEEE 35th Conference on Local Computer Networks (LCN), 631-636, 2010

[8] Mildred M. Caballeros Morales, Choong Seon Hong andYoung Cheol Bang, "An Adaptable Mobility-AwareClustering Algorithm in Vehicular Networks", In: proc. Of Network Operations and Management Symposium2011

[9] Christine Shea, Behnam Hassanabadi and Shahrokh Valaee, "Mobility-based Clustering in VANETs using Affinity Propagation", In proc. of Global Telecommunication Conference, 1-6, 2009

[10] Seyhan Ucar, Sinem Coleri Ergen and Oznur Ozkasap,VMaSC: Vehicular Multi-hop algorithm for StableClusteringin Vehicular Ad Hoc Networks", In: proc. of WirelessCommunications and Networking Conference (WCNC), 2381-2386, 2013

[11] L. Zhang, H. Elsayed and E. Barka, "A Novel Location ServiceProtocol in Multi-Hop Clustering Vehicular Ad Hoc Networks", In: proc. of International Conference on Innovations in Information Techno

A Review on Authentication Schemes in Vanets

Priya Sharma
M.Tech(CSE), Research Scholar
Department of Computer Science and Engg.
Amritsar College of Engineering and Technology
Amritsar,India
priyasharma.20013@gmail.com

Er. Amarpreet Singh
Associate Professor
Department of Computer Science and Engg.
Amritsar College of Engineering andTechnology
Amritsar,India
amarmandeep@yahoo.com

Abstract: Secure communication and privacy preservation are the two major concerns in the design of Vehicular Ad-hoc Networks (VANETs). Feebly designed vehicular network are more prone to attacks on the network and makes the security of drivers vulnerable. From security perspective of VANET features, it should be ensured that no intermediary can collect private information about drivers .VANETs should possess robust security architecture to function in un-trusted and unsecured environments as wireless attacks may come from anywhere and from all directions. As a result, authentication is regarded as a useful mechanism that can effectively protect vehicles from nasty or malicious users. In this paper , various emerging authentication techniques are discussed to provide basis to understand authentication levels ,schemes and criteria in VANETs. One or more technique can be combined to design more efficicent and cost-effective mechanisms for authentication.

I.INTRODUCTION

VANETs System consists of huge number of nodes, around number of vehicles exceeding million in the world today [13], these vehicles will necessitate an authority to govern it, every vehicle can communicate with other vehicles using short radio signal whose range can reach 1KM. This vehicular communication is an Ad-Hoc communication in which each associated node can progress profusely,and uses no wires. The Road Side Unit(RSU) perform like a router between the vehicles on the road and are also connected to other network devices. Each vehicle is equipped with separate On-board unit (OBU), which attach the vehicle with Road Side Unit via DSRC radios. A Tamper Proof Device(TPD) is used to conceal the vehicle secrets, along with the information regarding the vehicle approximating keys, drivers individuality, trip particulars, speed, route, etc.

Similar other device such as Event Data Recorder (EDR) is used in vehicles to register to all parameters especially during critical situations like accidents. Earlier vehicles were also provided with Electronic License Plate (ELP) embedded with unique cryptographically verifiable numbers that will be used as traditional license plates. The advantage of ELP's is that they will automate the paper based document checkups of vehicles. It will help in detection of stolen cars, identifying vehicles on crossing country borders or during annual technical checkups.[1] All the above mentioned components are used to protect Vehicular communication against wide range of threats. Still researches are made to enhance security of data transferred from one vehicle to another .That data may include the control message or warning message or other informative data [2].

1. Warning messages -to prevent detected risky situations.
2. Traffic management and added value -to provide Internet services.

Despite VANETs share general features with conventional ad-hoc networks, they have individual characteristics that are decisive in the design of the communication system [6] these include:

(i)Dynamic topology, (ii)Mobility models,(iii) energy supply and (iv) Localization functionality.

Unfortunately, a VANETs system can be vulnerable to security attacks which may compromise the driver's privacy (i.e. disclosing his personal data) and even cause life-threatening situations (i.e. false warnings resulting in road accidents). To provide security shield to the vehicles so as to save them from various attacks and risks here major concern is given to the protection of exchanged messages using authentication as one of the tool.[20]

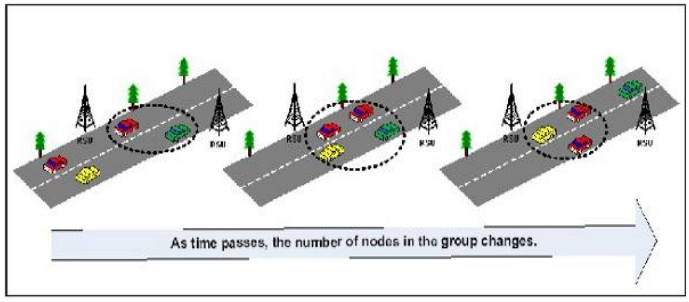


Fig1.The Dynamic nature of VANETs[23]

II.IMPORTANCE OF AUTHENTICATION IN VANETS

In recent studies, the use of Public Key Infrastructures and digital certificates have been proposed to provide a suitable solution to the authentication and authorization challenges in VANETs. The importance of authentication in vehicular communications is to ensure that, when a connection is established between two vehicles without previous knowledge of each other, they are actually communicating securely with their intended destination vehicle and not an intruder.[14]

But a secure network should possess following attributes:

Authentication :It is the verification of a user identity prior to granting access to the network. It is the first step of defense against intruders.

Non-repudiation :It is the verification that the data was sent with a user credentials so that without denial or repute the data can be associated to the sender.

Confidentiality : It is the assurance that the data could not have been accessed by any other user than the designated recipient for whom it was meant; thus insuring that the data was untouched until reception. Confidentiality is generally achieved by cryptography techniques.

Data integrity :It is the assurance that the content of the data was not modified while in transit. It is different from confidentiality as it allows for detection of data modifications.

Availability :It is the proportion of time that a system is in a functioning state.

Access Control :It means that user can access which type of resource and what permission user has.

Real-time constraints: At the very high speeds strict time constraints should be valued.[21]

Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information. Authentication is the keystone service, since other services depend on the authentication of communication entities[4,8].

III. QUALITATIVE REQUIREMENTS OF AUTHENTICATION IN VANETS

For authentication in Vehicular networks ,there are certain requirements which must be met for secure and qualitative authenticated vehicular communication:

1.Computation overhead: the amount of cryptographic operations a node has to compute for an authentication request in CPU time, for example,the time needed for verifying a digital signature. Lesser computational overheads leads to better quality of authentication.

2.Control overhead: the bandwidth overhead (in bytes per second) for an authentication request, for example, exchanging cipher keys or certificates.It should be less.

3.Latency: the time needed to respond to an authentication request and it should be as small as possible.

4.Initialization time: the time needed to initialize the authentication system, such as, setting up a certificate authority and key distribution.

5.Strong authentication: Authentication in vehicles should be strong.

6.Scalable: Authentication should be scalable.Highly scalable authentication improves secure communication.

7.Support for re-authentication and revocation procedures.[14]

IV.AUTHENTICATION LEVELS OF VEHICLES

We can provide authentication to nodes or vehicles at different level depending upon the authentication requirements of each node :

1.Node level authentication :it means that the message is proven to originate from certain node.

2.Group level authentication : here the message is proven to originate from a certain group of nodes.

3.Unicast authentication : in which the message is sent to only one node. Sometimes special messages are sent to specified node in vehicular ad hoc network .

4.Multicast authentication : here the message is sent to many nodes. Sometimes messages are sent not to all nodes in the vehicular ad hoc.[22]

5.Broadcast authentication: in which the message is sent to all nodes in the network.[14]

V.SECURITY MECHANISMS FOR MESSAGE AUTHENTICATION

A.Digital signature

Digital Signatures follows an Asymmetric Authentication Scheme.As user authentication[5] is a major concern in security issues so it verifies that only valid users exchange information. It not only avoids the malicious users from transmitting junk information and intercepting confidential information but also provides message legitimacy to protect the VANET system from outside attacks.

Digital Signatures are used to authenticate the safety messages. Since, safety messages do not contains any confidential information therefore we need only to authenticate them. This is the reason why no encryption of safety messages is required. To avoid the dissemination of false information, we need to ensure the authentication of the message. Though asymmetric authentication involves more overhead bits per data unit transmitted, but still Digital Signatures are preferred in VANET systems. Safety messages are need to be disseminated as fast as possible. Symmetric Authentication involves handshake mechanism which delays the transmission of safety messages.So here arises a need for using Digital Signatures to effectively disseminate the safety messages. The Digital Signatures are used in combination with Public Key Infrastructure(PKI). The sender encodes the message using public key cryptography and then signs it digitally before transmission. Public key cryptography provides security to the data while Digital Signature proves the authentication of the sender. A malicious user can intercept the information bits during transmission, modify

them using his public key and resends them, but still he would not be able to reproduce the digital signature of the authenticated user. The receiver will be aware that the information was transmitted by a malicious user as the message would not have authenticated digital signature[4]. Digital Signatures are assigned by a centralized government authority to prevent occurrences of any kind of discrepancy. There is a hardware called Tamper Proof Device(TPD) which signs all the messages transmitted from that user. TPD is a highly secure hardware device with its own battery and clock. TPD can only be accessed by authorized users. [2]

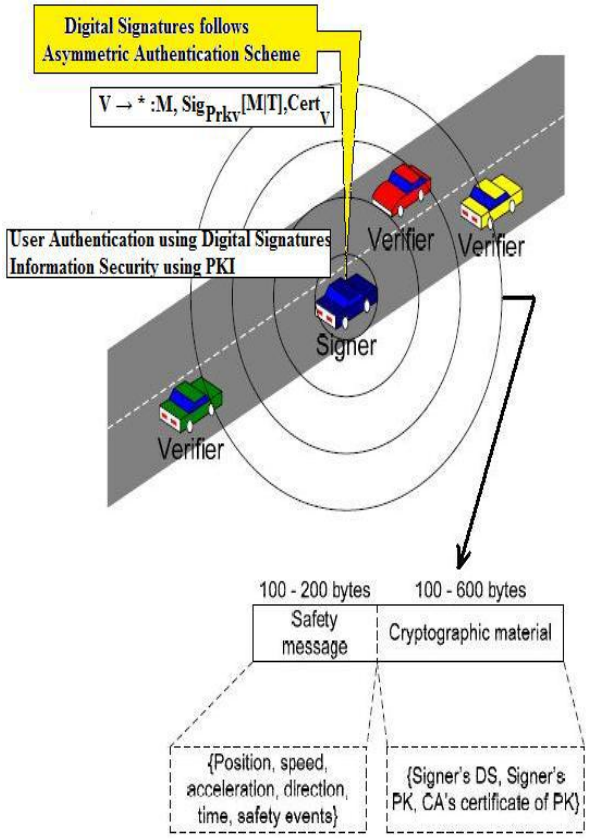


Fig2. Diagrammatic Representation of working of Digital Signatures authenticating a user.

B .Digital signatures with digital certificates

The user ensures the integrity of the message by signing the encoded message using Digital Signatures. This ensures the reliability of the message. The trustworthiness of the message can be increased by Certificate Authorities(CA) who will digitally sign the data and binds the public keys with private keys effectively to ensure User Authentication. In other words, CA issues certificates to the vehicles which mark the validity of the users. We need a centrally managed CA to avoid any discrepancy. Either a Government managed authority or the Vehicle manufacturers can act as the CA. In an Ideal situation, the vehicle manufacturer can provide the initial Temporary Certificate. This Temporary Certificate has to be validated to Permanent status only by the concerned Government Authority. The Certificate consists of details like the public key, the certificate lifetime and the Signature of the Certificate Authority. Regular Certificate Revocation will create a Certificate Revocation List. This list has to be appended to the Certificate after each revocation. The certificates that were signed by a CA can also be revoked in two cases of Information compromise:

i) Cryptographic keys get compromised
ii) A fraudulent user is using signed certificates to transmit fake information.

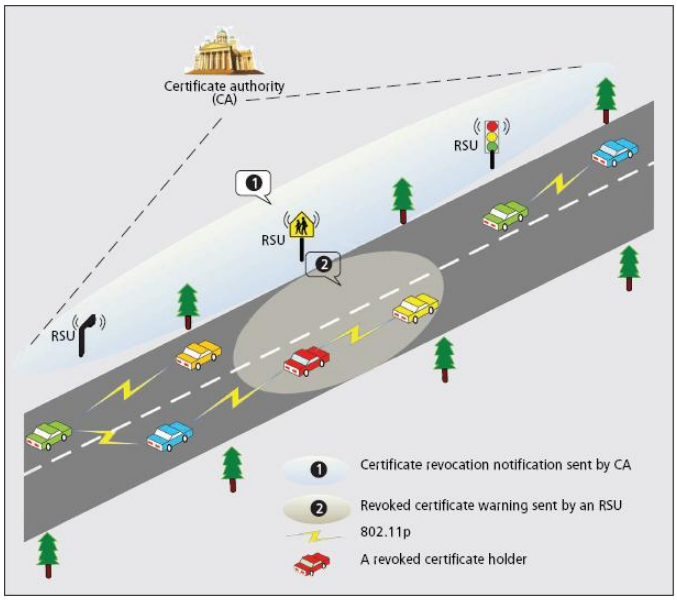


Fig3. RSU-aided certificate revocation.[23]

C.TESLA

TESLA is an acronym for "Timed Efficient Stream Loss-Tolerant Authentication". This authentication method is used for multicast and broadcast network communications. In VANET systems, PKI is not the only option to confirm User Authentication. So a completely different and efficient alternative to signatures is TESLA that instead of using Asymmetric Cryptography, uses symmetric cryptography with delayed key disclosure to prove that the sender was the authenticated source of the message. In other words, TESLA is a lightweight broadcast authentication mechanism that performs broadcast authentication mechanism and applies the same approach that is applied in the unicast authentication mechanism. This proves to be a more efficient way of broadcasting messages. TESLA is compliant to computational Delay of Service(DoS) attacks because symmetric

cryptography is significantly faster than signatures and thus delay is avoided. In spite of these versatilities, TESLA is susceptible to attacks arising due to memory-based Denial of Service[7]. In TESLA, the information send by the source is stored at the receiver's end until the corresponding key is disclosed. TESLA depends completely on time to provide the necessary asymmetry in the authentication scheme, allowing only the sender to generate a broadcast authentication at a given point of time. Though symmetric cryptography significantly reduces computation, but still it fails to prevent the occurrence of repudiation.

D.Group signatures

A group signature scheme allows members of a group to sign messages on behalf of the group. Verification of signatures can be performed with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, there exists a designated group manager who can, in case of a later dispute, open signatures, i.e., reveal the identity of the signer. Group signatures could for instance be used by a company for authenticating price lists, press releases, or digital contracts. The customers need to know only a single company public key to verify signatures. The company can hide any internal organizational structures and responsibilities, but still can find out which employee (i.e., group member) has signed a particular document.It is assumed that all communications between the group members and the group manager are secure.[9]

In the group signature, one group public key is associated with multiple group private keys. In a group signature scheme, even though an eavesdropper know that a message is sent by the group, it cannot identify the sender of the message. A general vehicular communication framework based on group signature is given in[17]

A group signature scheme must satisfy the following properties:

1. Only group members are able to correctly sign messages (unforgeability).
2. It is neither possible to find out which group member signed a message (anonymity) nor to decide whether two signatures have been issued by the same group member (unlinkability).
3. Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so (security against framing attacks).

A consequence of the last property is that the group manager must not know the secret keys of the group members.[9]

E. Identity based signatures

Identity Based Encryption Scheme (IBE) was first proposed by Shamir in 1984, this mechanism provides authentication, confidentiality, message integrity, non repudiation and pseudonymity. IBE scheme was originally used to simplify certificate management in email systems. The identity based encryption scheme is specified by four algorithms: Setup, Extract, Encrypt, and Decrypt

Setup: It takes security parameter k and returns system parameter with master key. The system parameters include a description of finite message space *M* and description of finite cipher text space *C*. These system parameters will be publicly known whereas the master key will be known only to private key generator (PKG).

Extract: This phase takes input from system parameters, master key and arbitrary ID and returns a private key *d*. Here ID is the arbitrary stream that will be used as public key and d is the corresponding private decryption key. So the extract phase generate private key from the given public key.

Encrypt: Input parameter for this phase are system parameters, ID, M, with these parameter it will generate the cipher text C.

Decrypt: It takes input parameters like system parameters cipher text C and private key d and returns the original message M. These algorithms must satisfy the standard consistency constraints i.e. the private key d must be generated through Extract phase when it is supplied with ID as the public key.[1]

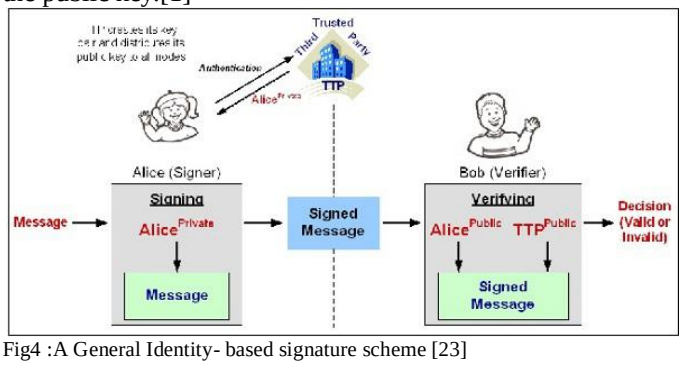


Fig4 :A General Identity- based signature scheme [23]

F.Hybrid Signature

Hybrid signature is a security protocol method which makes use of two types of digital signature: ETE signatures and HTH signatures. Given that there are alterable field(mutable fields) and unchallengeable field(non- mutable fields)in the packets of PBP, this security method uses hybrid signatures to ensure the integrity of the dissimilar type data individually. End-to-end signatures protect the mutable data between sources and destination. Hop-to-hop signatures protect the immutable data between two neighbors. [10]

G.Proxy signatures

A proxy signature scheme is a variation of the ordinary digital signature scheme which enables a proxy signer to generate signatures on behalf of an original signer. Later, the

verifier, which knows the public keys of original signer and a proxy signer can check a validity of a proxy signature issued by a proxy signer.[16]

In general, there are three different types of delegations: full delegation, partial delegation and delegation by warrant.

- In a full delegation proxy signature scheme, a proxy signer uses the same private key as an original signer and creates the proxy signature as an original signer does. The drawback of a full delegation comes from a difficulty of distinctive between an original signer and a proxy signer.
- In a partial delegation proxy signature scheme, the original signer derives the proxy key from his private key and passes it to the proxy signer in a secure channel.It has two types : protected and unprotected proxy signature schemes. In unprotected proxy signature scheme, a proxy signature is generated by both the proxy signer and an original signer. In this case, the verifier cannot distinguish the identity of a signer. In the protected proxy signature scheme, a proxy signature is generated by the proxy signature key of an original signer and also with a private key of a proxy signer.
- In the proxy signature scheme with delegation by warrant, an original signer provides the proxy signer a special message namely warrant. The warrant certifies that a proxy signer is legal and contains signer identity,delegation period and the types of a message on which proxy signer can sign.[11]

There are several kinds of proxy signature schemes.

1)Proxy multi-signature:

Proxy multi-signature means a proxy signer can generate the signature for a message on behalf of several original signers. It can be used in the following scenario: A company releases a document that may involve the financial department, engineering department, and program office, etc. The document must be signed jointly by these entities, or signed by a proxy signer authorized by these entities. One solution to the latter case of this problem is to use a proxy multi-signature scheme. The proxy multi-signature primitive and the first efficient solution were introduced by[15]. Since then proxy multi-signature has become an active cryptography research area.

2) Multi-proxy signature allows the original signer delegate his singing power to a group of proxy signers.

3) Blind proxy-signature allows the user to obtain a signature of a message from several signers in a way that each signer learns neither the message nor the resulting signature.[19]

H.Elliptic curve digital signatures

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematically derived form of Digital Signature Algorithm (DSA). It is a mathematical representation for the elliptic curve analogue of the DSA. It has been accepted as a standard worldwide. It is an ANSI standard, as well as IEEE, NIST and ISO standard. The strength per key bit is significantly greater in an algorithm using elliptic curves because elliptic curve discrete logarithm problem has no sub exponential-time algorithm. Being a mathematical entity, the security of elliptic curve can be described in mathematical terms only. The complex computation and mathematical hardness of the ECDLP contributes towards its security. It is advantageous to use ECDSA to provide secure and faster dissemination of information after authenticating the users in environments where amount of storage offered is less and lesser response time is allocated for user authentication. Asymmetric ECDSA key pair is used in VANET systems to provide User Authentication[2]. ECDSA can also be used to generate and verify signatures. Thus ECC is preferred as it provides same level security at 160 bit key length as of 1024 bit key length in RSA. [12]

Advantages of ECC

The ECC offers remarkable advantages over other cryptographic system:

1. It provides greater security for a given key size.

2. It provides effective and compact implementations for ryptographic operations requiring smaller chips.

3. Due to smaller chips less heat generation and less power consumption.

4. It is mostly suitable for machines having low bandwidth, low computing power, less memory.

5. It has easier hardware implementations.

So far no drawback of ECC had been reported.

VI.CONCLUSION

Security within vehicular ad-hoc networks is an important issue. One or more techniques can be used to provide authentication depending upon prevailing scenario. A combination of two schemes can also be used to reduce overheads and increase efficiency. Among the discussed technique in this paper digital signature is considered as the building block or fundamental security requirement. TESLA protocol offers authenticity at reduced costs without involving any shared secret between senders and receivers. ID-based schemes don't require distributing certificates and by that saves bandwidth. ECDSA is the most efficient scheme till date as compare to group signatures which is slower. Of all the discussed schemes ECDSA offers remarkable advantages.

References

[1] Kohli Sandhya & Rakesh Dhiman "Secure Message Communication using Digital Signatures and Attribute Based Cryptographic Method in VANET" International Journal of Information Technology and Knowledge Management July-December 2010, Volume 2, No. 2, pp. 591-594

[2] Dahiya, A., & Sharma, M. V. "A survey on securing user authentication in vehicular ad hoc networks".

[3]Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: SASN '05, New York, NY, USA, ACM (2005) 11–21

[4] S. Hahm, Y. Jung, S. Yi, Y. Song, I. Chong, and K. Lim, "Self-organized Authentication Architecture in Mobile Ad-hoc Networks" International Conference on Information Networking (ICOIN) 2005.

[5] M. Raya, P. Papadimitratos, and J.-P. Hubaux. "Securing Vehicular Communications" In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

[6]Zanella, A., Fasolo, E. "Inter-vehicular communication networks: a survey" In: 2nd Internal NEWCOM Workshop. (2006)

[7] Yih-Chun Hu and Kenneth P. Laberteaux. "Strong VANET security on a budget" In Proceedings of the 4th Annual Conference on Embedded Security in Cars (ESCAR 2006), November 2006.

[8] D. Park, C. Boyd, E. Dawson. "Classification of Authentication Protocols: A Practical Approach" Proceedings of the Third International Workshop on Information Security.

[9] Camenisch Jan ,et al "Efficient Group Signature Schemes for Large Groups (Extended Abstract)"

[10]Smita Garg " Reliability And Efficient Protocol For Position-Based Routing In Vehicular Ad Hoc Network" in International Journal Of Core Engineering & Management(IJCEM) Volume 1, Issue 4, July 2014

[11] Sattar J Aboud and Sufian Yousef "A practical proxy signature scheme" International Journal of Digital Information and Wireless Communications (IJDIWC) 2(4): 27-36, 2012

[12] Aqeel Khalique, et al "Implementation of Elliptic Curve Digital Signature Algorithm" International Journal of Computer Applications (0975 – 8887)Volume 2 – No.2, May 2010

[13]SUMO-Simulation of urban mobility [EB/OL]. http://sumo.sourceforge.net/. Access time: 2011-08-27.

[14] Khalid Haseeb ,et al "A Survey of VANET's Authentication", 2010

[15]Yi, L., Bai, G., Xiao, G., 2000" Proxy multi-signature scheme: a new type of proxy signature scheme" Electronics Letters 36 (6), 527–528.

[16] Sattar J Aboud and Sufian Yousef "A PRACTICAL PROXY SIGNATURE SCHEME" International Journal of Digital Information and Wireless Communications (IJDIWC) 2(4): 27-36
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2225X-658X)

[17]J. Guo, J.-P. Baugh and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. IEEE INFOCOM*, Anchorage, Alaska, May 2007.

[18] Yong Hao,et al " A Distributed Key Management Framework with Cooperative Message Authentication in VANETs" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[19]Xiaofeng Chen ,et al "ID-Based Multi-Proxy Signature and Blind Multisignature from Bilinear Pairings".

[20] Jetzabel Serna, et al, "Geolocation-based Trust for Vanet's Privacy" Journal of Information Assurance and Security 4 (2009) 432-439

[21] Upasana Singh et al, "Review of Solutions for securing the Vehicular Networks" Int. J. Comp. Tech. Appl., Vol 2 (5), 1652-1656

[22] Anna Lysyanskaya,et al, "Multicast Authentication in Fully Adversarial Networks" .

[23] http://www.intechopen.com/books/computational-intelligence-and-modern-heuristics

VANETs AND ITS SECURITY CLASSES

Er. Chhailadeep Kaur[1], Er. Anjali Passi[2], Dr. TanuPreet Singh[3]
[1]Assistant professor, CSE Department, GNDU Amritsar campus (INDIA)
er.chhailadeep@gmail.com
[2]Research Scholar, DAV University, Jalandhar(INDIA)
yadu.anjali@gmail.com
[3]Professor & HOD, ECE Department, Amritsar College of Engineering, Amritsar (INDIA)

Abstract
In today's world Vehicular Ad hoc Network done promising job towards public safety and provide important element to the transport facility. Security is the main concern to VANET as there are number of ways of attacking the VANET by analyzing communication medium, DOS attack ,DDOS attack and so many .The main aim of this purpose is to know various kind of attacks happened in VANETs.

***KEYWORDS*:** NETWORK, Road side unit, Traffic, VANETs, V2V, V2I

I INTRODUCTION

To manage the traffic manually is difficulttask. Increase in traffic indirectly affects the safety of people and environment of traffic. In last few year observation it is clear that the nearly 1.2 million people lost their life in road accident .So many companies invest their money to manage the traffic .So VANETs are introduced to manage the road traffic and safe the road side accident.[2]

Now in developing stage of technology provides an efficient and well mannered way to manage the transportation technique. With the help of internet potential and communication devices managed the transportation system very efficiently and in a great manner. These facilities can be divided into three parts: Fixed network, Mobile wireless network and hybrid network. The fixed network leads to have many problems like it require access points, cable wires and some equipment which must be digital .the wireless network i.e. mobile ad hoc network are the superset of Vehicular Ad hoc Network .VANETs are the important class of MANET where traffic are managed, distributed ,decentralized network and self organized network.VANETs are self- organized network where vehicles nodes are connecting and communicate with each other and focuson reducing the traffic insecurities with the help of internet facilities.

VANETs also called to INTELLIGENT TRANSPORT SYSTEM (ITS)

The mode of communication can also be further divided into:

- V2I(Vehicle –To-Infrastructure)
- V2V(Vehicle -To-Vehicle)

Vehicle–To-Infrastructure: In this mode of communication, the road side sensors are placed to know the vehicle movement and gathered all important information for managing the real time traffic. In this mode, there is need of infrastructure such as sensors.

Vehicle–To-Vehicle: In this mode of communication, vehicles are communicated with each other without the need of road side sensor. The main Objective is to decrease the level of accident and traffic jam on road by observing the density of traffic and many other activities on road side. [2]

Road Side Unit (RSU): The road side unit collects the important information such as jam on traffic, average speed of vehicle and density of vehicles, and many more. It broadcast this collectively information to the nearby vehicles of particular distance. It captures the real time traffic information and accurately broadcast to the vehicle.

IITYPES OF ATTACKERS

The various types of attackers are:

- Insider and Outsider
- Malicious attacker
- Rational attacker
- Active and passive attacker

AInsider Attacker
This type of attacker is insider who is authorized user and well knows about the network technologies. Insider attackers have the great knowledge of design, its network configuration which they can change according to their need. Insider attacker is more dangerous than outside attacker. They have the capabilities to launch any type of attack to disturb the network configuration. Simply in law man word, we can say that wrong things in network done by right man.

B Outsider Attacker
The attacker of this kind has less power than insider attacker. They observe the network traffic and traffic configuration after that launch the attack .The main aim of attacker is to misuse the network protocol.

CMalicious Attacker
Malicious attacker is those who have not any personal benefit for disturbing the network system.

D Rational Attacker
Rational attacker is those who have their personal benefit to attack the traffic of road. They generally do all those activities to get some money or someone hire them to disturb the traffic management system. They did activities for money.

E Active attacker
They send some kind of signal or packet to activate other attacker. From the word of active attacker, we can conclude that they remain to be active throughout so that they can't be unaware of some important information to pass the other attacker.

FPassive Attacker
They observe traffic on network or monitor whole scenario of traffic

III CHARACTERISTICS OF VANETs

- High Mobility: In this, it is harder to find position of vehicular node and to protect the node privacy because nodes in VANETs work at very high speed.
- Frequent Information exchange: As the road side unit helps to gathered the collectively information of road traffic, jam. Any vehicle can communicate with each other and exchange information frequently.[3]
- Wireless Communication: The Design of VANETs has been done for the wireless environment. So that any vehicle get the information.
- Avoid collision : In collision avoidance if two vehicles are coming in the same point and that point is not clearly visible then with the help of VANET both the drivers get a message of warning from this vehicle are safe to collide.[4]
- TimeOptimization: If any vehicle suffers the jam or accident in road then vehicle passed the information to each other so in this way time waste get less.
- Cooperative Driving: Road side unit are available on road. These unit broadcast the message of jam, rail collision, warning zone, parking site so that driver can be more attractive by receiving message.
- Availability of map information and current point
- Change in topology of network: As node rapidly changes its position with respect to speed of vehicle then network topology has to frequently upgrade itself.

IV ATTACKS IN VANETs

Attacker in VANETs plays important role to distract the network by changing its originality of message. Researchers have studied many different kind of attacks happened in VANET.Some of proposed classes of attacks are:[4][11]

- Attack on Network
- Attack on Application
- Attack on Timing of Vehicle
- Supervise Attack

AAttackson network
In VANETs, node and infrastructure are the main element [6].The attacker generally focuses on Vehicular nodes and infrastructure so that create problem for the specific or valid user that can't access the network. An attackers can change the network configuration or send any DOS attack, DDOS attack, Sybil attack, Node impersonate attack

iDOS (Denial Of Service)attack: DOS attack is the most dangerous attack on network. As the network availability for users is most important concern in the environment of vehicular. [1]Inthis, attacker overload or jam the main medium of communication so that there is no availability of network for specified user .The main aim of attacker is not to access the network to specified user. It create problem to user to access infrastructure and vehicle to vehicle communication also can't work for DOS attack happened in network.

In figure 1,attacker A generate the DOS attack where user B,C,D cannot able to communicate with each other and also cant able to connect with the infrastructure .In this way it jams the whole network area and communication path between V2I and V2V.

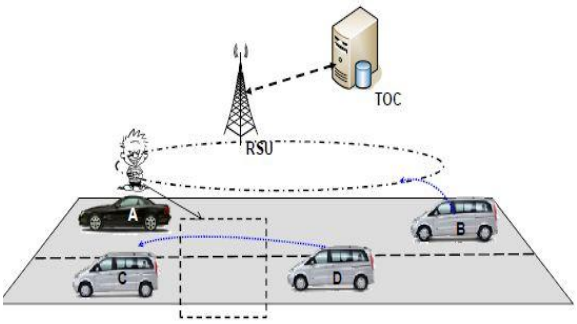


Fig 1 DOS attack which affects the V2V and V2I

ii DDOS (Distributed Denial Of Service) Attack: This kind of attack is dangerous as their mechanism is in distributingmanner. In this attack, there may be different location and different time slot which affect the particular user .It is more effective than DOS attack .The main objective of this attack is to decrease the speed of network. In Figure 2 shows that attacker generates the DDOS attack on vehicle A by Vehicle B, C, and D.

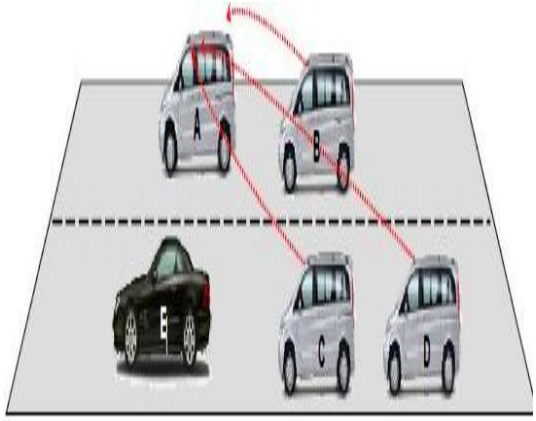


Fig 2 DDOS attack between V2V

In Figure 3 shows that the attackers (B, D, C) attack on the infrastructure from different location whereas A, E vehicle try to access the network because of overload in network they can't able to access the network .This is called DDOS attack between V2I.

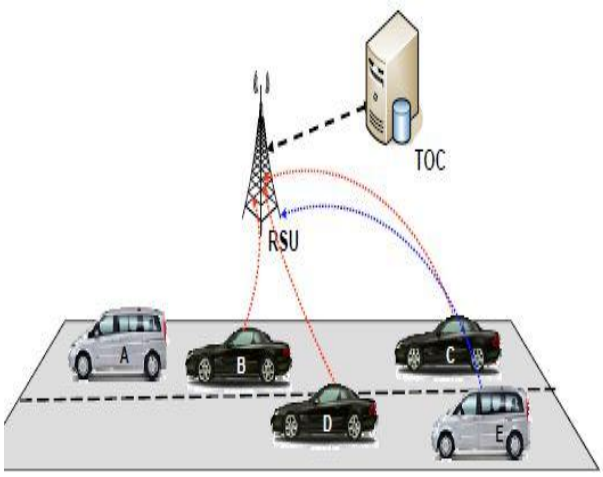


Fig 3 DDOS attack between V2I

iii Sybil Attack : In this attack ,wrong messages are send such as jam in traffic and generate many messages to other vehicle with different fabricated identity(source ID).In this way it provide illusion to other nearby vehicle so that other vehicle quit that road for the sake of attacker.[7][9]

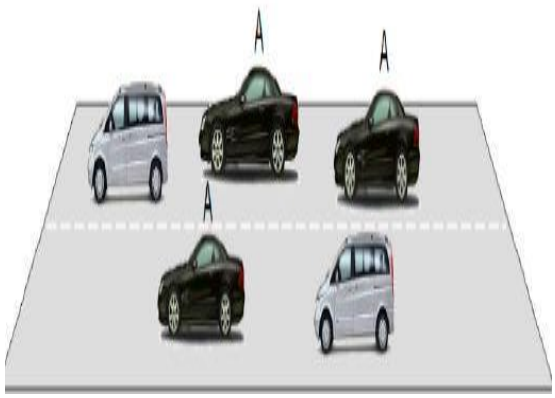


Fig 4 Sybil Attack

B Attacks on application

There are two type of vehicular potential i.e. safety and non-safetyapplication [5] .The main aim of this attack is to alter the content and pass the wrong message to nearby vehicle. In safety application ,it generate the important warning message to the nearby vehicle and assume that nearby vehicle is attacker than attacker alter the content of message and send the wrong messages to other user. This creates the road accident .The warning message can be road on construction, crash, Lanechange, rail collision and so many.

In this figure 5 shows that vehicle A send the warning Zone message to vehicle B but as vehicle B is attacker alter this information as 'Road clear' to vehicle C.

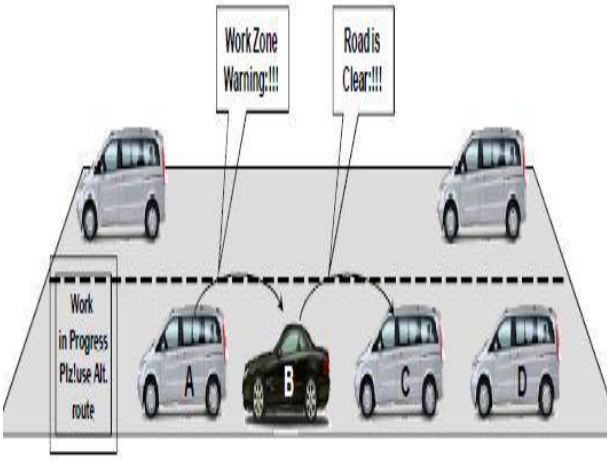


Fig 5 Safety Applications Attack

Non safety application is used to manage the traffic .As Road side Unit provide the information about shopping mall parking or some availability of parking area.

In this figure 6 Road side unit provide the information of parking slot availability and vehicle A pass this information to vehicle B but vehicle B alter this content into 'No Parking Slot' is available which generate the traffic on road.

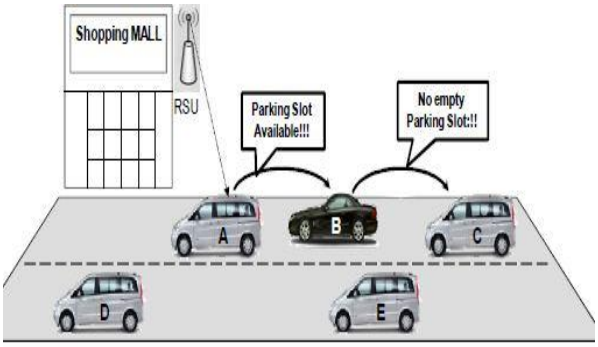


Fig6 Non Safety Application Attack

C Attacks on timing

In this attacker cannot change the original message content but delay the message to reach the other vehicle. In this figure 7 shows that vehicle B send the message of warning to vehicle C but vehicle C do not send this message at right time and delay to send this message to vehicle D .As other vehicle D get this message when accident actually occurred at location Y

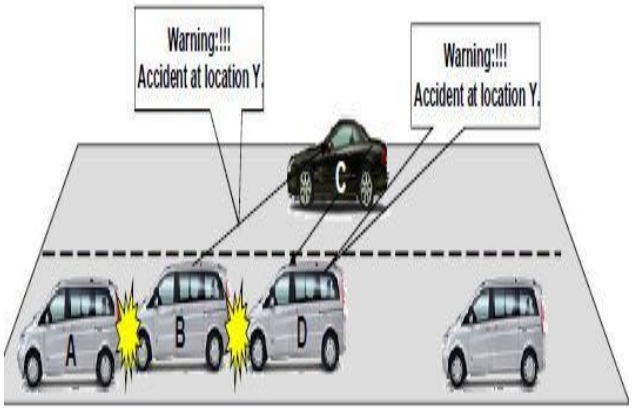


Fig 7 Timing Attack

D Supervise attack

In this attack, the attacker observes or monitors the communication medium between V2V and V2I and also observes the channel. For example police man plan to find the criminal from that route whereas the attacker listen whole communication and alert the other criminal about police's plan. In this case attacker should be alert so that important information can be passed to their criminal person. In this attacker only done their job of listening, not alter or changed the network message or anything else.

V SECURITY

For the security purpose of VANETs it must satisfy the following things:

- Authentication of message: The message regarding traffic or any other kind of message comes from authorized user. It must not be non authorized person.[5]
- Integrity message: the important information regarding traffic or road accident, jam, configuration must not be altered. The receiver data must be same as send by sender[2]
- Non-Repudiation message: If there is any communication between sender and receiver then sender cannot deny or refuse of sending any information to receiver.
- Confidentiality: The information must be kept secret .It must be secret from unauthorized user to gain information.
- Availablity: This means that there must be availability of network and application if there may be any chances of faults or malicious attack on network.
- Privacy: The privacy should maintain as such user information such as driving license, vehicle plate, its speed, and direction should be private. This information

only revealed in case of any crime happening or car accident occurs. This information is revealed to solve the dispute or for investigation purpose.[10]

- Traffic jamming: An attacker try to create jam the area so that it takes time to resolve the jam area and in the meanwhile attacker will perform their motive work.
- Enactment: An attacker can impersonate as an vehicle of emergency which misguide other vehicle vehicle or slow down the vehicle.It must not be there .For this it must be avoidable.[8]

V CONCLUSIONS

Security is the important concern to VANETs attack .As attacker attack the VANETs by various way by monitoring the path, sending the wrong message to other vehicle, delay to send the message, attacker use DOS so that user cant able to access the network .Safe information should be exchange from one vehicle to another vehicle .In this paper malicious attackers have their maximum try to distract or disturb the network .In this case fast cryptographic algorithm needed. Protocol of Ad hoc plays an important role in the VANETs. So VANETs security is needed at most extend level because in this case minor mistake can harm the human life.

REFERENCE

[1] D.Jiang,V.Taliwal, A.Meier, W.Holfelder and R.Herrtwich,"Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless Communication Magazine,Vol.13,No.05,Nov 2006,pp:36-43.

[2] Ram Shringar Raw, Manish Kumar, Nanhay Singh "Security Challenges, Issues And Their Solutions For Vanet", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013

[3] S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004

[4] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[5] YaseerToor et al., "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEECommunications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3,pp. 74-88.

[6] Ahmed Soomro, Hasbullah H.B., J.lb. Ab Manan (2010) *WASET* issue 65, ISSN 2070-3724

[7] Ajay Rawat, Santosh Sharma, Rama Sushil," Security Attacks And Its Possible Solutions",Issn: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-301-304

[8] AyonijaPathre ,Chetan Agrawal, Anurag Jain," Identification Of Malicious Vehicle In Vanet Environment From Ddos Attack",Jgrsc,Issn-2229-371x,Volume 4, No. 6, June 2013

[9] G. Guette,B.Ducourthial,"On the sybil attack detection in VANET", LaboratoireHeudiasyc UMR CNRS 6599,France.

[10] M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks"Journal of Computer Security,vol.15, january 2007, pp: 39-68

[11]HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan,"Denial of Service (DOS) Attack and Its Possible Solutions in VANET",World Academy of Science, Engineering and Technology, pp.411-415,Volume-65, 2010 .

A Survey of Greedy Routing Protocols for Vehicular Ad Hoc Networks

Sargun
Student M.Tech (ECE)
Guru Nanak Dev University
Amritsar, India
sargun08.kaur@gmail.com

Sobia Maan
Student M.Tech(ECE)
Guru Nanak Dev University
Amritsar, India
maansobia@yahoo.com

***Abstract*- A vehicular ad-hoc network is a new technology which has garnered enormous attention in recent years. Vehicular ad-hoc networks are special cases of mobile ad-hoc networks. Routing algorithms based on greedy forwarding such as greedy perimeter stateless routing are known to be very suitable for a vehicular ad-hoc network. In this paper, a survey of greedy routing protocols for vehicular ad-hoc networks is provided, and the advantages and disadvantages of these routing protocols are discussed, and some open issues and possible directions of future research related to using greedy routing protocols for vehicular ad-hoc networks are defuned.**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a set of mobile hosts capable of communicating with each other without the assistance of base stations [1]. MANET represent complex distributed systems that include mobile nodes that can dynamically self organize into arbitrary ad-hoc network topologies, allowing people and devices to seamlessly work in areas with no preexisting communication infrastructure such as, disaster recovery environments. Avehicular ad-hoc Network (VANET) is a form of mobile ad-hoc network (MANET), in which vehicles communicate with each other and with nearby fixed roadside equipment [2].In a VANET, vehicles move non-randomly along roads and exchange information with other vehicles and roadside infrastructure within their radio range [3]. A VANET provides both vehicle-to-infrastructure (V2I) communication and vehicle-to-vehicle (V2V) communication. The unique characteristics of VANETs include [4-5]:

- *High mobility with the constraint of road topology*: The vehicles in VANETs are usually moving at high speeds and non-randomly along roads.
- *Rapidly changing network topology*: Due to the highly variable speeds between vehicles, the network topology in VANETs tends to change frequently.
- *Frequently disconnected network*: Due to the rapidly changing network topology, the connectivity of VANETs could also be disconnected frequently.
- *Geographical type of communication*: Most applications in VANETs require identification of the vehicles in a certain region, instead of the specific vehicles. Compared to other networks, VANETs often have a new type of communication which addresses a geographical area where packets need to be forwarded (e.g., in safety-deriving applications).
- *Time-sensitive data exchange*: Most safety-related applications require data packet transmission in a timely manner. Thus, no security schemes can harm the network performance of VANETs.
- *Potential support from infrastructure*: Unlike common MANETs, VANETs can actually take advantage of infrastructure in the future. This property has to be considered to improve protocols and schemes for VANETs.
- *Abundant energy and storage*: The VANET nodes have abundant energy and computation resources, since nodes are vehicles instead of small handheld devices.
- *Better physical protection*: The VANET nodes are better protected than those nodes

in other MANETs. Thus, VANET nodes are more difficult to compromise, which is also good news for security provisioning in VANETs.

II. GREEDY ROUTING PROTOCOLS

In this section, a timeline of the greedy routing protocols for VANETs is presented and the potential influence with each other. Figure 1 shows the timeline of the greedy routing protocols according to their publication dates, and which protocols have been affected by others.

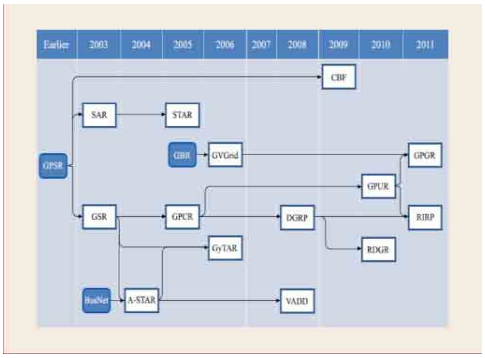


Fig.1.Timeline

A. *Greedy Perimeteer Stateless Routing*

Greedy perimeter stateless routing (GPSR) [7] is the best known greedy routing protocol for VANETs. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology. GPSR consists of two methods for forwarding packets: greedy forwarding and perimeter forwarding. GPSR exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. This process repeats at each intermediate node until the intended destination of the packet is reached. It goes back to greedy forwarding as soon as it overcomes local maxima.

B. *Geographic Source Routing*

Geographic source routing (GSR) [8] is the first protocol to use a map of the streets, and is mainly proposed for urban environments to avoid the problem of GPSR. GSR tries to overcome the disadvantages of position-based routing approaches designed for MANETs when applied to VANETs in urban scenarios. Using a static street map and location information about each node, GSR computes a route to a destination by forwarding messages along streets [9]. In GSR, a source node computes the shortest path to an intended destination using Dijkstra's algorithm based on the distance metric. The computed path consists of a sequence of junction IDs known as anchor points (AP), along which packets should be forwarded to reach the destination.

C. *Spatially Aware Packet Routing*

Spatially aware packet routing (SAR) [10] attempts to overcome some of the weaknesses of the recovery strategy used by GPSR [9]. SAR algorithms consist of GSR and the GSR-based packet forwarding. As shown in Figure 4, the source vehicle S can map itself and the destination vehicle D into the spatial model, and calculate the shortest path to the destination with a shortest path algorithm such as the Dijkstra algorithm. The source then sets the GSR to the shortest path, which consists of a list of intermediate vertices. The GSR will be embedded into the header of all data packets sent by the source vehicle.in SAR each forwarding vehicle maps the positions of its neighbors into the graph model and chooses the neighbor with the shortest path along the GSR to the destination as the next hop. After a vertex in the GSR is reached (i.e. the forwarding vehicle finds the vertex to be located within its radio range), this vertex will be removed from the GSR and the packet will be forwarded tothe next vertex of the GSR. With this approach, a packet will move successively closer to the destination along the GSR from one vertex to the next.

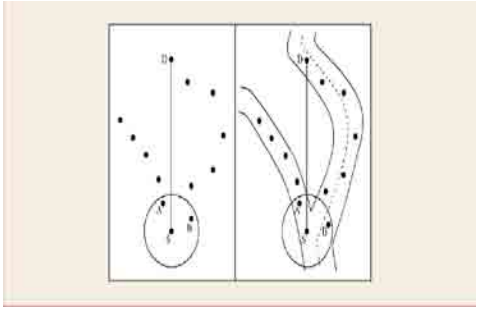


Fig.2. Concept of SAR

D. Anchor-based Street and Traffic Aware Routing

Anchor-based street and traffic aware routing (A-STAR) [11] is designed for V2V. A-STAR also aims to improve the problem where the perimeter mode of GPSR utilizes next-neighbor hops along a street instead of selecting the farthest neighbor along a street for the next hop [9]. It utilizes city bus routes to identify an anchor path with high connectivity for packet delivery in city environment. The anchors in the A-STAR are both geographic forwarding points to route packets and junctions that a packet must pass through to reach its destination.

E. Spatial and Traffic Aware Routing

Spatial and traffic aware routing (STAR) [12] is quite different from other position-based routing algorithms, and is designed to fix the drawbacks of the SAR algorithm. SAR has the advantage of its underlying spatial model, allowing it to forward packets along streets. STAR able to exploit both street topology information achieved from geographic information systems and information about vehicular traffic in order to perform accurate routing decisions, as shown in Figure 3.

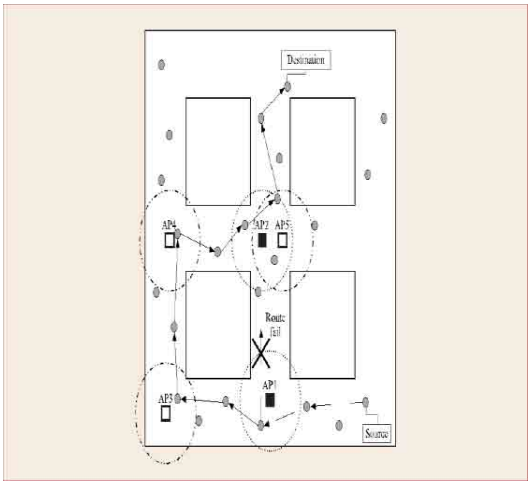


Fig 3. The Routing procedures for STAR

F. Greedy Perimeter Coordinator Routing

The main idea of GPCR is to take advantage of the fact that streets and junctions form a natural planar graph, without using any global or external information such as a static street map as shown in Figure 6. GPCR consists of two parts: a restricted greedy forwarding procedure and a repair strategy and junctions. Therefore it does not need a graph planarization algorithm. In the restricted greedy forwarding of GPCR, junctions are the only places where actual routing decisions are made. Therefore, packets should always be forwarded to a node on a junction rather than being forwarded across a junction.This is done in a greedy fashion: the neighboring node with the largest progress towards the destination is chosen. As a consequence, the repair strategy of GPCR consists of two parts: (1) on each junction it has to be decided which street the packet should follow next, and (2) in between junctions a special form of greedy forwarding is used to forward the packet towards the next .junction.

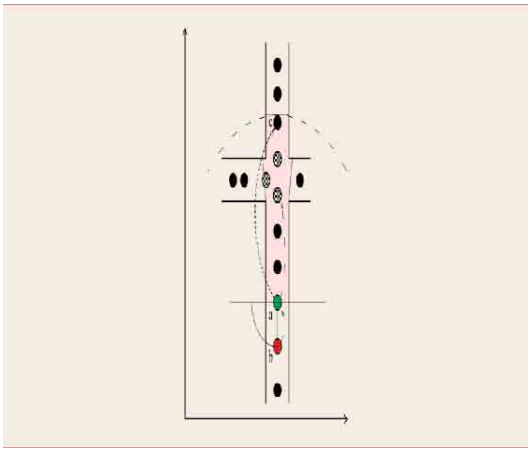


Fig 4. Routing procedures for GPCR

G. Greedy Traffic Aware Routing

GyTAR considers vehicle direction, vehicle velocity, multi-directional roads, and the changing traffic environment into its routing strategy. It consists of two modules: (1) Selection of the junctions through which a packet must pass to reach its destination, and (2) an improved greedy forwarding mechanism between two junctions. Hence, using GyTAR, a packet moves successively closer towards the destination along streets where there are enough vehicles to provide connectivity [13].

H. GVGrid

GVGrid [14] is an on-demand, position-based routing protocol that constructs a route from a source (a fixed node or a station) to vehicles that exist in a destination region. GVGrid is designed not for sparse regions with high-speed vehicles such as highways, but for dense regions with low-speed vehicles such as

cities. It also reconstructs the route when it is broken by the movement of vehicles. GVGrid divides the geographical area into uniform-size squares called grids.

I. Vehicle-Assisted Data Delivery

Vehicle-assisted data delivery (VADD) [15] is based on the idea of carry and forwarding. Different from existing carry and forwarding approaches, VADD uses predicable mobility, which is limited by the traffic pattern and road layout. Extensive experiments are used to evaluate the proposed data delivery protocols. Results show that the proposed VADD protocols outperform existing solutions in terms of packet delivery ratio, data packet delay, and protocol overhead. VADD has three packet modes: Intersection, StraightWay, and Destination.

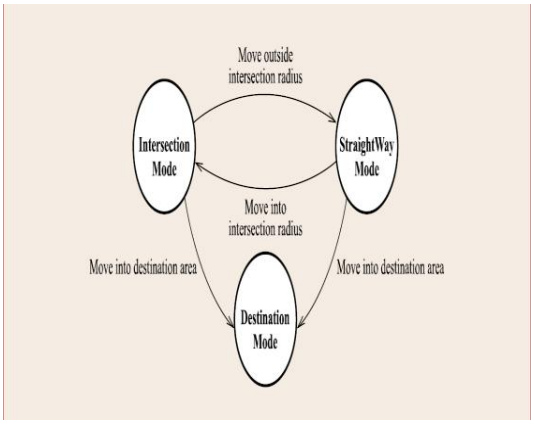


Fig 5. Three packet mode of VADD

J. Contention Based Forwarding

The contention-based forwarding (CBF) [16] algorithm is a greedy position-based forwarding algorithm that does not require the proactive transmission of beacon messages. In CBF, the next hop is selected through a distributed contention process based on the actual positions of all of the current neighbors. In this contention process, CBF makes use of biased timers. To avoid packet duplication, the first node that is selected suppresses the selection of further nodes using an area-based suppression algorithm.

K. Directional Greedy Routing Protocol

The Directional Greedy Routing Protocol (DGRP) [17] transmits data to moving nodes using the greedy forwarding and perimeter methods. However, unlike existing GSPR, DGRP takes into account the moving directions and velocities of nodes as well as the position data of 1-hop neighbors of the transmitting node. In DGRP, the position data of a node is acquired through periodic beacon messages, which predict moving velocities based on beacon message intervals and the moving distance of nodes as shown in Figure 6.

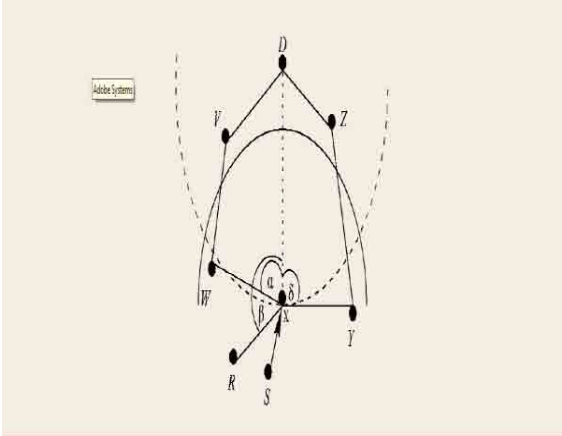


Fig 6. The predict procedures of DGRP

L. Greedy Perimeter Urban Routing

GPUR selects a relay node based on information about the road characteristics, which is similar to GPCR. However, unlike GPCR, GPUR selects a relay node from nodes with 2-hop neighbors to reduce the routing error problem and the probability of local maxima in urban areas.

M. Reliable Directional Greedy Routing

Reliable Directional Greedy Routing (RDGR) [19] is a reliable position-based greedy routing approach which uses the position, speed, direction of motion, and link stability of neighbors to select the most appropriate next forwarding node. In order to improve the DGR protocol and increase its reliability, the proposed strategy introduces some new metrics to avoid packet loss.

N. Grid-based Predictive Geographical Routing

Grid-based Predictive Geographical Routing (GPGR) [20] employs road segments based on a routing approach with street awareness, and it uses knowledge of the road topology provided by a static street map. Therefore, data packets are routed between vehicles, following the road topology and the road segments in reality. This method aims to improve the routing protocol for IVC based on

vehicle movement information such as position, direction, and velocity, paid with information on road topology. To do this, GPGR assumes that each vehicle knows its location by GPS, was with most related geographic routing protocols, and has a digital street map for road information. The geographic area of VANET is partitioned into a two-dimensional logical grid.

O. Reliability-Improving Position-based Routing

The Reliability-Improving Position-based Routing (RIPR) [37] algorithm consists of a greedy mode and perimeter mode, similar to GPSR. It also considers the road characteristics, as well as the node's position through the exchange of periodic beacon messages. Therefore, RIPR can solve the link breakage problem caused by selecting a stale node as the relay node, and reduce the local maximum caused by the road characteristics

I. Comparison of Greedy Routing Protocols

Table 1 is a qualitative comparison of the existing VANET routing protocols that use greedy forwarding approaches. We have classified greedy VANET routing protocols based on three sets of criteria: objectives, design approaches, and requirements.

	V2V	Geographic	Predictive	Carry-and-forward	Road-aware	Traffic-aware	Anchored routes	Map required	GPS required	Traffic data required
GPSR	✓	✓					✓		✓	
SAR	✓	✓		✓	✓		✓	✓	✓	
GSR	✓	✓			✓		✓	✓	✓	
A-STAR	✓	✓			✓	✓	✓	✓	✓	
STAR	✓	✓			✓	✓		✓	✓	
GPCR	✓	✓			✓		✓	✓	✓	
CBF	✓	✓			✓				✓	
GVGrid	✓	✓			✓			✓	✓	
GyTAR	✓	✓	✓	✓	✓	✓		✓	✓	✓
DGRP	✓	✓			✓				✓	
VADD	✓	✓			✓				✓	
GPUR	✓	✓			✓				✓	
RDGR	✓	✓			✓				✓	
GPGR	✓	✓	✓	✓	✓			✓	✓	
RIRP	✓	✓	✓		✓			✓	✓	

Table 1.Comparison of Greedy Routing Protocols

III CONCLUSION

In this paper, the existing greedy-based routing algorithms for VANETs is introduced, and the advantages and disadvantages of those routing protocols is analyzed. A timeline of greedy VANET routing protocol development and a qualitative comparison of their objectives, design approaches, and requirements is provided. All these approaches tend to focus on V2V and require GPS. They also utilize the absolute or relative locations of each node to predict the location of a relay vehicle and/or forward messages toward the next relay vehicle or a destination vehicle.

IV REFERENCES

[1] Jiang, X., Camp, T. (2002)," A Review of Geocasting Protocols for a Mobile Ad HocNetwork", Proceedings of the Grace Hopper Celebration (GHC), CONFERENCE.

[2]A. Boukerche, H. Oliveira, E. Nakamura, A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems", *Computer Communications*, vol. 31, no. 12, pp. 2838-2849, 2008.

[3] S.-H. Cha, K.-W.Lee, H.-S.Cho, "Grid-based predictive geographical routing for inter-vehicle communication in urban areas," *International Journal of Distributed Sensor Networks*, May 2012.

[4]Z. Li, Z. Wang, C. Chigan, "Security of vehicular ad hoc networks in intelligent transportation systems," *Wireless Technologies for Intelligent Transportation Systems*, Nova Science Publishers, 2009.

[5] Characteristics of VANETs, http://www.ece.mtu.edu/~zli1/index_files/Page764.htm.

[6]F. Li, Y. Wang, "Routing in vehicular

[7] B. Karp, H.T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. International Conference on Mobile Computing and Networking (MobiCom)*, pp. 243-254, 2000. Article (CrossRefLink

[8] C. Lochert, H. Hartenstein, J.Tian, H. Füßler, D. Hermann, M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *Proc. of the IEEE Intelligent Vehicles Symposium*, pp. 156-161, Jun 2003. Article (CrossRefLink)

[9] J. Bernsen, D. Manivannan, "Greedy routing protocols for vehicular ad hoc networks," in *Proc. of the 7th International Conference on Wireless Communications and Mobile Computing (IWCMC)*, pp. 632-637, Aug. 2008. Article (CrossRefLink)

[10] J. Tian, L. Han, K. Rothermel, C. Cseh, "Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks," in *Proc. of the IEEE Intelligent Transportation Systems*, pp. 1546-1551, Oct. 2003. Article (CrossRefLink)

[11] B.-C. Seet, G. Liu, B.-S.Lee, C.-F.Foh, K.-J. Wong, K.-K Lee, "A-STAR: A mobile ad hoc routing strategy for metropolis vehicular communications," in *Proc. of the 3rd International IFIP-TC6 Networking Conference (Networking)*, pp. 989-999, May 9-14, 2004. Article (CrossRefLink)

[12] F. Giudici, E. Pagani, "Spatial and traffic-aware routing (star) for vehicular systems," in *Proc. of International Conference on High Performance Computing and Communications*, pp. 77-86, Sep. 2005. Article (CrossRefLink)

[13] M. Jerbi, S.-M.Senouci, R. Meraihi, Y. Ghamri-Doudane. "An improved vehicular ad hoc routing protocol for city environments," in *Proc. of the IEEE International Conference on Communication (ICC)*, pp. 3972-3979, June 2007.

[14] W. Sun, H. Yamaguchi, K. Yukimasa, S. Kusumoto, "GVGrid: A QoS routing protocol for vehicular ad hoc networks," in *Proc. of the 14th IEEE International Workshop on Quality of Service (IWQoS)*, pp.130-139, June 2006. Article (CrossRefLink)

[15] J. Zhao, G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1910-1922, May 2008. Article (CrossRefLink)

[16] T. Li, Y. Li, J. Liao, "A contention-based routing protocol for vehicular ad hoc networks in city environments," in *Proc. of the 29th IEEE International Conference on Distributed Computing System Workshops (ICDCS)*, pp. 482-487, June 2009. Article (CrossRefLink)

[17] R. Kumar. S. V. Rao, "Directional greedy routing protocol (DGRP) in mobile ad-hoc networks," *in Proc. of IEEE Information Technology (ICIT 2008)*, pp. 183-188, Dec. 2008. Article (CrossRefLink)

[18]M.-W. Ryu, S.-H.Cha, K.-H. Cho, "A vehicle communication routing algorithm considering road characteristics and 2-hop neighbors in urban areas," The Journal of Korea Information and Communications Society, vol. 36, no. 5, pp. 464-470, May 2011.

[19]K.Prasanth, Dr. K. Duraiswamy, K.Jayasudha and Dr. C. Chandrasekar, "Improved Packet Forwarding Approach in Vehicular Ad hoc Networks using RDGR Algorithm," *International Journal of Next Generation Network (IJNGN)*, vol. 2, no. 1, Mar. 2010. Article (CrossRefLink)

[20] S.-H. Cha, K.-W. Lee, and H.-S. Cho, "Predictive Grid-Based Predictive Geographical Routing for Inter-Vehicle Communication in Urban Areas," *Hindawi International Journal of Distributed Sensor Networks*, vol. 2012, Mar. 2012. Article (CrossRefLink)

Content Distribution in VANETs Improved via Network Coding

Er. Navjot Kaur
M.Tech Scholar
Department of CSE
Amritsar College of Engineering and Technology
Email Id: kaur.navjot30590@gmail.com

Dr. Tanupreet Singh
Professor and Head of Department
Dept of ECE
Amritsar College of Engineering and Technology
Email Id: tanupreet.singh@gmail.com

Abstract*—Vehicular Ad hoc Network (VANETS) is a kind of wireless ad hoc networks that allows vehicles to communicate with each other. In the recent era it is growing with its popularity. Vehicular communication is an open medium for transmitting the data. Because of the open medium VANETs can face the problem of safety transmitting the content. For this reason content distribution to vehicles has become a challenge. Content distribution allows the content to be transmitted safety between the vehicles and between vehicle and AP i.e. V2V and V2I. The paper presents various protocols for content distribution in Vehicular Ad hoc Networks. It also states the challenges, issues and attacks associated them. It also outlines that how content is distributed in Car Torrent and by Network Coding. The paper says that Network coding helps to improve the performance of the system and it also optimize the VANET flow.

Keywords: **- Car Torrent, LTE (Long Term Evolution), Network Coding, VANETS, V-Torrent.**

I. INTRODUCTION

In the recent era navigation safety has become the main driver. With the increasing demand and popularity of mobile application, new interest has emerged that is related to Vehicular Ad hoc Networks. VANETs are usually the moving of smart vehicles in the network. It takes the moving cars as nodes in order to create a mobile network. The participating cars can act as a wireless router or nodes. These participating cars can provide communication between the vehicles or between the vehicles and the Access point. The connection between the cars is possible approximately up to 100 to 300 meters. When these nodes fall out of the range then a drop out in a network occurs [1].

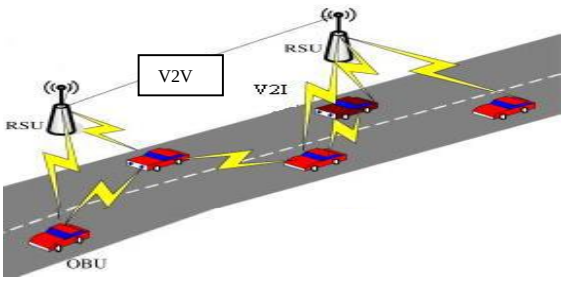


Figure 1: Structure of VANETs [3]

In VANETs, mobile network can be created when other vehicles can join each other in order to transmit the content. The connectivity between the vehicles can be provided by Wi-Fi, Bluetooth or other mobile protocols such as Bit Torrent, Car Torrent, and Network Coding [1].

One of the emerging and challenging areas in VANETs is content distribution in Vehicular Ad hoc Networks. Content Distribution allows the safe navigation of the music, videos, games, movies among the vehicles and the AP. Example for it may be downloading of the video camera stream of the vehicles facing an accident or the road emergency (flood, fire, earthquake etc). Mobile users are able to download the content from the internet by using the concept of War driving i.e., searching for a Wi-Fi wireless network [2].

In the rest of the paper we have discussed about the protocols of content distribution in section II. Section III covers the content distribution via VANET Torrent in which we have talked about the LTE (Long Term Evolution) and Wi-Fi channels. Section IV covers the content distribution via Car Torrent which is explained with the help of Wi-Fi connection. Section V contains the network coding that helps in improving the performance of the network. Moreover it also optimizes the V-Torrent, and improves the security of the network. Section VI contains conclusion. And at last section VII contain the future scope.

II. PROTOCOLS OF CONTENT DISTRIBUTION

In real world environment it is unrealistic to have a friendly Wi-Fi connection at the open intervals. In Order to provide solution to it we have peer-to-peer "file swarming" that allows the mobile users to share their multimedia content. An example to this is Bit Torrent. In it the file is segmented into chunks. These chunks are distributed among the mobile nodes according to their requirement. By doing so the work of the content provider is reduced and also increases the speed of downloading [2].

An extension to the above protocol is the Car Torrent [11, 12]. It is also a peer to peer "File Swarming" protocol. Car Torrent uses the k- hop gossip messages that are distributed across a limited range. All the peers can collect information from the sender. For Example R desires a piece that P and Q

have. So the node R will get the piece from the node which has shortest distance to the R.

Further extension of the above is Code Torrent [11]. Here the encoding is done at the source and the intermediate nodes before transmitting the file. At the receiver end the piece of chunk is decoded. If the receiver fails to decode it, then the piece is recovered by Network coding [2].

In the modern era, every individual is interested in accessing the data from any node at any time according to their application requirement. So this is leading to the depletion of the traditional routing mechanism. In the recent years ICN (Information Centric Network) has introduced a new routing scheme i.e., Geo Routing. A Geo Routing scheme comprises the features of scalability, mobility, flexibility and robustness. A vehicle can quickly and efficiently acquire a multimedia stream with the help of the Information Centric Network [2]. ICN can receive the content much faster than the Car Torrent and Code Torrent [2].

III.CONTENT DISTRIBUTION VIA VANET TORRENT

Vehicular Ah hoc Networks provide the connectivity between the wireless devices either through Wi-Fi or LTE (long Term Evolution. LTE usually provide the point to point connection between the moving nodes. On the other hand Wi-Fi is short lived. Downloading in Wi-Fi is done with the help of UDP and downloading in LTE is done with the help of TCP. Therefore LTE provides better performance. But as it is Long Term Evolution therefore it can be lossy and noisy. The solution to it will be Network Coding, which improves the quality of connection and makes it lossless [2].

Moreover LTE connection is expensive and is limited up to a distance i.e., it allows only some mobile nodes to connect. On the other hand Wi-Fi has no cost. In some cases Wi-Fi connection is not available, so in that case the only choice we have is the LTE. LTE channel also provide solution to the mobile users when the Wi-Fi channel is overloaded. A mobile user can have access from both the channels. But it is usually seen that usually LTE channel suffers because of the obstacles that may be due to noise, wind, rain etc [2].

The other issues are security, privacy and energy consumption. LTE channel is more secured from the attacks than the Wi-Fi connection. Mobile users that require privacy while downloading will prefer the LTE channel. LTE channel consumes more energy than the Wi-Fi channel [2]

Another issue is the mobility and the channel connectivity which can confuse the network .Therefore it needs to be protected via a network coding. At last we can say that there is an issue of getting the content. Content can be transferred among the logical peers who are in actual the physical peers. The peers that are accessing the data must have some interest for the content. The multimedia content is usually transmitted between the peers of interest [2].

III. CONTENT DISTRIBUTION VIA CAR TORRENT

Car discovery in Car Torrent is done by passing gossip messages. Car Torrent is like a co operative content distribution. A car entering the highway can request for a file with specific name from Wi-Fi. Then the Wi-Fi responds to that file by sending the multiple chunks. More it also provide the requested car the multiple request for the same file. The moving nodes generate the gossip messages from time to time so that the other cars can connect accordingly. This type of gossip mechanism allows peers to communicate and cooperates with each other [2].

Now let us explain this by taking an example. Suppose a new node X transmit the gossip message along with the list of chunks. The intermediate nodes help in transmitting this gossip message to the other nodes. Now Y receives the gossip and responds to the first chunk and sends it to X. Node X sees the response and send the chunks until all are receives by Y. By initializing all these things we can say that it is a kind of send-wait protocol [2, 5].

Gossiping also provide some advantages to content distribution in vehicular ad hoc networks. It enhances the working of VANETs by providing the connectivity between the nodes through send and wait process. The problem that could occur in it is the delay. Delays are not tolerable in real world [2].

Consider an example of the soccer game. Assume that the mobile node want to have access to the soccer video stream. He tries to download from the Wi-Fi AP. If the Wi-Fi connection is not present in that range, then he tries to connect with other vehicles. The moment the other vehicles are also not able to respond to the request then the mobile node can choose the LTE channel. ICN reduces the cost, delay time of the video stream. ICN can be named as: content centric network, Named Data Network [2, 6].

The experimental results of Mario Gerla et all [2] has shown the implementation of Car Torrent and also evaluated the performance of the Car torrent by taking the two scenarios. They have also shown that how the various peer recognize each other presence and connect with each other. They have also outlined the piece selection strategy for downloading the files from one and other.

In the first scenario, two cars share their files by using two laptops. In the other scenario the files are accessed and downloaded from the Wi-Fi connection and between the vehicles. These can be said as the parking lot scenario and the moving scenario. Each and every vehicle has the wireless interface card for the vehicle to vehicle communication and for vehicle to infrastructure communication. As the vehicle approaches the access point, the moving node sends a gossip request. The AP then responds to the requested chunk of the moving vehicles. In order to avoid the interference the two cards are set to channel 1 and channel 11.in the moving scenario the good put is lower than the parking lot as there is interference from other vehicles

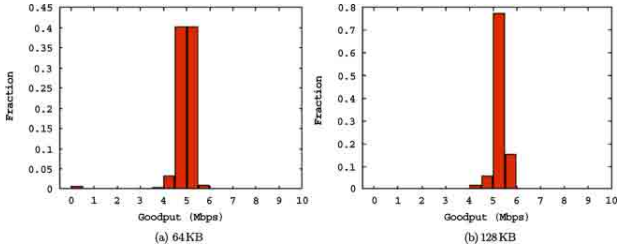


Figure 2: Scenario of parking lot [2]

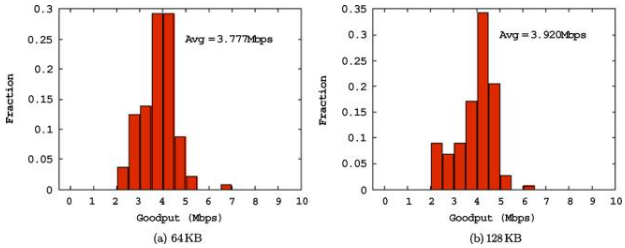


Figure 3: Scenario of moving vehicles [2]

IV. IMPROVED PERFORMANCE BY NETWORK CODING

Network coding is used to improve the performance in both the connections i.e., the Wi-Fi connection and the LTE connection. It usually increases the network performance. Network coding is used to encode the chunks and inject them into the networks. The interested nodes after receiving the chunks can decode them as per their requirement. Even a single invalid chunk can corrupt the message, which in turn leads to the reconstruction of the original message. For this several secured Network Coding mechanism have been introduced [7, 8].

Now the question is what is secured network. A secured network coding verifies the validity of the encoded message. The mechanism used for it is cryptography, which uses the homomorphism signatures and the hash function [7-10]. Zhao et al. introduce a coding block authentication method by computing orthogonal vectors of each coded block [11].Gennaro et al .propose an RSA based homomorphic signatures scheme and a homomorphic hashing scheme for network coding over integers [7].

The problem of "coupon collection" that occurs in the car torrent is erased by the Network coding. This is shown in the fig 4. Here the downloading time of the Car Torrent and code Torrent is shown [2].

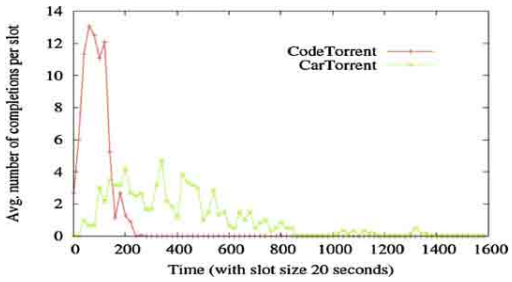


Figure 4: Comparison between Car Torrent and Code Torrent[2]

Network coding not only improves the performance and throughput. But also helps to do some extra work such by the forwarding. The forwarders can forward the packet without encoding them in order to reduce the overheads in the network. When the forwarders act so the then they are known as selfish forwarders. These selfish nodes forward the packets in a secure manner[2] .The social norm can be explained in it by using the distributed game playing, that consist of reward and punishment based on the node behavior.

As shown in Table1, there are two players in a one-shot NC forwarding game: the intermediate node R (the selfish forwarder) and the source–destination pair (S-D). Node R can choose to perform: secure network coding and forwarding (NCF); simple forwarding without network coding (F) or; total packet drop (Drop). The S–D pair receives a benefit of *B* for delivering each packet, and the relay node R has a cost of c1 for encoding each packet and c2 for forwarding each packet. Here p is the packet loss rate on the lossy link between R and D. obviously the one-shot NC forwarding game has Nash Equilibrium of "Drop", i.e. no player has a benefit. However if the role is altered between the relay node and the sender-destination then the relay node can perform the NCF [2].

	Intermediate node R		
	NCF	F	Drop
S-D pair	B,-(c1+c2)(1-p)	B(1-p),-c	0,0

Table1: One –Shot Forwarding game [2]

Therefore we can say that social norm can be applied on VANET Torrent or V-torrent to optimize its performance.

V. CONCLUSION

This paper clearly discussed the various protocols and technologies to be used for Content Distribution in vehicular Ad hoc Networks. We have also outlined that how the various mobile nodes interact with each other through the Wi-Fi and the LTE connections. Our discussion is also based up on the various issues, challenges and the solution for content pulling in a network. We have also addressed the Car Torrent and Network Coding protocol. It was seen that the Network Coding can optimize the performance of the VANETS. However network coding also helps in making the network secure and pollution free.

VI. FUTURE SCOPE

As we have seen that the network coding in the intermediate node causes the pollution issues. These issues can be solved by homomorphic signatures and the cache coding. Cache coding concept can play an important role in future for the Vehicular Ad Hoc Networks. Cache coding can help to cache the content at the intermediate nodes so that it can be used in the future. Moreover cache coding should be able to maintain the integrity of the network.

REFERENCES

[1] S. Selvakanmani, A.V Kalpana, S. Nalini, "Implementation of Video Streaming in Urban VANETs" International Journal of Computer Applications & Information Technology, Vol. I, Issue III, pp.(2278-7720), 2012

[2] Mario Gerla, Chuchu Wu,Giovanni Pau,Xiaoqing Zhu, " Content distribution in VANETs" ,pp.(3-12), 2014

[3] Chirag Suryakant Thaker, Ati Shirishkumar garg , Nashifa Mohmadshafi, "Securing Peer to Peer Content Distribution Network based on Network Coding in VANETs", International Journal of Computer Applications ,Volume 66– No.4, pp (0975 – 8887) ,2013

[4]U.Lee, J.-S.Park, J.Yeh, G.Pau, M.Gerla, "Code torrent: content distribution using network coding in VANET", pp.(1–5), 2006,

[5]K.Lee, S.-H.Lee, R.Cheung, U.Lee, M.Gerla , First experience with Car Torrent in a real vehicular adhoc network testbed", pp.(109–114),2007.

[6]V.Jacobson, D.K.Smetters, J.D.Thornton, M.F.Plass, N.H.Briggs, R.L.Braynard, "Networking named content", pp.(1–12), 2009.

[7]R.Gennaro, J.Katz, H.Krawczyk, T.Rabin, "Secure network coding over the integers", in: Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography , pp.(142–160), 2010

[8]D.Boneh, D.Freeman, J.Katz, B.Waters, "Signing a linear subspace: Signature schemes for network coding" ,2009.

[9]D.Charles, K.Jain, K.Lauter, "Signatures for network coding", pp.3–14, 2009

[10]R.Johnson, D.Molnar, D.Song, D.Wagner, "Homomorphic signature schemes", 2002.

[11]F.Zhao, T.Kalker, M.Medard, K.Han, "Signatures for content distribution with network coding", IEEE International Symposium on Information Theory, pp.(556–560), 2007.

[12]S.Das, A.Nandan, G.Pau , Spawn : "swarming protocol for vehicular ad-hoc wireless networks" ,pp.(93–94), 2004

[13]A.Klemm, C.Lindemann, O.Waldhorst, "A special-purpose peer-to-peer file sharing system for mobile ad hoc networks , "IEEE 58th , Vehicular Technol-ogy Conference, vol.4, pp.(2758–2763), 2003,

A REVIEW ON CROSS LAYER BASED CONGESTION CONTROL SCHEMES IN MANET

Er. Ramandeep Kaur
M.Tech Scholar,
Dept of Computer Science & Engineering,
Amritsar College of Engineering and
Technology (Manawala)
Email Id- Ramandeephundal1990@gmail.com

Manmeet Kaur
Assistant Professor
Dept. of MCA
A.C.E.T. Amritsar
mink_manu@yahoo.com

Abstract— Mobile Ad Hoc network made up of wireless nodes that organize a communication network without centralized infrastructure, Cross layer allows interaction among various layers which helps in enhancing the network performance. In MANET due to mobility of nodes, packets may be lost because of two reasons, Link failure and congestion. Link failure caused by the dynamic nature of network Congestion occurs when the resources are limited and packets are dropped during transmission. Retransmission of packets result in network overload as the resources are overburdened and more energy is consumed and the network is congested. There are number of techniques available to handle congestion in cross layers. In this paper these congestion control schemes are reviewed. Two techniques- congestion triggering mechanism and energy efficient congestion control scheme are discussed.

***Index Terms*: MANET, Cross Layer, Congestion Control, Energy Efficient, Packet Loss, Retransmission.**

I. INTRODUCTION TO MANETs

Mobile Ad hoc network (MANET) is made up of wireless nodes that develop a network without support of any kind of infrastructure that are capable of communicating with each other. Mobile Ad Hoc network is an emerging research area with practical applications [1].Due to mobility of nodes changes in topology can occur or may be breakdown of node due to loss of energy. It causes packet losses in the network. Packet loss occurs when the link breaks or buffer is full which results in congestion.

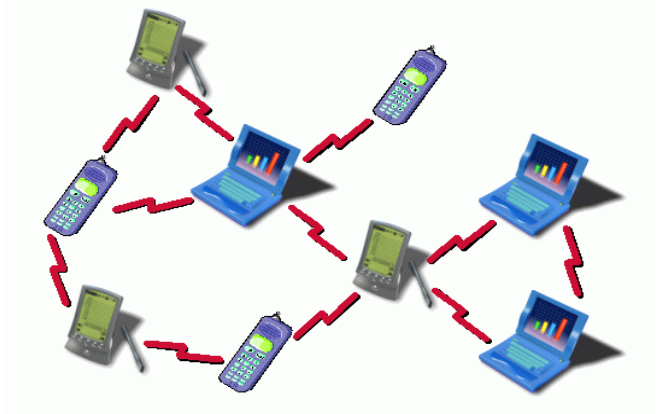


Fig1. MANET [2]

A. CHARACTERISTICS OF MANET

Following are some characteristics of MANET [2]:

Infrastructure-less and Autonomous: MANET does not depend on any infrastructure or centralized administration. Every node acts as an independent router and generates independent data.

Multi-hop routing: Default router is not available; each node performs as a router and forwards each other's packets to enable information sharing between mobile hosts.

Dynamic topologies: In MANET, due to mobility of nodes, the multi hop network topology which can change frequently and unpredictably and results in change of route, network partitions, and the packet losses.

Variation in link and node capabilities: Variation in node radio capabilities can result in asymmetric links. Every mobile node might have a different configuration of software and hardware which results in variability in processing capabilities.

II. CROSS LAYER CONCEPT

Cross layer is the violation of OSI/TCP layered model. Cross layer allows the communication and interaction between various layers which is not possible in OSI/TCP model. By enabling sharing of information between different layers helps in optimizing network performance. If changes made in one layer such as at physical layer, transmission rate varies, nodes or links connected to the physical layer also need changes which is possible with the help of interaction between layers. Cross layered design is

- maintaining the functionalities that are associated to the original layers
- allowing co ordination, and interaction of protocols between layers.

There are many existing methods which represent how to exchange information among layers. Following are some methods [11]

1. *Interlayer signaling pipe*: In Interlayer signaling pipe, a signaling pipe is linked with layers to provide communication.
2. *Direct Interlayer Communication*: Direct Interlayer Communication allows non-neighboring layers of stack to exchange information.
3. *Central Cross-Layer Plane*: In Central Cross-layer Plane method, a database is present which is accessed by layers.
4. *Network Wide Cross Layer Signaling*: Network wide cross layer signaling deals with information gathered at different protocol layers of distributed network nodes.

For network resources, The Physical layer, Data link layer (MAC layer) , routing layer are combined. Transmission power and data rate is decided at physical layer which influence MAC and routing decisions. Scheduling and allocating channels is the task of MAC layer. Choice of route through which data travels is made by routing layer [3].

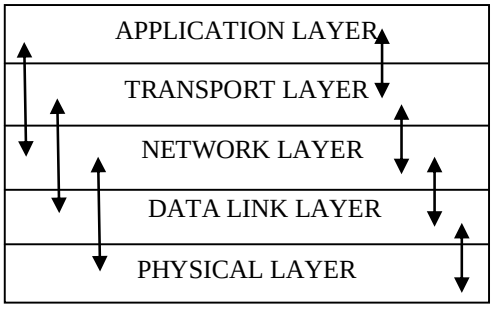


Fig 2.Cross layer design- Information sharing[3]

Fig2.represent the cross layer design in which information sharing among different layers takes place.

A.CROSS LAYER BASED CONGESTION CONTROL

Congestion control is one of the issue in MANET. To control the incoming traffic into a network is the congestion control mechanism. Sending a reduced packet rate at the sender node may be one of the solution to control congestion. Transmission control protocol joins the congestion control with dependability to perform congestion control in the absence of feedback about congestion position. There are Techniques to control congestion which are: Flow control , network congestion control, congestion avoidance , resource allotment and congestion control algorithm which is used in TCP named Additive increase and Multiplicative decrease (AIMD)[3].Congestion can cause the following:

Increased delay: Detecting the congestion in network leads to increased delay. In critical situation finding a new alternate congestion free route also cause delay.

More overhead: The processing and communication effort needed to establish new congestion free route and in multipath routing more overhead for maintaining multiple paths

High Packet losses: During the period of detection of congestion, Packets may be lost. Congestion control techniques reduce the network traffic which can be result in packet losses [3].

B.TCP BASED FLOW CONTROL AND CONGESTION CONTROL

TCP protocol is window based flow and congestion control protocol that is used to maintain transmission of data by using sliding window techniques .The purpose of scheme is to assure that the sender must level its transmission rate to fulfill their own and receiver's needs. The TCP sender can determine the number of packets it can send into the network prior to receive an Acknowledgement. A Variable denoting window varies over time to limit the connection's sending rate.

The flow control and the congestion control both are the two different techniques that regulates the sending rate of a TCP connection. Two techniques are similar as both try to avoid connection from sending data at the increased rate.

To prevent a TCP sender from overflowing the receiver's buffer , flow control is needed. In each ACK transmitted, the Receiver advertises a window limit to the sender. The window is called as receiver advertised window (rwin). Controlling the Congestion is related with traffic inside the network, purpose is to avoid failure inside the network.TCP sender uses limiting window named congestion window (cwnd).If the network is large then degradation is expected to be high. Due to reason Wireless networks are of lossy nature, there may be loss because of its medium and link interruption as the nodes are moving [4].

III. RELATED WORK

Jin Ye et al. [7] the author proposed an enhanced TCP with cross layer congestion notification over Wired-wireless hybrid networks. Being differentiated from the existing TCP protocols, the congestion of channel competition in MAC layer. The model is built on the ECN scheme, which had proven to be effective on congestion control and widely supported in number of situations. The model is having better feasibility and scalability. In future, the work will be based on other congestion metrics in MAC layer and how explicitly notify TCP sender, by which the proposed TCP model can be applied into other congestion control schemes.

Daniel Scofield et al. [8] designed HxH, a hop-by-hop transport protocol that uses credit-based congestion control and reverse ACKs to solve the problem with TCP. The problems include contention, interference, the hidden and exposed terminal problems, shared queues, half-duplex links, and route changes due to mobility. Credit-based congestion control reacts immediately whenever network conditions change, and can refine fairness among flows competing on the same path. The weakness of the proposed approach is that, congestion control algorithms that use rate-based and pricing based feedback is not used.

S.Sheeja, Dr.Ramachandra V Pujeri "Efficient Energy Based Congestion Control Scheme for Mobile Ad hoc Networks" [6]. In this paper Efficient Energy based Congestion Control Scheme (EECCS) technique was proposed for improving energy efficiency of mobile nodes. It helps in avoiding congestion and to increase network lifetime. Probability of retransmission of packet reduced in this scheme. For providing minimum energy consumption, Energy consumption model is needed and to avoid congestion Multipath routing scheme is used. By using the extensive simulation results, the proposed scheme EECCS attains the better packet delivery ratio, High network lifetime, low delay and overhead, minimum energy consumption.

Imran Chowdhury et.al [9],the author proposed an energy efficient and cooperative congestion control protocol (EECCCP) for cooperative multicasting in mobile ad hoc networks. It overcomes the weaknesses of existing multicast congestion control protocols like AODV and EERCCP. In the first phase it builds a cooperative multicast tree rooted at the

source, by including the nodes with higher residual energy towards the receivers. In the second phase an admission control scheme in which a cooperative multicast flow is admitted or rejected relying upon on the output queue size. Finally tests shows either the relay node has the potential path to the required destination, if not then choose another node which has the second highest residual energy as a new relay node.

K.Srinivas and A.A. Chari proposed [10] Energy Efficient Cross Layered Congestion Detection and Control Routing Protocol also referred as ECDC. The proposed model focused to deliver an energy efficient mechanism to quantify the degree of congestion at victim node with maximal accuracy. The model involves controlling of congestion in two steps: first is to control congestion with effective energy efficient congestion detection and next is optimal utilization of resources. Packet loss in network routing occurs due to link failure and congestion. Many existing congestion control solutions do not have the ability to distinguish between packet loss is either of link failure or packet loss due to congestion.

Suryaprakash Reddy et.al [12] proposed the routing algorithm Energy efficient Ordered Congestion Control using Cross layer support , it is refined the OCC to gain the ability of energy conservation in congestion discovery. In this effort it attempts to limit the role of MAC layer to detect link failure and developed a new strategy to detect the congestion at a relay node level and path level.

S.Sheeja and Ramachandra.V.Pujeri [13], As congestion causes packet loss so to avoid congestion Cross layer based Congestion Control Scheme was proposed. This scheme reduces the packet loss in the network. In the scheme there are four phases: In first phase, cross layer design is considered to share information, in second congestion detection scheme is explored , third is congestion control phase and in last phase new packet format proposed. By simulation the scheme achieves better throughput, congestion ratio, packet delivery ratio , end to end delay and less overhead.

S.Sheeja and Ramachandra.V.Pujeri, [14] & [15], the congestion avoidance scheme and efficient security scheme is proposed using cross layer approach. The congestion free routing is established to reduce the highest packet loss in this approach.

D.Sunitha , A.Nagaraju , G.Narsimha [16] , In this paper, A cross-layer based approach for improving TCP performance in Multihop Mobile Ad hoc Networks (MANETs) is proposed. The proposed congestion triggering mechanism triggers congestion whenever the channel occupied ratio (COR) reaches a maximum threshold value and the received signal strength is less than minimum threshold value.

IV.CROSS LAYER CONGESTION CONTROL TECHNIQUES REVIEWED

1) CONGESTION TRIGGERING MECHANISM [16]

A. *OVERVIEW AND METRICS*

Congestion triggering mechanism triggers congestion according to two situations: one is when the channel occupied ratio (COR) reaches a maximum threshold value and the received signal strength (RSS) is less than a minimum threshold value. Congestion control scheme controls the rate of data sending of the sender by considering available bandwidth, delay of its link and COR. Following are Metrics used in mechanism:

i) COR (CHANNEL OCCUPIED RATIO): The channel is said to be busy or engaged when it is either sending data or receiving data. Busy channel is represented by its network allocation vector (NAV). COR provides the early signal of congestion. COR is given by ratio of total lengths of busy periods to the total time during time interval t_n. T is Total transmission time and T_B is total length of busy periods. The COR can be written as

$$COR=T_B/T \quad \ldots\ldots\ldots (1)$$

By considering channel utilization factor, threshold value (Th_{COR}) can be determined .It is selected as:

$$COR \sim Uc\ (\ COR <= Th_{COR}\ ) \ldots..(2)$$

Where Uc is the utilization factor which is the measure of ratio of channel busyness time for successful transmissions to the total time T.

ii) RECEIVED SIGNAL STRENGTH ESTIMATION

The received signal strength (Rs) is given as

$$Rs = P_{res}\, d\hat{}\, b \quad \ldots\ldots\ldots\ldots (3)$$

Where, P_{res} is the reception power at a reference distance and it is of one meter. b is the distance-power gradient value that differs with the surrounding terrain conditions.

iii*) AVAILABIE BANDWIDTH ASSESSMENT*

Suppose BW_T is the total bandwidth and BW_A is the available bandwidth, then in term of Th_{COR} and COR, the available bandwidth of a node is calculated as,

$$BW_A = \begin{cases} BW_T\,(Th_{COR}\text{-}COR)Data/AvgTs, & when(COR<Th_{COR}) \\ 0, & when COR>= Th_{COR} \end{cases} \quad \ldots\ldots\ldots\ldots (4)$$

Data represents the average payload size and Avg Ts denotes the average successful transmission time at the MAC layer.

iv*) DELAY CALCULATION*

The time interval between data transmission and reception is said to be the delay of link (L_i). Consider T_D as the time of data transmission and T_R as the time of data reception, then the delay incurred in link Li can be given as,

$$Delay\ (Li) = T_D - T_R \ldots\ldots\ldots (5)$$

B.CONGESTION TRIGGERING MECHANISM

Various types of data losses that occurs due to link failures, attacks etc. This mechanism consider two parameters: RS (received signal strength) and COR(Channel Occupied Ratio). Each node calculates Rs and COR using equations given in (3) and (1) respectively. Congestion Triggering scheme is incorporated in each node of the network to monitor the Network. Take Th_{COR} as the threshold value of COR and

minThRs as the threshold of minimum received signal strength value. Suppose that each node periodically calculates COR and Rs. The calculated values are compared with ThCOR and minThRs respectively. When the calculated COR reaches ThcOR or the received signal strength goes below minThR congestion notification message triggers. The congestion notification message is transmitted to the source via a flag named as Con-notify flag. While receiving Con-notify flag, the source starts mechanism to control rate. Congestion triggering scheme is traced in the following algorithm,

Algorithm

Let Th $_{COR}$ be the maximum threshold value of COR
Consider min Th $_{Rs}$ as the threshold of minimum received signal strength value.
Assume n1, n2, ... N as a set of mobile nodes in the network
Node ni calculates COR using equation (1)
Node ni calculates Rs using equation (3)
COR and Rs values are compared with their threshold values
>$_{=}$if (COR Th $_{COR}$ && Rs < minTh $_{Rs}$) then
Data loss is triggered by congestion ni transmits Con-notify flag to the source node
End if

In Fig3 . there is a network of nine nodes, the source sends data to the destination through nodes 4-6-7.

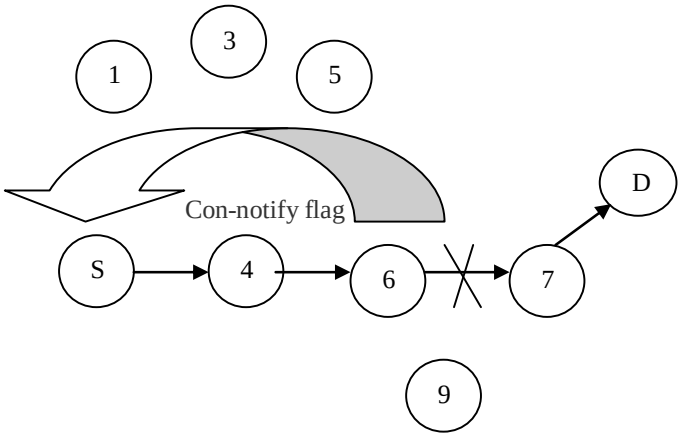


Fig3.Congestion triggering mechanism [16]

While transmission of data between nodes 6 and 7values of COR and Rs is calculated and at node 6 the estimated COR value exceeds threshold value, Rs is less than minimum threshold value. Node 6 frequently sends the Con-Notify Flag to the source node.

C.CONGESTION CONTROL SCHEMES

S and D are source and destination nodes respectively .When the source sends data to destination, source forward first packet to an intermediate node($I_{1)}$, node receives packet the data link layer of node I_1 measures delay for its link , bandwidth and channel busyness ratio. This information is given to MAC header and then forward to next intermediate node I_2.This node perform the same task and update information in the MAC header. when the packet reaches to the destination D, The MAC header carries information about bandwidth, delay and COR of all the links along the path. D node forward this information along with acknowledgement to the S node. Source node use this information in adjusting its traffic sending rate. Fig4 .shows this congestion control technique.

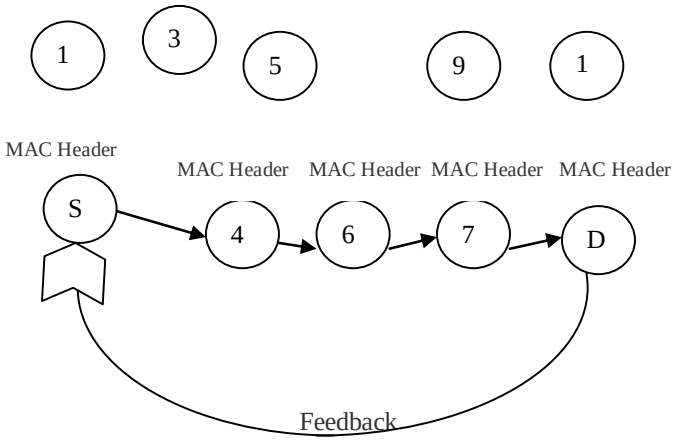


Fig4.Congestion control Technique [16]

D.FAIR RESOURCE ALLOCATION SCHEME

Channel resource (CR) can be expressed as:

$$CR = ((Th_{COR} - COR)/COR) * L_T$$

Where L_T is current traffic load which is the sum of incoming and outgoing traffic.

To get efficiency in transmission and fairness in resource allocation, the proposed resource allocation scheme utilizes AIMD along with COR and CR. When CR>0 flow increase rate of data sending, CR<0 flow decrease data sending rate.

2) ENERGY EFFICIENT BASED CONGESTION CONTROL SCHEME [6]

This scheme helps to avoid the retransmission and packet drop and to maximize network lifetime. .It is implemented with the help of three phases. In first phase, multipath routing is deployed to minimize effect of packet loss, packet drops and to gain load balancing .In second phase energy consumption model is combined in the cross layer model to achieve minimum energy consumption. In third phase packet format of this proposed scheme is examined to supervise the status of the congestion level, energy level and packet loss level . The flowchart of this scheme is represented in Fig5.

A. MULTIPATH ROUTING BASED ON CROSS LAYER APPROACH

For network resources, physical layer, Media access layer and routing layers gathered. At physical layer, transmission power and data rate is decided which impact MAC and routing decision.MAC layer handle the task of scheduling and allocating the wireless channel. Routing layer select the route to transmit the data packets to the destination node. In fig6 multipath concept is shown between source and destination node. Suppose the packet is transmitted through first path, if the capacity of path exceed then the packet drop occurs. so in

this situation the multipath is recommended to reduce the effect of congestion. the alternate links and nodes are combined for transmission of packet to the destination.

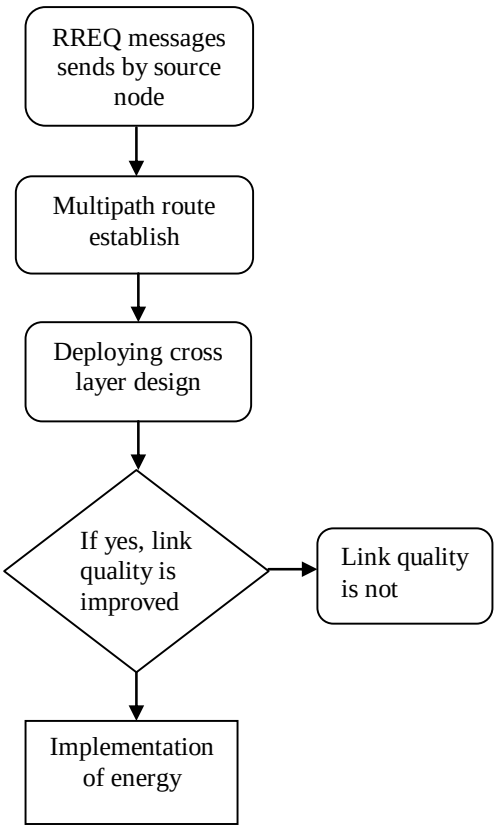


Fig 5.Flowchat of EECCS scheme [6]

The flowchart represent working of this scheme .the multipath routing is shown in Fig6

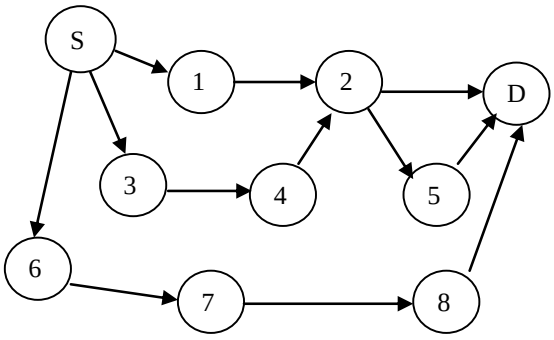


Fig 6.Implementation of multipath routing

In fig6.S is the source node and D is the destination node. S transmit data through node 1 and 2 to the D node, .if there Is congestion between this path then the source node can follow the alternate path of node 3,4,5 OR 6,7,8 node.

B.ENERGY CONSUMPTION MODEL

Due to mobility, mobile nodes consumes more energy. To monitor the energy Consumption to be at minimum level, the probability of packet retransmission should be reduced. Energy consumption model is implemented in [6].Position of nodes may be of three states like transmission, reception and idle. Every state represents different energy levels in energy consumption model.

C.PACKET FORMAT OF EECCS SCHEME

Source ID 2	Destination Id 2	Hop count 1	Energy level 4	Packet loss ratio 4	FCS 2

Fig 7.Packet format

In Fig7.the packet format proposed for EECCS scheme shows source and destination Id are of 2 bytes ,Hop count represent the number of n connected to particular node the energy level shows whether the retransmission of packets takes place with high energy consumption. Packet loss ratio is considered during information sharing phase.FCS(Frame check sequence) Is for error correction and detection .it is of 2 bytes.

V.HIGHLIGHTS OF DISCUSSED SCHEMES

SCHEMES	CONGESTION TRIGGERING MECHANISM	EFFICIENT ENRGY BASED CONGESTION CONTROL SCHEME
Simulator used	NS-2	NS-2
Protocol used	AODV	DSR
Performance metric	1.Packet delivery ratio 2.Average end to end delay 3.Throughput 4.Packet drop	1.Control overhead 2.End-to end delay 3.Packet delivery ratio 4.Packet loss ratio 5.Energy consumption level 6.Network lifetime

Fig8.Highlights of both schemes

Performance metrics used in schemes are [6] ,[16]:

Packet delivery ratio is defined as the ratio of total number of packets received at the destination successfully over the total number of packets transrnitted

.

Average end-to-end delay is averaged delay over all surviving data packets from the sources to the destinations.

Throughput is the total bandwidth received at the destination. It is measured in Mb/sec.

Packet Drop is the average number of packets that are dropped in the destination.

Control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Packet Loss Ratio is the ratio of occurrence of packet lost to the total number of packets used in the network during one transmission phase is defined as packet loss rate.

Energy consumption level maintains the energy level of node which is spent for sending and receiving a data to the total energy spent on the network.

Network Lifetime shows the lifetime of the nodes for the energy spent on route maintenance phase.

VI.**CONCLUSION**

In this paper, cross layer based congestion control techniques are discussed. A cross layer based approach for enhancing TCP performance in Multi hop Mobile Ad hoc network. Congestion control is to control incoming traffic into a network. The congestion triggering mechanism studied which triggers congestion by taking some parameters, when channel occupied ratio reaches maximum threshold value and received signal strength is less than minimum threshold value then a congestion notification message is transmitted to the source which initiate rate control mechanism. Efficient energy congestion control scheme avoids congestion and it improves energy efficiency of mobile nodes. Probability of retransmission of packet is reduced with the help of multipath routing. To acquire minimum energy consumption, energy consumption model is used and the packet format of this scheme monitors the status of congestion level, energy level and packet loss level. Two schemes are different as one triggers congestion and another try to avoid congestion.

VII. FUTURE SCOPE

There are number of techniques present to control the congestion in cross layer approach. New technique can be proposed in the Future. Congestion triggering mechanism can also work on another protocols like Pro active, Reactive and Hybrid routing protocol.

REFERENCES

[1] PROF.D.N.REWADKAR, SMITA KARVE "SPONTANEOUS WIRELESS AD HOC NETWORKING: A REVIEW" ININTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, VOLUME 3, ISSUE 11, NOVEMBER 2013

[2] Mahima Chitkara, Mohd. Waseem Ahmad "Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols" IJCSMC, Vol. 3, Issue. 2, February 2014, pg.432 – 437.

[3] S.Sheeja ,Ramachandra V.Pujeri " Cross Layer based Congestion Control Scheme for Mobile Ad hoc Networks" in International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013

[4] D. Sunitha, A.. Nagaraju and G. Narsimha "A Cross-Layer Approach for Congestion Control in Multi Hop Mobile AdHoc Networks" lnternational Conference оп Computing for Sustainable Global Development 2014

[5] Vorgelegt yon , Ruy de Oliveira and von Brasilien "Addressing the Challenges for TCP over Multihop Wireless Networks"

[6] S.Sheeja, Dr.Ramachandra V Pujeri "Efficient Energy Based Congestion Control Scheme For Mobile Ad hoc Networks" Journal of Theoretical and Applied Information Technology 10th June 2014. Vol. 64 No.1

[7] Jin Уe, Jianxin Wang, Qinghua Liu, Yuhong Luo, "An Improved TCP with Cross-layer Congestion Notification over Wired/Wireless Hybrid Networks", ICYCS, pp 368-373, 2008

[8]. Daniel Scofield, Lei Wang, Daniel Zappala: "HxH: a hop-by-hop transport protocol for multi-hop wireless networks", WICON 2008: 16

[9] Imran Chowdhury, Asaduzzaman, Saki Kowsar, "An Energy Efficient and Cooperative Congestion Control Protocol in MANET", International Journal of Computer Applications (0975 – 8887) Volume 58– No.17, November 2012, pp.27-34.

[10] K. Srinivas, A. A. Chari, " ECDC: Energy Efficient Cross Layered Congestion Detection and Control Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012, pp.316-322

[11] Er. Ramandeep Kaur, Dr. Tanupreet Singh "A Review On Cross Layer Design And Signaling Methods In Mobile Ad Hoc Network" in

[12] T.Suryaprakash Reddy, Dr. P. Chenna Reddy, "EOCC: Energy-Efficient Ordered congestion control using cross layer support in Mobile Ad Hoc Network routing",International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012, pp.1-9

[13] . Sheeja S, Dr. Pujeri Ramachandra V. "Cross Layer based Congestion Control Scheme for Mobile Ad hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.

[14]S.Sheeja and Ramachandra.V.Pujeri, "Effective Congestion Avoidance Scheme for Mobile Ad Hoc Networks", International Journal of Computer Network and Information Security, January 2013, Vol.1, pp.33-40.

[15] S.Sheeja and Ramachandra.V.Pujeri, "Cross Layer Based Secure Multipath Routing Scheme for Congestion Avoidance in MANET", European Journal of Scientific Research, Vol. 97, No. 3, 2013, pp.331-344.

[16] . Sunitha D. , Nagaraju A., Narsimha G. "A Cross-Layer Approach for Congestion Control in Multi hop Mobile Ad Hoc Networks" International Conference on Computing for Sustainable Global Development(2014).

A New Cross Layer Routing Protocol Named Dynamic Packet Guidance (DPG) for Mobile Ad hoc Networks

Er. Navneet Kaur
M.Tech Research Scholar
Amritsar College of Engineering & Technology, Amritsar
ndhammoo@gmail.com

ABSTRACT:

Dynamic packet guidance (DPG), a new routing protocol is introduced for MANETs. As compared to several other routing protocols, DPG provides low end to end delay, low to medium delay, smaller overhead thus reduces energy consumption of nodes according to the results of simulation. A new cross layer routing protocol DPG proves to be very useful in dense networks. Several other routing protocol operates dependently upon falling nodes whereas DPG operates independently of falling nodes and very often undergoes route discovery because of the gradient value in its gradient cache of all the nodes present at the time of transmitting data packets.

I. INTRODUCTION

Now-a-days, communication between the two mobile nodes does not depend upon any fixed infrastructure due to quickly changing environments, thus there is great need for such networks which can be expected to operate without infrastructure. Mobile Ad hoc Networks (MANETs) provides such environment, where nodes are free to move and communicate with one another without centralized administration. Files and resources can be shared by users via MANETS. Many new routing protocols has been developed for MANETs, designers of these routing protocols faces different challenges. The basic need for such a routing protocol is to generate minimum communication overhead, low end-to-end delay, medium to high speed, low-to-medium load, efficient delivery of packets. The major problems faced by the designers are packet loss, fading, bandwidth constraints of the wireless links and rapidly changing topology. In response to above problems, various Ad hoc routing protocols have been proposed which we discuss in the next session of the paper. In this paper we propose the new cross layer routing protocol named dynamic packet guidance(DPG)protocol which suites better in the situation where there is small delay, reduced overhead which is essential property while delivering the data packets between the smaller number of pairs of nodes. Also in this paper, we compare the proposed routing protocol named DPG with the rest of the routing protocol that are being used in the literature such as Ad hoc on Demand Distance Vector (AODV), Dynamic source routing (DSR), and the Dynamic MANET on-Demand (DYMO).

II. AD HOC ROUTING PROTOCOL

a. Dynamic Source Routing

Dynamic source routing (DSR) protocol usually contains complete sequence wise list of the nodes, from where the data packets should pass, hence it uses the explicit source routing. Due to use of explicit source routing, it provides support to use multiple route and permits the sender to select and control the routes for its own packets. With the increase in data packets, header length also increases which is a drawback for the DSR.

In Ad hoc networks, arbitrary route destination is achieved by the two mechanism one is route discovery another one is the route maintenance. When the route to destination node (D) is not known to send the packet to node D through S attempts then the route discovery came into existence. Let us assume the example to explain the concept of route discovery, suppose the node S wants to send the packet but the source node(S) does not know the exact route to destination node (D). To initiate the route discovery, firstly the node S transmits route request (RREQ) packet to all the its neighbouring nodes. RREQ contains the unique request identifier of the initiator of RREQ. RREQ contains the list of address of all the nodes through which RREQ travels for the route discovery.

When node D receives RREQ, it forwards RREQ to the initiator of the route discovery, with the copy of the RREQ. To roll back the RREQ to its source node (S) , node D uses its route cache for route back to the initiator. Another approach to route back the RREQ is to simply reverse the route of the RREQ. When node S finally receives the RREQ, it

uses the route cache for sending the data packets to the destination node (D).

b. Ad Hoc On Demand Vector (AODV)

AODV uses the distance vector algorithm concept. To forward the data packet to the destination node it uses routing table mechanism. AODV creates next hop at all the intermediate nodes which are active in the communication. To find the route to the destination node D, AODV broadcasts the RREQ packets. When the RREQ packets reaches the one of the intermediate node or the destination node, then the route is made available to the initiator of RREQ by unicasting the RREP packets. AODV maintains the link status of next hop in active routes. When the link is broken, route error (RERR) message has been delivered to all its nodes to inform the link loss. AODV does not allow the multiple routes to single destination thus, a new route discovery always has to be initiated when the route is broken.

c. Dynamic MANET On Demand(DYMO)

DYMO is the simpler approach to the AODV routing protocol. DYMO uses the same route discovery mechanism as used in AODV. Basically, DYMO lowers the system requirements for executing the nodes. Some new features like path accumulation and MANET internet gateway scenarios are included in DYMO. Path accumulation is achieved during the transmitting of RREQ packets through the network. In the Dynamic MNAET On Demand (DYMO) routing protocol, when the intermediate node receives the RREQ, DYMO protocol includes the route of previously attended node by deducting the route of all the RREQ passed nodes rather than the those of the initiator of the RREQ packets.

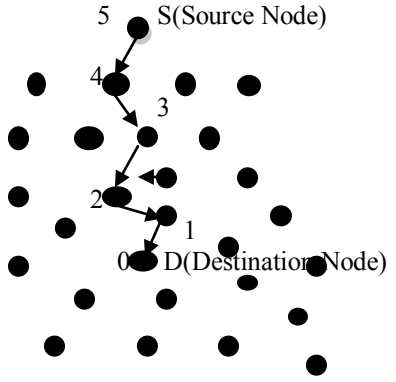


Fig 1.Forwarding the packets from node S to node D according to descending order of their gradient value.

III. Dynamic Packet Guidance (DPG) protocol

Gradient concept is used in the DPG protocol. Gradient is a numerical value which represents the distance of the source node(S) from the destination node (D) to deliver the data packets in terms of minimum number of the hopes. Let us consider overview of how gradients are used in the DPG protocol. Both the gradients and MAC layer request–to-send/clear-to-send(RTS/CTS) handshake between the neighbours. The main purpose of the handshake is to deliver the data packets through the network. When a particular node wants to send the data packet to its intermediate nodes, then it transmits the short RTS message which includes the length of the data packet and the destination node along with the gradient value of its own. Nodes which have higher gradient value does not participate in packet forwarding whereas the nodes which have lesser gradient value transmit the CTS reply to indicate the packet forwarding. To forward the packet each node has to wait for the small interval of the time to ensure that only one node at a time delivers the packet before the sending CTS message. Now CTS informs the eligible neighbours not to participate in the packet forwarding. The nodes which sent the CTS successfully can demand for the acknowledgment for the data packets. This process is continued until the destination node is reached. MAC layer request-to-send/clear-to-send handshake provides two functions in DPG routing protocol.

- Upon hearing RTS/CTS messages, nodes will no longer send the data packet along with the destination node and with its own gradient value to the immediate node, thus creates virtual carrier. This virtual carrier minimize the collision on Wireless Channel.
- With the transmission of CTS, all the neighbour nodes stay silent in packet forwarding which prevents the multiple copies of data packets in packet forwarding which not only reduces the bandwidth but also the energy consumed during the packet forwarding by networks.

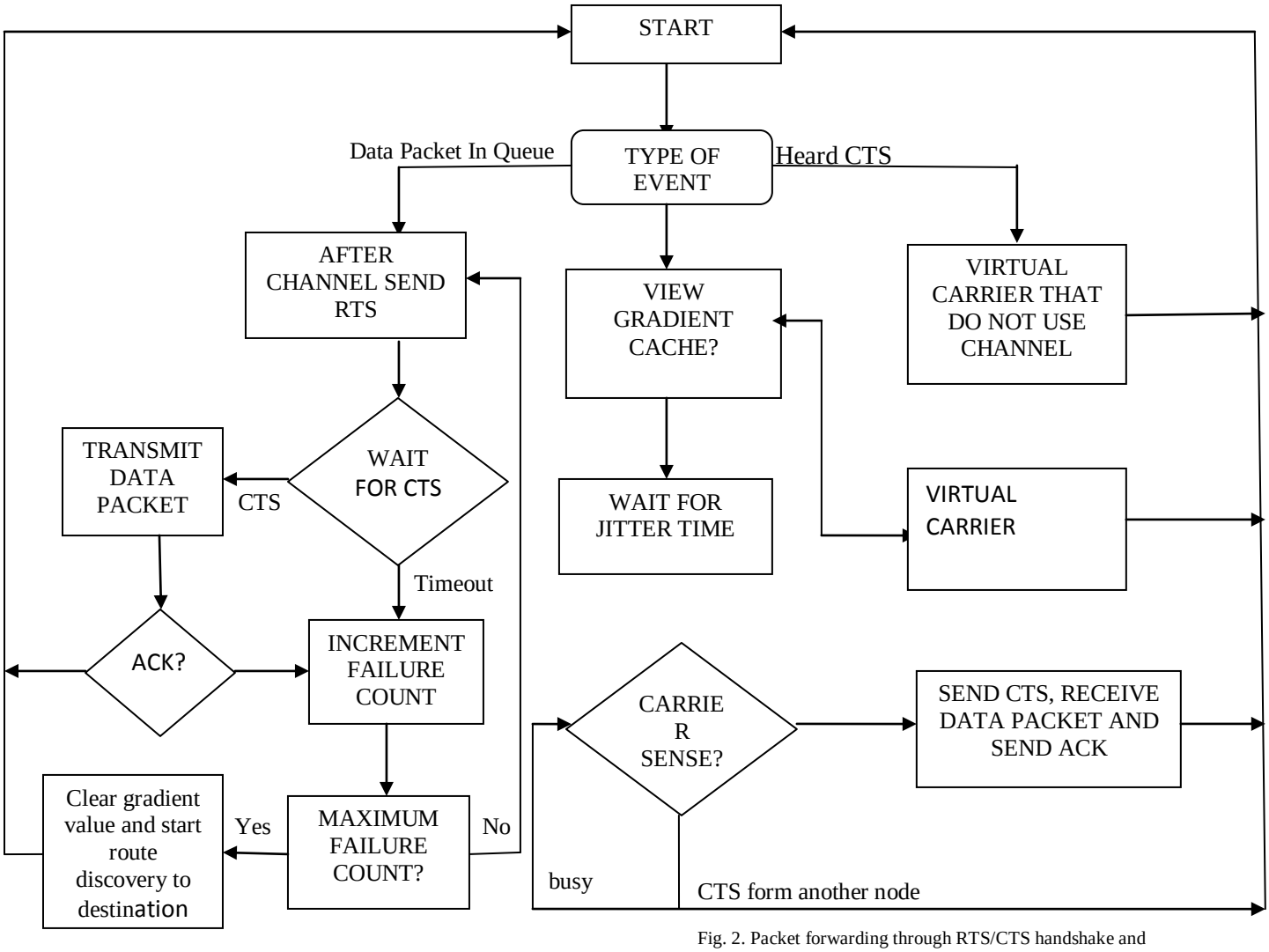


Fig. 2. Packet forwarding through RTS/CTS handshake and gradient.

a. Route Discovery

To explain the concept of route discovery let us consider the illustration, suppose the source node(S) wants to send the data packets to the destination node(D), it initiate the process by sending the RREQ packet to the whole network. when the RREQ packet reaches the destination node then it will broadcast the RREQ packet through the network. All the intermediate nodes note down the minimum number of the hops that node travel for the packet forwarding, hence calculate the gradient value. This gradient value is stored in the gradient cache of all the intermediate nodes for future use.

When the source node(S) receives the RREP, it sends the data packet with the gradient value to the destination node. DPG does not allow very often route discovery for any sub-sequent packet forwarding due to its gradient value stored in the gradient cache of all the node whenever needed the source node(S) checks gradient value for the destination node in its gradient cache if it matches then there is no need for the route discovery.

b. Final Thoughts regarding DPG routing protocol

- Packets are being broadcast in wireless LAN by an Acess point (AP) using the basic rate of 2Mbps in IEEE 802.11b which includes the wider range of devices. Mainly it uses the global broadcast scenario. MANETs generally are not compatible with the global broadcast scenario. The new proposed cross layer routing protocol named DPG uses the local broadcast scenario. The main function of local broadcast is to deliver the data packet in packet forwarding.

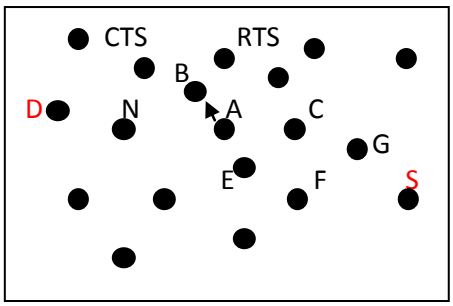


Fig.3. RTS/CTS Handshake in DPG protocol.

With the mapping of RTS/CTS handshake with the local broadcast, avoids the blockage of whole network. Suppose the node A wants to forward the data packet to the another node B as in Fig.3,but we notice that the node C and node E hears the RTS message but does not respond to CTS message because of higher gradient value to node D. Thus nodes F and G are not get disturbed by CTS and will not interfere with node A transmission, thus prevents the blockage of whole network.

- In Fig3, only those nodes which have smaller gradient value are able to send CTS to node A. The nodes having the smaller gradient value lies in left region of node A, will able to send CTS transmission to node A. Suppose if a node hear RTS message from the node A but does not respond to CTS from node B, therefore decided to send its own CTS? DPG handles the above situation by mandating that only one node hears the data packet from node A ,that node stay silent afterwards.
- To solve the collision between the two nodes, time at which node noted the gradient value in its gradient cache is noted. Prior gradient value is taken into account.

IV. Comparison of DPG with DSR, AODV, DYMO.

The proposed cross layer routing protocol named DPG uses the broadcast technology for RREQ and RREP packets to be transmitted through a network for packet forwarding whereas the AODV, DYMO routing protocols unicast the both RREQ and RREP packets in a network. DSR provides the routing information in its header therefore have variant header length. Whereas DPG, AODV, DYMO have the fixed header length because they does not include the routing information in its header.

AODV and DYMO routing protocols uses the concept of next hop if the next hop moves out of the range of the network for packet forwarding then the route is broken. Therefore AODV AND DYMO have to restart the new route discovery. Whereas in DPG, new route discovery is very often used due to the gradient value which serves as the next hop, thus avoiding single point of failure. Hence, DPG and DSR provides multiple route rather than the new route discovery.

In DSR, RERR message is generated which informs the source to itself find the route for packet forwarding whereas in case of DPG routing protocol, falling nodes does not affect the operation. Rather than those of DSR routing protocol, DPG has the fixed number of the header length which makes it capable of having higher number of nodes .

V. Simulation Results

In the simulation process, we compare the DPG with other routing protocols like AODV, DSR, DYMO on the basics of average delay, standard deviation of delay and average energy conservation.

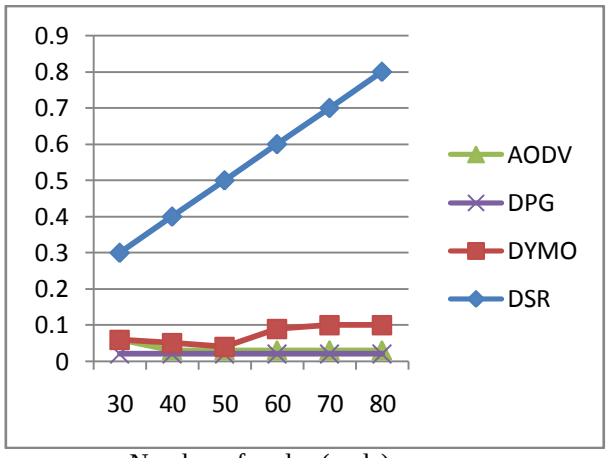


Fig. 4.Average Delay versus Number of nodes

The above graph Fig. 4 shows the average delay versus number of the nodes. Here in the above graph we concluded that DPG routing protocol has lower value of average delay as compared to AODV, DSR, DYMO which in turn reduces the route discovery mechanism during packet forwarding. The low level of average delay comes out in the graph is due to its route maintenance capability while transferring data packets from source node (S) to destination node(D).Thereafter, we came to know in the simulation process that average delay time of DPG routing protocol increases with enhancement of number of the nodes because topology changes more frequently with increasing no of nodes thereby results in many broken routes before reaching the valid route.

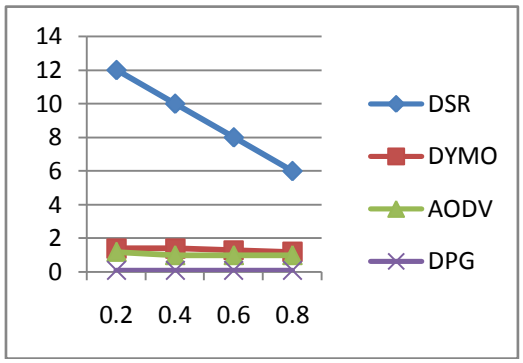


Fig.5.Standard deviation of delay versus ratio of falling nodes

From the above Fig.5.it is clear that the standard deviation of delay is lesser in DPG routing protocol which also reduces route discovery mechanism very often because the most of packets which are delayed during the same time interval thus itself reaches the situation where there is lesser possibility for route mechanism process.

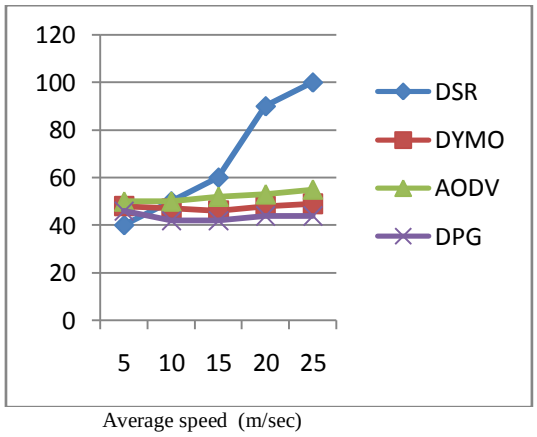


Fig.6.Average consumed energy versus average speed

Fig.6. shows that the proposed cross layer routing protocol named DPG consuming the lesser amount of energy because of lower overhead through which nodes transmit less thereby consume lesser energy.

4. REFERENCES

[1]M.Hawa et al/Int.J..Electron.Commun.(AEU)66.2012p.996-1005

[2] Corson S, Macker J. RFC2501: mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. Internet Eng Task Force 1999.

[3] Perkins C, Bhagwat P. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Comput Commun Rev 1994;24(4):234–44.

[4] Johnson D. Routing in ad hoc networks of mobile hosts. In: IEEE workshop on mobile computing systems and applications. 1994. p. 158–63.

[5] Johnson D, Hu Y, Maltz D. RFC4728: the dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. Internet Eng Task Force 2007.

[6] Perkins C, Royer E. Ad hoc on-demand distance vector routing. In:IEEE workshop on mobile computing systems and applications. 1999.p. 90–100.

[7] Perkins C, Belding-Royer E, Das S. RFC 3561: ad hoc on-demand distance vector (AODV) routing. Internet Eng Task Force 2003.

[8] Chakeres I, Perkins C. Dynamic MANET on-demand (DYMO) routing. Internet Eng Task Force 2010 [draft-ietf-manet-dymo-21].

[9] Haas ZJ, Pearlman MR. The performance of query control schemes for the zone routing protocol. IEEE/ACM Trans Netw (TON) 2001;9:427–38.

[10] Gupta A, Sadawarti H, Verma A. Performance analysis of AODV, DSR & TORA routing protocols. IACSIT Int J Eng Technol 2010;2(2).

[11] Das S, Perkins C, Royer E. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Pers Commun 2001;8(1).

[12] Broch J, Maltz D, Johnson D, Hu Y, Jetcheva J. A performance comparison of multi-hop wireless ad hoc network routing protocols. In: Proceedings ofthe ACM/IEEE international conference on mobile computing and networking. 1998.

[13] Dressler F. Self-organization in ad hoc networks: overview and classification.ACM Comput Commun 2008;31(13):3018–29.

[14] Tseng Y-C, Ni S-Y, Shih E-Y. Adaptive approaches to relieving broadcast storms in a wireless multihop ad hoc networks. IEEE Trans Comput 2003;52: 545–57.

Evolution of Computer: From Personal to Cloud with Security Issues

Harminder Singh
Research Scholar, E.C.E. Department, A.C.E.T., Amritsar
harmindersingh.ece@gmail.com

Guneet Kaur
Assistant Professor, E.C.E. Department, A.C.E.T., Amritsar
erguneetkaur@gmail.com

Abstract- **In this on going era of research, innovation, development and implementation of experiments, computer is the basic need. Today computer has become so common that every human being can immediately count the number of machines in the house or in the office. With increasing time the size of computer is decreasing, it has undergone a hardware change from a room to desktop and from desktop to pockets. But with the growing number of computers in the globe, the challenge originates to safeguard the data of the users i.e. security concern is the main issue in the globe, every country wants and tries to protect the computer of its government and its people from external vulnerable attacks that sometimes hack or in other words steal the data from the machines that the user is unaware from the attack. In this paper a brief summary has been tried to jot down about the evolution of computer from home to industry and from personal to cloud also with some related security issues.**

Keywords- Cloud Computing, Computer Security, Security Policy, Risks, Vulnerability, Implementation.

I. INTRODUCTION

In the past the definition or operation of computer was limited to a machine that performs logical calculations and reduce human burden. With increase in development, the definition grows to send e-mails with introduction of internet. But now the meaning of computer has totally changed i.e. the new explanation of the word computer is that a machine/place where one can do shopping, can undergo distance education, can pay bills, can do recharges, can book railway-air-bus tickets, can order breakfast/lunch/dinner or pizza, can do bank transactions and many more. All these applications ease the moment of the humans but also bring some serious security issues.

II. LITERATURE REVIEW

i. "An overview of the security concerns in enterprise cloud computing" by Anthony Bisong and Syed (Shawon) M. Rahman in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011. In this publication the authors has discussed about the background history of computer, cloud computing growth across the globe, security threats, risks, vulnerabilities, steps to cloud security with its strengths and benefits.

ii. "Computer security by Carl E. Landwehr in IJIS (2001) 1: 3–13/Digital Object Identifier (DOI) 10.1007/s102070100003. In this the main target areas of the author was to introduce computer security, properties, principles, policies (Commercial, Military and others), privacy, security mechanism (Authentication, Authorization, Auditing, Linking users with domains), assurance and security considerations.

iii."International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011 by Dina Meoli and Traci May-Plumlee in Journal of textile and apprarel, technology and management volume 2, issue 2, spring 2002. Under this applications and use of computers is discussed like wired electronis apprarels (Smart shirts, Embroidered fabric keypads in jackets) with their conductive technologies that are used in industries along with enabling technologies, component integration and the challenges.

iv."Technology of competition and the structure of the computer industry" by Timothy F. Bresnahan and Shane Greenstein in the journal of industrial economics volume XLVII. In this publication the authors has explained the history, evolution and presence of computer in industries with the IBM System/360, platform persistence and the IBM System/370, economics of persistence, microcomputing, minicomputing, superminicomputer and the origin of competition.

III. CLOUD COMPUTING

Cloud Computing, as the name suggests is a connection/group of users on a very large scale that share the common data and information, e.g. can be of distance education or online shopping portal other definition of cloud computing is the availability of servers, clients, data bases and applications that are provided on demand by a company through internet. Enterprises are looking towards the vast implementation of this computing to reduce down their cost and to increase their profit. There are several major cloud computing providers in the world such as Google, Yahoo, Microsoft, Amazon and many more, these providers provide the users with infrastructure to perform the desired task on the common platform.

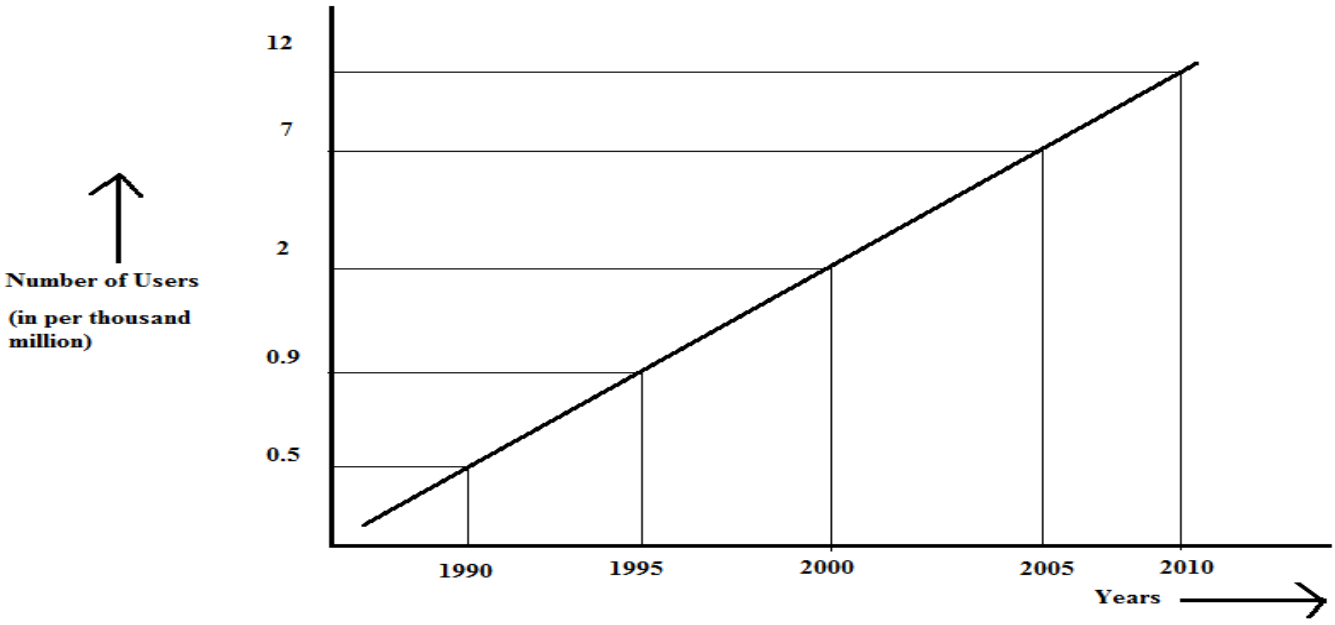


Fig. 1: Showing computer sales around the globe from the year 1990-2010.

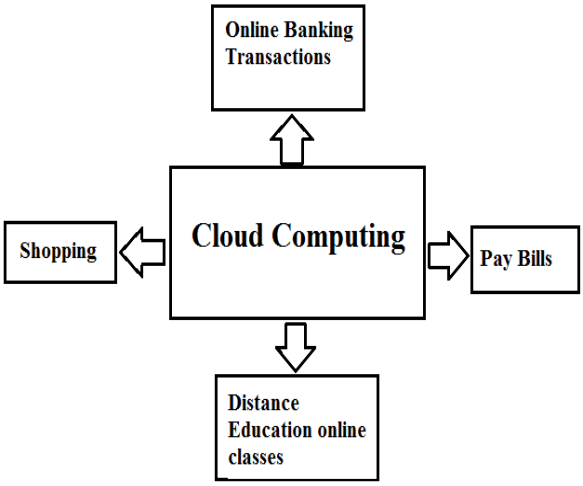


Fig. 2: Depicting various applications of cloud computing.

IV. COMPUTER SECURITY

Computer Security is a great issue of concern for application developers in the world, because securing an computer is as much important as launching an application. Today, nearly all the transactions, sale-purchase of goods on internet is carried through credit-debit cards, so the issue originates to protect the privacy and account of the user from being hacked or lost in the internet while or after making the payment, because a crucial time in the transaction is that when the user enters its password and account number.

In military services and in the functioning of an government, the sent-received information is having the threat of hacked. The main point of an data hacker is to find out the *weak-link* in the organization or in the transmission time because its very difficult to steal data by physical presence so technique used is to locate this link to easy the work.

V. SECURITY POLICY

With the increasing use of cloud computing on a very large scale the further step of data hackers, cyber-thieves, viruses, trojans and worms is to start intervening and attacking.

A security policy by the company provides the user an agreement stating that your privacy and data will be secure in the database of the company, this policy was absent in the past and some incidents occurred due to non-availability of this. E.g. incident like "I-LOVE-YOU" virus[1], this happens as their was no policy to protect the users. A nation can provide security to its users and this is happening is almost every country.

An crucial example of security policy can be taken from healthcare services: patients have to disclose each and everthing about their disease/problem to the doctor, and the doctor has to maintain a record of all patients in a confidential mode and they may have to disclose it to the insurance company for the claim by filling up the subscription form. Government regulations are required to control the information flow[2] to any third party.

While working on computer, an account has to be taken for the *delayed and denied* information as this has the possibility of an odd functioning. Today computers are used in energy distribution, water supply and transportation

services, so a keen eye has to be on security of these services that are directly connected to the countrymen of the nation.

Security policy in domains.

A domain is an collection of server-client systems, in which there is an server which is the head/administrator which provides and governs the flow of data to its client members and also between the them.

It is said that if you want to keep a secret then the best way is to keep silent or don't write that. Or, according to Benjamin Franklin's Poor Richard "There may be a secret if two of them are dead [3]."

As in cloud computing there is the use of domain application for the ease of data flow it is difficult to check/verify whether the client joined is an a real user or is a potential threat to the system. So the system defines a security parameter that decides the scope of what to be protected, what to be flowed at which time to which user by checking the authentication.

But in today world also, there are some cases where the users needs to be connected to some few users like in the case of connection to a building, where it becomes easy for the *intruder* to access the link, where an intruder is an individual who gain access on false ground parameters by violating security policies without any grant of authorization. Another example is the installation of modem on the PC to gain connection to the internal corporate network which works on small scale communication in the absence of any strong security policy. Since the intruder's behavior on the network is same like that of normal users so it becomes difficult to distinguish it from other normal users [4].

VI. SECURITY THREATS, RISKS AND VULNERABILITY.

i. Security Threats

The Cloud Security Alliance (Cloud Computing Alliance, 2010) defines the following threats:-

- Ill-treat and Criminal Use of Cloud Computing.
- Insecure Application Programming Interfaces.
- Ill-natured Insiders/Intruders.
- Shared Technology Unprotected.
- Data Loss/Leakage.
- Account, Service and Traffic Hijacking.
- Unspecified Risk Profile.

ii. Risks

It is defined as an event that has an potential to harm by using some ongoing application or from some upcoming operation. In an IT Organization Security parameters are understood and defined as the potential to harm and destroy the privacy and confidentiality.

Going towards cloud gives some major risks of loosing someone's intellectual belongings, trade secrets and personal information. An potential of loss is that the information may fall into an wrong hand that can misuse according to the one's wish.

iii. Vulnerabilities

Vulnerability is defined as an weak-point point in an network from where an intruder enters to harm the public interest. Shifting your all data to an cloud service is just like "placing your all eggs in one basket" [5].

Researches showed that it is possible for an hacker to locate the target's data and uses various moves to gather that [6].

It has also seen that hackers use their virtual machines to attack on original workstations/machines, by being as a member in the main network, to steal data and other important information. The first task of an intruder is to get the password [7] of the account holder/user in order to get the access for other linked information.

VII. SECURITY PRINCIPLES

i. Accountability

Users behave better if they know that they may be questioned for their wrong deeds. It works in three ways: Firstly it should be transferred from a human being to the computer that a wrong action is not to be performed on the machine/computer, so that the responsibility is to to be shared between the user and computer. Secondly, the operations of the computer system within the system/network must be authorized. And finally the audit process must be carried out.

ii. Least Advantage

Under this the principle of granting only those privileges to the computer that are to be designated for its function is followed i.e. no extra grants/privileges are provided[8]. Even though the individual knows the use and practical implementation of the application, it is not granted the permission to use it unless that is provided with the appropriate authentication by the provider.

iii. Default Security and Defence in Depth

Under default security principle the machine should be assembled with the physical architecture not with the pre installation of the User ID and Password i.e. these two are the functions of the user. There is violation of this principle if there is pre establishment of default sharing settings, administrative functions and users rights.

In Defence in Depth mechanism it is told not to put all the information at a single place because it would be difficult to recall the data in case of information hacking and data loss. This operation may face an odd in the network because it provides prior negative image of the provider and creates

complexity that the provider is not capable of restoration of the data.

VIII. CLOUD COMPUTING IMPLEMENTATION

Following are the steps to understand the security issues related to cloud implementation:- [9]

i. Recognize the Cloud.

Under this the size and parameters of the network are understood according to the type of usage and requirement. Also the in-depth knowledge of transmission-reception of data is required.

ii. Transparency Requirement.

In this the cloud supplier makes sure about the originality of the security architecture used in the organization and should willing to undergo regular security audit to maintain transparency.

iii. Strengthen the Internal Security

The providers should make sure that their internal security to the network and towards the user's data is sufficiently strong with the association of firewalls etc, and comply with the cloud security measures.

iv. Examining the Legal Implications

By viewing and experiencing that what the user is sending-receiving in the cloud is according to the laws and regulations or not. If it is not according to the legal practices then the provider can examine and re-scan the authentication of the user to verify between the real user and the hacker.

v. Paying Attention

By constantly viewing any modifications, developments or changes in the cloud technologies, cloud related laws and regulations and practices that may has effect on the security aspect.

IX. CONCLUSION

Cloud Computing is the combination of several technologies and is gaining importance day by day. But with the advantages of reduced cost equal threats are also their that limits its growth. Business leaders who rare in, or wants to be in this computing should take some serious steps and measures to tackle the problem of security.

Security management is an centralized process that is carried out at the providers side and is used by the user. Reliability and Performance in concern with the cloud industry should be maintained to gain the confidence of users in this network.

Issues in the way of cloud computing should be destroyed completely or should be weaken at the initial point of implementation, wait should not be done for the condition to turn vulnerable.

X. REFERENCES

[1] Markoff J (2000) An 'I love you' virus becomes anything but. The Week in Review, New York Times, 7 May 2000.

[2] U.S. Department of Health and Human Services (2000) Health insurance reform: standards for electronic transactions, 45 CFR Part 160 and 162. Office of the Secretary of Health Care Finance Administration, 20 August 2000. url: http://aspe.hhs.gov/admnsimp/final/txfinal.pdf.

[3] Franklin B (1968) Poor Richard's almanac. In: Bartlett J; Beck EM (eds.) Bartlett's Familiar Quotations, 14 edn. Little, Brown, Boston, p 421b.

[4] McHugh (2001) Intrusion and intrusion detection. Int J Inf Secur, this volume.

[5] Perez, S. (2009). The Cloud Isn't Safe?! (Or Did Black Hat Just Scare Us?). August 5, 2009.ReadWriteWeb. Retrieved from http://www.readwriteweb.com/archives/the_cloud_isnt_safe_or_did_blackhat_just_scare_us.php.

[6] Talbot, D. (2009). Vulnerability seen in Amazon's cloud-computing. Technology Review. Friday, October 23, 2009. Retrieved on March 4, 2010 from http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf.

[7] Greene, T. (2009). *New attacks on cloud services call for due diligence.* Network World. Southborough: Sep 14, 2009. Vol. 26, Iss. 28; pg. 8, 1 pgs. Retrieved from http://www.networkworld.com/newsletters/vpn/2009/090709cloudsec2.html

[8] Saltzer JJ, Schroeder MD (1975) The protection of information in computer systems. Proc IEEE 63(9): 1278–1308

[9] Edwards, J. (2009). Cutting through the fog of cloud security. Computerworld. Framingham: Feb 23, 2009. Vol. 43, Iss. 8; pg. 26, 3 pgs.

Performance Analysis of AODV, DSDV and ZRP Routing Protocols under Blackhole Attack in Mobile Ad Hoc Networks- A Review

Er.Jasmeen Kaur
M.Tech Scholar,
Department of Computer Science and Engineering,
Amritsar College of Engineering And
Technology (Manawala)
Email Id- jais2432134@gmail.com

Dr.Tanupreet Singh
Professor and Head of Department,
Department Of Electronics and
Communication Engineering,
Amritsar College of Engineering And
Technology (Manawala)
Email Id- tanupreet.singh@gmail.com

Abstract— Mobile Ad Hoc network is the 'Self-organizing and Dynamic network having the capabilities of real time network. It can alter the network path due to congestion'. There are various security Attacks in Mobile Ad hoc networks. One of them is the Attack named as Blackhole attack which is occurring into the Network Layer. In this review paper the performance analysis of different routing protocols like DSDV (proactive), AODV (Reactive) and ZRP (Hybrid) have been done both under the Blackhole attack and without the Blackhole attack by varying number of nodes. In This the different parameters like Throughput, Average end to end delay, Packet drop ratio(PDR) and Packet Drop rate(PDRR) are used to evaluate the performance of the routing protocols DSDV, AODV and ZRP under Blackhole attack in Mobile Ad hoc networks.

***Index Terms*—MANETs, AODV, DSDV, ZRP, PDR, PDRR**

I. INTRODUCTION

MANETs- Mobile Ad hoc networks are the 'self organizing and Dynamic network having the capabilities of real time network'.

It is a collection of wireless mobile connections or nodes that can communicate with each other without the centralized controller authority. Due to the characteristics of MANETs for instance wireless connection and dynamic network and distributed network Mobile Ad Hoc Network is exposed to many security attacks like Wormhole attack, Black hole attack, Gray hole attack, Flooding attack, jellyfish attack, Sybil attack etc.

Though, wireless networks are fully distributed and have the ability to work without the aid of any permanent infrastructure or access points. [1]

A. Types of Ad Hoc Network

- Mobile Ad Hoc Network (MANET).
- Vehicular Ad Hoc Network (VANET).
- Internet based Mobile Ad Hoc Network (iMANET).

B. Characteristics of MANETs

The various characteristics of MANETs are [2] :

1. Fully Distributed.
2. Wireless connection.
3. Dynamic network i.e. The nodes can join or leave the network anytime.
4. Flexible.
5. Heterogeneous Nodes.
6. No centralized controller Authority.
7. Peer to Peer Connectivity of the nodes.
8. It must be vary with regular topology changes due to mobility of nodes.
9. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.

C. Applications of Mobile Ad hoc Network

1. Military Network.
2. Sensor Network
3. Emergency Services.
4. Wearable Computing.
5. Personal Area Network (PAN).

D. *Attack:* In Mobile Ad Hoc Network an attack is any try to damage, expose, alter, disable, sneak or gain unauthorized access to make unauthorized use of a resource.[4]

E. Types of Attacks in MANETs:

Two types of attacks in MANET:

1) Passive attacks
2) Active attack

Passive Attacks: In Passive attack, the intruder listen to network in order to get data, what is going on in the network channel? It listens to the network in Order to know and understand how the nodes are interacting with each other, how they are placed in the network. Before the intruder launch an attack against the network, the intruder has enough data about the network that it can easily steal and introduce attack in the network. [5, 6]

Active Attacks: In active attack the intruder unsettle the performance of the network, sneak significant information and attempt to harm the data during the exchange in the network [5, 6].

Active attacks can be of two types. It can be internal or an external attack.

Internal Black hole attack

This kind of black hole attack has an internal mischievous node which fits in between the paths of given source and destination. As soon as it gets the opportunity this mischievous node make itself a fresh data path medium. At this level it is now able of controlling attack with the start of data transmission. This is an internal attack because node itself is appropriate or locates to the data path. Internal attack is more risky to protect against because of difficulty in detecting the internal mischievous node. [5]

External Black hole attack

External attacks are actually locates outside the network and refuse access to network traffic or creating congestion in network or by distracting the whole network. External attack can become a type of internal attack when it grab or take control of internal mischievous node and control it to attack other nodes in MANETs. [5]

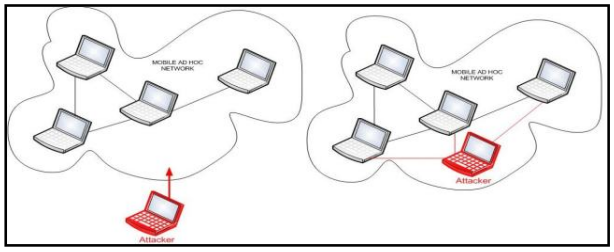


Fig-1 External and Internal attack in Mobile Ad Hoc Network [5]

F. Security Issues in MANETs

The various security issues in MANETs are [7].

- Lack of secure boundaries.
- Risks from compromised nodes inside the network.
- Lack of centralized management facility.
- Restricted Power Supply.
- Scalability.

G. Security Solutions to Mobile Ad Hoc Network

The various security goals to evaluate if mobile ad hoc network is secure or not are as follows [1].

- Availability: Availability means the resources gain access to authorized parties at assumed times. Availability applies to both data and to services also. It makes sure that the durability of network service in spite of Denial of Service attack.
- Confidentiality: This makes sure that computer related resources are gain access only by authorized parties. Securing of information which is swapping through a MANET. It should be secured in opposition to any disclosure attack like Eavesdropping- unauthorized access to messages.
- Integrity: It means that the resources can be adjusted only be authorized parties or only in authorized way. Integrity makes sure that a message being transmitted is never corrupted.
- Authentication: Authentication is basically to sure that members in communication are authenticated and not impersonators. The assets of network should be gain access by the authenticated nodes.
- Authorization: It goal assigns different access rights to different types of users.
- Resilience to attacks: It needs to support network functionalities when a part of nodes is compromised or terminated.
- Freshness: It makes sure that the intruder node does not resend the foregoing captured packets.

H. Types of Security Attacks in MANETs:

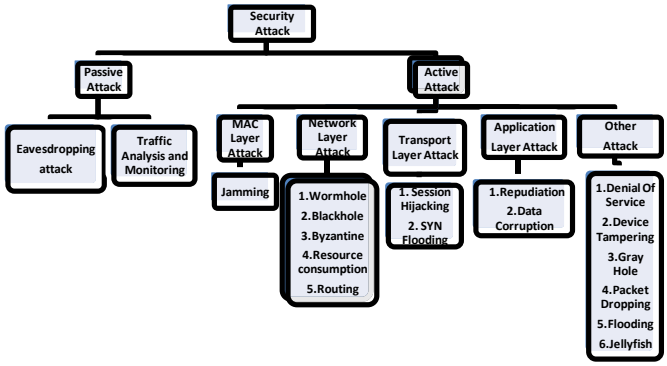


Fig-2 Types of Security Attacks in MANETs

II. BLACKHOLE ATTACK

Black hole attack is the one of the security attacks that is occur in the network layer. In this attack mischievous node uses the routing protocol to promote or to shows itself as having the shortest path to the destination node to which node it wants to interrupt. In Flooding based protocol, if the response from the mischievous node arrives at the requesting node before the reply from the real node or source node then, a fake path has been created. When the information is actually start transmitting it grasps all the packets that were originally meant for the destination node. This mischievous node then can be deciding whether to drop the packet to perform the Denial of Service attack or to use its location on the path as the Man-in-the-middle attack. [8, 9]

A. How Blackhole Attack occur?

In the Fig-2, the source node "A" wants to send the data packet to the Destination node "F". Firstly the Source node initialize the RREQ i.e. the Route request message to all the nodes, to find the shortest path to the destination, then it will

wait for the RREP (Route Reply) message. But before sending the RREP message from the other nodes, the mischievous node enters into the path and Send the RREP message to the source node that it has the shortest path to the destination. Then the Source node can ignore all the RREP messages and send the data packets through the mischievous node and it can delay or drop all the packets before reaching to the destination. In this way the mischievous node can act as the Blackhole attack node into the path.

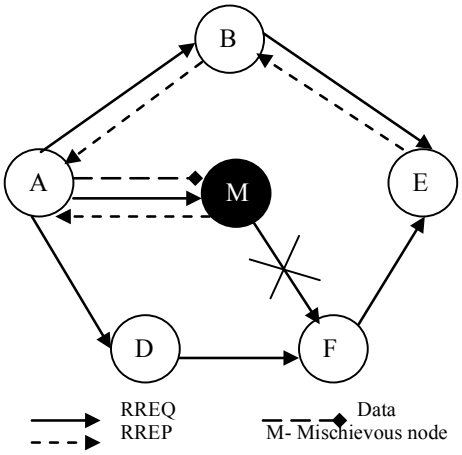


Fig-3 Black Hole Attack[10]

III. Related Work

The Work done by the researchers on MANETs Routing Protocols as Table 1 shown below, some of the researchers have done a comparative study on reactive, proactive and Hybrid protocols with and without Black Hole node in MANET.

Table-1 Related Work

Author Name Reference	**Protocols Used**	**Simulator**	**Performance Metrics**	**Variable Parameters**
S.R.Shirke et al. [11]	AODV	NS-2	PDR, PDRR, Throughput	Number of Mischievous nodes.
Harmandeep Singh et al.[12]	AODV, OLSR, ZRP	NS-2	Throughput, Average end to end Delay, PDR	Number Of Mischievous nodes.
Amin mohebi et al. [13]	AODV, DSR	NS-2	Throughput, Network load, End to End Delay	Number Of Mischievous nodes.
Vidyapathi et al. [14]	AODV	NS-2	Packet Received, End to End Delay , Throughput, PDR	Number of Nodes.
Jaspal Kumar et al. [15]	AODV, IAODV	NS-2	Packet Delivery Fraction Ratio, Throughput, Average end to end delay	Number of Nodes.
Tanupreet Bhatia et al. [16]	AODV	NS-2	Average throughput, PDR, NRL, Dropped Packets, Jitter	Pause time, Number of nodes, speed, Number of Mischievous nodes.
Ashutosh Lanjewar et al. [17]	AODV	NS-2	Power Consumption, End to End delay, Network Load	Number Of data tranfers
Ashok M. Kanthe et al. [18]	AODV	NS-2	Throughput, PDDR, End to End Delay	Number of Mischievous Nodes.
Zaid Ahmed et al. [19]	AODV, idsAODV, HDAODV, EAODV	NS-2	Throughput, Delay, PDR, Energy usage, NRL-Protocol Overhead.	Number of Mischievous nodes.
Mahmood salehi et al. [20]	DSR, OLSR	NS2.34	PDR, End to End Delay, Number of Routing Packets.	Number of Mischievous nodes.
S Muzamil Basha et al., SR Raj Kumar et al., GN. Vivekananda et al., Raghu Veer Matam et al. [21]	DSDV, AODV, ZRP	NS-2	Average End to End Delay, PDR, PDDR, Throughput	Varying Number of nodes.
Tanupreet Bhatia et al. , A.k. Verma et al. [22]	AODV	NS-2	Average Throughput, PDR, NRL, Dropped Packets	Varying the Pause time, Number of nodes, Speed of nodes, Number of Mischievous nodes

IV. Different Routing Protocols in Mobile Ad Hoc Networks

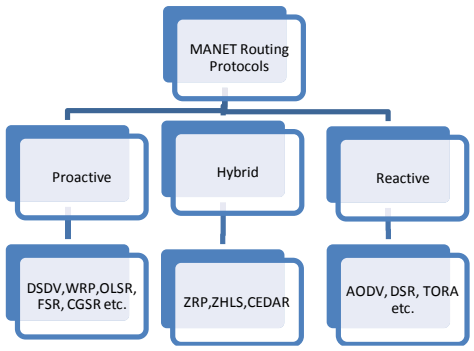


Fig-4 Routing Protocols

Routing Protocols: "Routing is the process of interchange information from one program to the other program in a network."[23].
Routing is the process of forwarding packet from source to its destination using most effective or efficient route. Efficiency of the route is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each device node acts as specialized router itself [24].

There are three types of Routing Protocols in ad hoc networks:

a) Proactive/Table driven routing protocol
b) Hybrid Routing Protocol
c) Reactive Routing Protocol

4.1 Proactive routing protocol

Proactive routing protocol is also known as the Table Driven Routing Protocol. In proactive routing method every node simultaneously maintains complete routing information of the network. This is achieved by flooding network from time to time with network status information to find out any possible change in network topology.

Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile ad hoc environment.

Destination Sequenced Distance Vector routing protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm.

Examples of Proactive Routing Protocols are: [25].
a) Global State Routing (GSR).
b) Hierarchical State Routing (HSR).
c) Destination Sequenced Distance Vector Routing (DSDV).

4.2 Reactive routing protocol

Every node in this routing protocol maintains information of only active routes to the destination nodes. A path search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the path. Quickly changing wireless network topology may break active route and cause subsequent route search [26].

Examples of reactive protocols are:
a) Ad hoc On-demand Distance Vector Routing (AODV).
b) Dynamic Source Routing (DSR).
c) Location Aided Routing (LAR).
d) Temporally Ordered Routing Algorithm (TORA).

4.3 Hybrid routing protocols in MANET

Hybrid routing protocol is the combination of the proactive and reactive routing protocols. There are number of routing protocols of globally reactive and locally proactive states. Hybrid routing algorithm is ideal for Zone Based Routing Protocol (ZRP)

V. OVERVIEW OF DSDV, AODV, ZRP ROUTING PROTOCOLS IN MANETS

A. DSDV (Destination sequence Distance vector)

DSDV is a Proactive or Table driven routing protocol in Mobile Ad Hoc Networks. From the name Table Driven it is clear that in DSDV every node maintain a table listing all the other nodes it has known either directly or indirectly by some neighbors. Each node has a single entry in the routing table as shown below in table i.e. Table-2. The entry will have the information about the node's last known sequence number, its IP address, and the Hop Count to reach that node. Along with this information the table also stores the information about the next hop count neighbor to reach the Destination node, the timestamp of the last updating will received for that node [21].

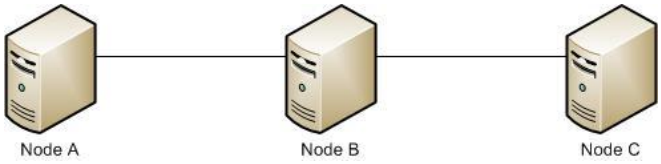


Fig-5 DSDV Routing Protocol

Table-2 contains description of all possible paths reachable by node A, along with the next hop, number of hops and sequence number. [21]

Destination	Next Hop	Number of Hops	Sequence Number	Install Time
A	A	0	A 46	001000
B	B	1	B 36	001200
C	B	2	C 28	001500

B. AODV (Ad hoc on Demand Distance Vector)[9,21]

AODV is the reactive routing protocol which consists of two parts:

1. Route Discovery
2. Route Maintenance

The AODV is the On Demand Distance vector routing protocol which is used to find the path between source nodes to destination node when desired. It uses Request Message such as Route Request (RREQ) and Route Reply (RREP) for establishing a path from source to the destination.
In AODV during the path finding phase when a node get a Route Request (RREQ) message if respond to the source node with the route reply (RREP) message in which it contain the information and sequence number to the destination on the basis of route reply message then network decide which one will be the best path for sending the data to the target node i.e. the destination node. [9]

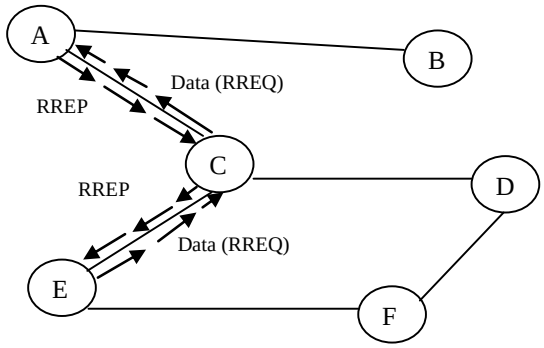


Fig-6 AODV Routing Protocol

C. ZRP (Zone Routing Protocol)

Zone Routing protocol is comes under the Hybrid routing protocol of MANETs. The fundamental approach is to integrate a hybrid protocol that utilize the benefits of both a reactive and a proactive protocol. It was designed to moderate or mitigate the difficulties of those two schemes. Proactive routing protocol uses extra amount of bandwidth which suffers from long path request delays and inefficient flooding the whole network for path determination. ZRP addresses these difficulties by combining the best properties of both the reactive and proactive approaches. In ZRP, the distance and a node, all nodes within -hop distance from node belongs to the routing zone of node. However, size of a routing zone depends on a parameter known as zone radius. In ZRP, each node maintains the routing information of all nodes within its routing zone [27].

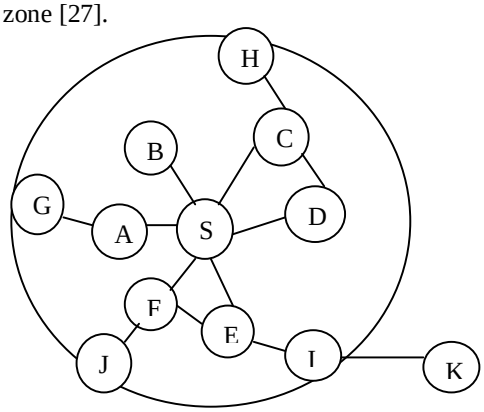


Fig-7 Zone Routing Protocol [27]

VI. PROPERTY COMPARISON OF DSDV, AODV AND ZRP ROUTING PROTOCOL [28,29,30]

TABLE-3 COMPARISON OF DSDV, AODV, ZRP ROUTING PROTOCOLS

Protocol Property	DSDV	AODV	ZRP
Category	Table Driven	Reactive	Hybrid
Loop Free	Yes	Yes	Yes
Multicasting	No	Yes	Yes
Large Network Size	No	Yes	Yes
QoS	No	No	No
Periodic Broadcast	Possible	Possible	Possible
Route Maintained	Route Table	Route Table	Route Table
Protocol Type	Distance Vector	Distance Vector	Link Reversal
Communication Link	Uni-directional	Bi-directional	Bi-directional
Mobility	Performance will low	High	High
Route Philosophy	Flat	Flat	Flat
Message Overhead	Minimum	Moderate	Moderate
Multiple	No	No	No
Reactive	No	Yes	Yes

VII. NS2 SIMULATION

NS2 is the simulator used by the large amount of researchers;, It is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc.

To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator, and one of the most widely used network simulators.NS2 simulator is developed in c++ as Back End and OTcl as Front End. If we want to develop a network then both TCL i.e. Tool Command Language as scripting Language with C++ to be used. [21]

A. Performance Metrics:

The performance metrics that is considered for the evaluation of MANETs routing protocols with and without Blackhole Attack are:

1. Throughput
2. Average End-to-End Delay
3. Packet Delivery Ratio (PDR)
4. Packet Drop Rate (PDRR)

1. *Throughput:* It is the average rate of Successful transmitted data packets in bytes per second within runtime. It is denoted by Tp.[19]

$$Tp = \frac{No.\ of\ bytes\ received * 8}{\text{Simulation time} * 1000} \quad \text{kbps}$$

2. *Average End-to-End Delay:* There are possible delays caused by buffering during route discovery are latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

It is calculated by time taken for a data packet to be transmitted across an MANET from source to destination gives the average end-to-end delay for the received packets.

This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance [15].

Tr = Receiver Time and Ts = Sender Time

3. *Packet Delivery Ratio (PDR):* The ratio of the data packets delivered to the destinations to those generated by the CBR i.e. constant bit rate sources. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher the PDR better the result. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness. To improve the performance of the network system the PDR must be high as feasible [14].

$$PDR = \frac{\textit{Total number of packets received}}{\textit{Total number of packets sends}}$$

4. *Packet Drop Rate (PDRR):* It is the ratio of the data lost at destination to those generated by the CBR sources. The packets are dropped when the node is not able to find the valid route to the node specified as an intermediate node in the route to reach the destination node [18].

$$PDRR = \frac{\textit{Total no. of packets dropped at destination}}{\textit{Total no. of packets created by CBR source}}$$

B. Comparison of DSDV, AODV and ZRP routing protocol on the basis of Performance Metrics[31]:

Table-4 Comparison of DSDV, AODV, ZRP Routing Protocols on the basis of Performance Metrics.

Metrics	DSDV	AODV	ZRP
Throughput	Highest	More than ZRP	Lowest
Average End-to-End Delay	Lowest	More than DSR	Low
Packet Delivery Ratio	High	Medium	Low

VIII. IMPLEMENTATION

Table-5 Simulation Parameters [21]

Parameter Name	DSDV	AODV	ZRP
NS Version	NS 2.35	NS 2.35	NS 2.35
channel type	Wireless Channel	Wireless Channel	Wireless Channel
netif	Phy/WirelessPhy	Phy/WirelessPhy	Phy/WirelessPhy/802_15_4
mac protocol	Mac/802_11	Mac/802_11	Mac/802_15_4
Radio propagation	Two Ray Ground	Two Ray Ground	Two Ray Ground
Antenna Type	Omni Antenna	Omni Antenna	Omni Antenna
Mobility Model	Random waypoint	Random waypoint	Random waypoint
Mobility	40 m/s	40 m/s	40 m/s
ifq	Queue/DropTail/PriQueue	CMUPriQueue	Queue/DropTail/PriQueue
ifqlen	100	100	100
Packet size	256 bytes	256 bytes	256 bytes
number of nodes	15 and 200	15 and 200	15 and 200
routing protocol	DSDV	AODV	ZRP
Zone Radius	-	-	4
Area	1024×800 m	1024×800 m	1024×800 m
Transmission range	200m	200m	200m
simulation time	2000 sec	2000 sec	2000 sec
Topology	Random	Random	Random
Traffic type	CBR(UDP)	CBR(UDP)	CBR(UDP)

IX. RESULTS

A. Simulation Results of DSDV with and without Blackhole Attack in MANETs

Protocol	No. of Nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
DSDV	10	77	71	35	29	0.12	0.2	78	109
	20	68	71	36	30	0.16	0.16	64	210
	30	58	83	53	51	0.20	0.17	55	210
	40	51	60	46	40	0.15	0.13	49	250
	50	49	58	48	43	0.33	0.18	46	270
	60	44	61	49	47	0.27	0.22	45	290
	70	39	56	52	51	0.41	0.27	41	305
	80	34	49	58	56	0.39	0.31	38	315
	90	30	37	61	59	0.52	0.37	33	329
	100	17	29	64	62	0.43	0.43	27	344

Table-6 Results of DSDV With and Without Blackhole Attack [21]

B. Simulation Results of AODV with and without Blackhole Attack in MANETs

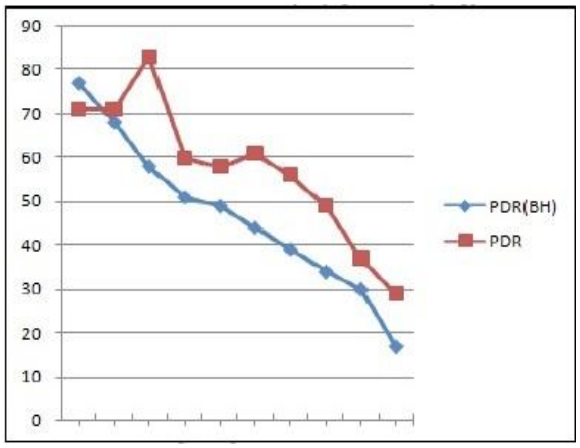
Protocol	No. of Nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
AODV	10	68	95	25	5	0.04	0.28	64	89
	20	61	99	27	13	0.14	0.45	46	93
	30	52	99	50	15	0.16	0.5	45	93
	40	39	99	45	24	0.15	0.52	38	93
	50	34	99	46	25	0.23	0.65	34	93
	60	30	98	45	27	0.14	0.61	30	91
	70	26	97	46	27	0.24	0.60	27	90
	80	21	95	46	26	0.13	0.58	23	89
	90	19	94	46	26	0.26	0.55	19	87
	100	15	90	45	27	0.16	0.49	14	84

Table-7 Results of AODV with and without Blackhole Attack [21]

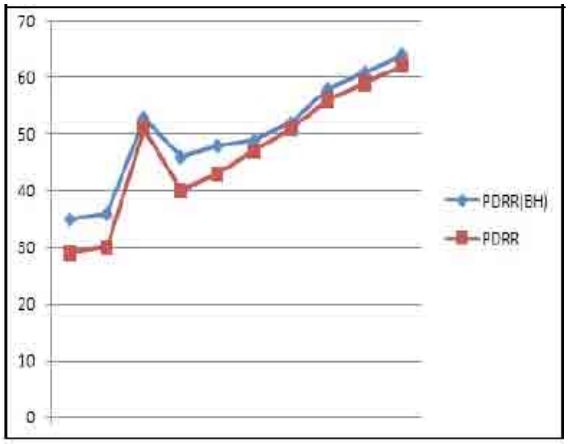
C. Simulation Results of ZRP with and without Blackhole Attack in MANETs

Protocol	No. of Nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
ZRP	10	95	85	26	5	0.031	0.38	95	156
	20	88	70	27	13	0.132	0.48	85	230
	30	75	60	49	15	0.128	0.53	73	210
	40	72	44	43	24	0.184	0.62	71	175
	50	70	34	44	37	0.121	0.73	68	110
	60	65	29	45	45	0.153	0.69	65	95
	70	59	25	45	47	0.091	0.83	60	97
	80	55	19	47	49	0.132	0.79	54	85
	90	51	17	47	54	0.045	0.64	49	80
	100	49	14	44	61	0.119	0.51	42	76

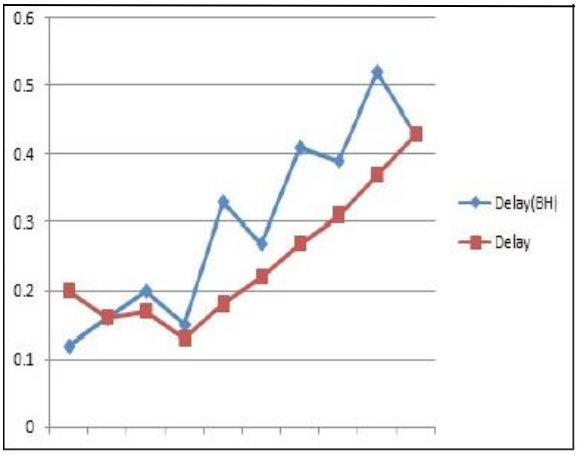
Table-8 Results of ZRP with and without Blackhole Attack [21]



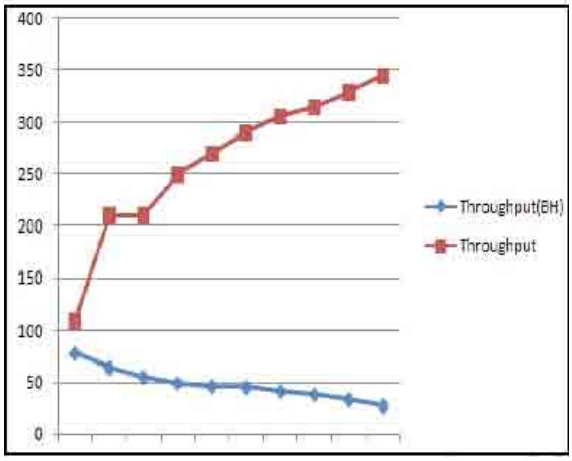
Graph 1.1 DSDV_PDR and PDR (BH) Vs Varying Number of Nodes.



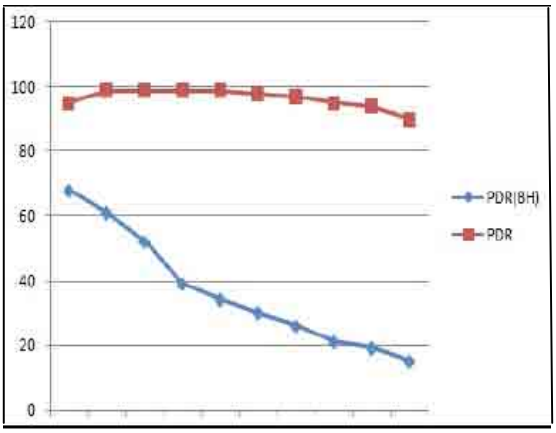
Graph 1.2 DSDV_PDRR and PDRR (BH) Vs Varying Number of Nodes.



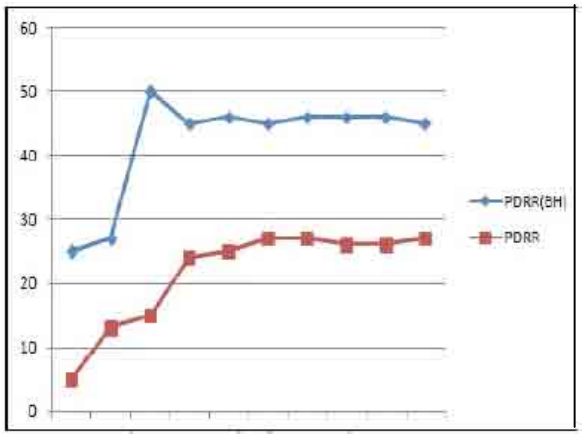
Graph 1.3 DSDV_Delay and Delay (BH) Vs Varying Number of Nodes



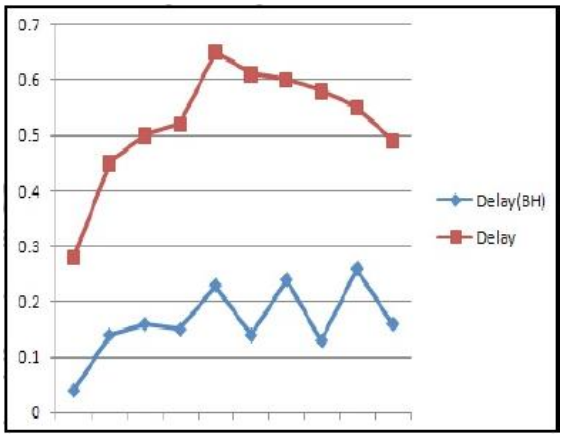
Graph 1.4 DSDV_Throughput and Throughput (BH) Vs Varying Number of Nodes



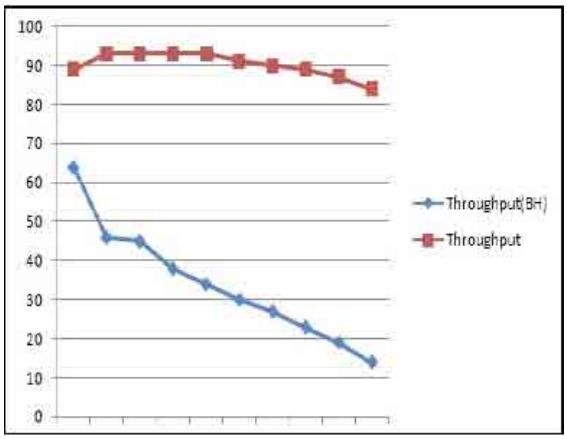
Graph 2.1 AODV_PDR and PDR (BH) Vs Varying Number of Nodes



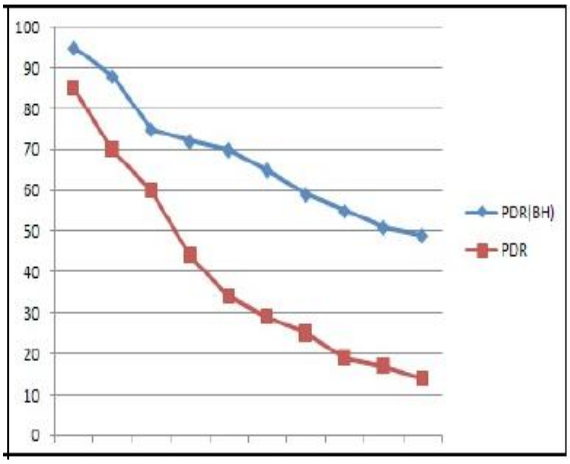
Graph 2.2 AODV_PDRR and PDRR (BH) Vs Varying Number of Nodes



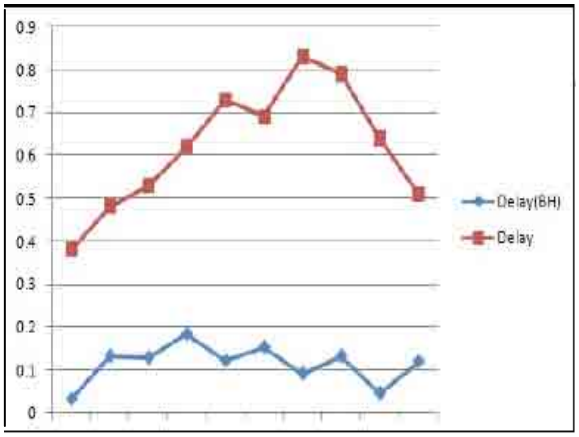
Graph 2.3 AODV_Delay and Delay (BH) Vs Varying Number of Nodes



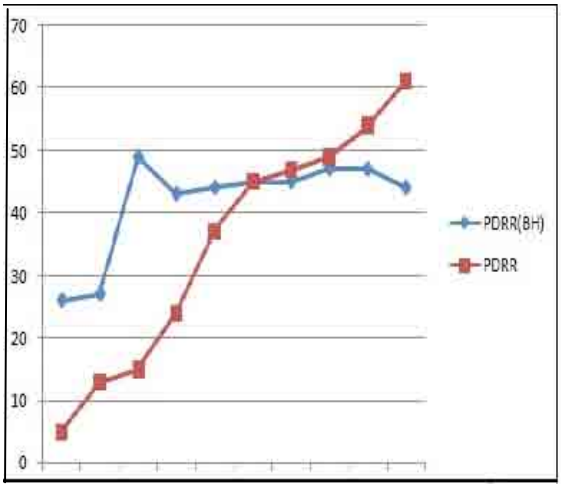
Graph 2.4 AODV_Throughput and Throughput (BH) Vs Varying Number of Nodes



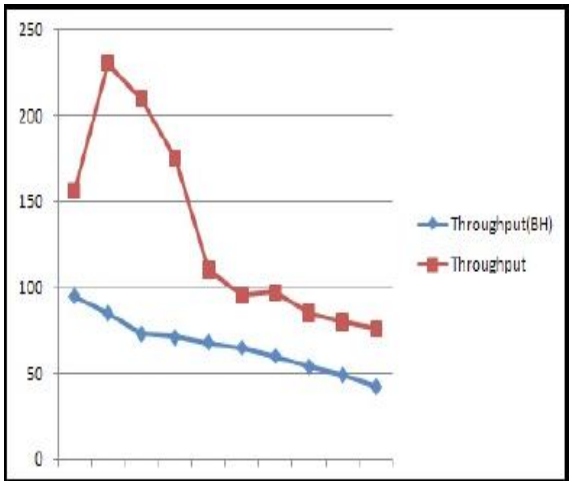
Graph 3.1 ZRP_PDR and PDR (BH) Vs Varying Number of Nodes



Graph 3.3 ZRP_Delay and Delay (BH) Vs Varying Number of Nodes



Graph 3.2 ZRP_PDRR and PDRR (BH) Vs Varying Number of Nodes



Graph 3.4 ZRP_Throughput and Throughput (BH) Vs Varying Number of Nodes

X. CONCLUSION

In this paper, the review has been done by analyzing the Performance Of various Routing Protocols like DSDV, AODV and ZRP in MANETs with the different Performance Metrics as Packet Delivery Ratio (PDR), Packet Drop Ratio (PDRR), End-to-End Delay, and Throughput both with the Blackhole attack and without Blackhole attack. At last, the conclusion is that the effect of Blackhole attack is more on AODV Protocol in contrast to DSDV and ZRP Routing Protocols.

XI. FUTURE WORK

The performance may vary with different types of parameters and Protocols. In this paper the work is done on the three routing protocols which are DSDV, AODV, and ZRP. The further research can be done with the help of other routing protocols in MANETs such as DSR, Olsr, TORA, WRP, CGSR, FSR etc to analyze the Performance under Blackhole Attack. And also the Performance can be evaluated on the basis of other Performance Metrics. We can also analyze the Performance of various routing protocols under other security attacks like Wormhole Attack, Jellyfish Attack, Sybil Attack DoS Attack, Flooding Attack etc.

REFERENCES:

[1] Aarti, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering,volume-3, Issue 5, May 2013, pp. 252-257

[2] http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/

[3]http://skirubame.ucoz.com/_ld/0/29_Topic_1 MANET_v.pdf

[4]http://www.slideshare.net/sunitasahu101/attacks-in manet#btnNext Last Visited- 22, May, 2014

[5] IRSHAD ULLAH & SHOAIB UR REHMAN, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Electrical Engineering, and Thesis no: MEE 10:62 June, 2010

[6] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[7] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Network- A Survey", Department of Computer Science and Electrical Engineering , University of Maryland, Baltimore County

Available:http://www.csee.umbc.edu/~wenjia1/699_report.pdf

[8] Mohammad Al-shurman and Seong-Moo Yoo, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE'04, April 2-3 2004,Huntsville, AL, USA, pp. 96-97

[9] Ms.Nidhi Sharma, "Black Hole Node Attack in Manet",2012 second international conference on Advanced Computing & Communication Technologies, pp. 546-550

[10] Latha Tamilselvan, "Prevention of Blackhole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)

[11] S.R. Shirke, V.R. Ghorpade,"Intrusion Dection System for AODV protocol in MANET", International Journal of Engineering Research & Technology, Vol. 2, Issuse 5, 2013.

[12] Harmandeep Singh, Manpreeet Singh,"Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs", International Journal of Advanced Trends in Computer Science and Engineering, Vol. 2, No. 3, May - June 2013.

[13] Amin Mohebi, Ehsan Kamal, Simon Scot,"Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack", I.J. Modern Education and Computer Science", Vol. 10, 2013.

[14] Vidyapathi, Sundar, Harshita, Komal, "Securing MANET From BlackHole And WormHole Attacks", International Journal of Engineering and Technology" Vol. 5, No 3, Jun-Jul, 2013.

[15] Jaspal Kumar, Kulkarni, Daya Gupta,"Effect of Black Hole
Attack on MANET Routing Protocols", International Journal of Computer Network and Information Security",Vol. 5, pp. 64 - 72, 2013.

[16] Tarunpreet Bhatia, Verma,"Performance Evalution if AODV under Blackhole Attack", International Journal of Computer Network and Information Security" Vol. 12, pp. 35-44, 2013.

[17] Ashutosh Lanjewar, Neelesh Gupta,"Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol", International Journal of Computer Network and Information Security, Vol. 11, No. 4, April, 2013.

[18] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, (2013)"Effects of Malicious Attacks in Mobile Ad-hoc Networks","IEEE International Conference on Computational Intelligence and Computing Research", 2012.

[19] Zaid Ahmad, Jamalul-lali Ad Manan, Kamarulariin Abd Jalil,"Performance Evaluation on Modiied AODV Protocols",IEEE Asia-Paciic Conference on Appiled Electromagnetics, Dec. 11-13, 2012.

[20] Mahmood Salehi, Hamed Samavathi,"DSR Vs OLSR: Simulation based Comparision of Ad-hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks", Sixth Intervation Conference on Next Generation Mobile Application, Services and Technologies, IEEE, 2012.

[21] S Muzamil Basha , SR Raj Kumar et al., GN. Vivekananda et al., Raghu Veer Matam " Improved Performance Analysis of DSDV, AODV, ZRP Under Blackhole Attack in MANETs" IJECT Vol. 4, Issue 4, Oct-Dec 2013

[22] Tanupreet Bhatia, A.k. Verma "Performance Evaluation of AODV under Blackhole Attack" I.J. Computer Network and Information Security, 2013, 12, pp 35-44

[23] Humayun Bakht, "Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks",http://www.computingunplugged.com/issues/issue200410/00001395001.html, April-2003.

[24] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug-1998.

[25] Padmini Misra, "Routing Protocols for ad hoc mobile wireless Networks", http://www.cse.ohio-state.edu /~jain/cis788-99/ftp/adhoc_routing/#TDRP, Nov-1999.

[26] Mario Joa-Ng, "A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks", IEEE Journal on selected areas in communications, Vol. 17, No. 8, Aug-1999.

[27]http://www.ijcaonline.org/archives/volume88/number4/15344-3684

[28] http://ijret.org/Volumes/V02/I08/IJRET_110208058.pdf

[29]https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0CE4QFjAF&url=http%3A%2F%2Fwww.researchgate.net%2Fprofile%2FMuzamil_Basha%2Fpublication%2F258049573_Inclusive_performance_scrutiny_of_DSDV_AODV_and_ZRP_MANETs_Routing_Protocols_Inclusive_performance_scrutiny_of_DSDV_AODV_and_ZRP_MANETs_Routing_Protocols%2Flinks%2F00b49526cf436eeab1000000&ei=7GUUVNkMgrW4BOe2gLAJ&usg=AFQjCNFNUAaRqqx1QIXe5hfiF0cdFfsEtw&bvm=bv.75097201,d.c2E.
Available online

[30] http://www.theijes.com/papers/v1-i2/I012054060.pdf

[31]http://www.ijsrp.org/research-paper-0613/ijsrp-p1836.pdf

Selection of shortest and secure path by Improvements in AODV protocol in Mobile Ad-Hoc Network

Gagandeep Singh Hundal[1*], Dr. Sunil Kumar Gupta[2], Rajeev Bedi[3]

[1]M.Tech Student, CSE Dept., BCET Gurdaspur, Punjab, India

[2]Associate Professor, BCET Gurdaspur, Punjab, India

[3]Assistant Professor BCET Gurdaspur, Punjab, India

*gagandeep.hundal@gmail.com

ABSTRACT

Networks with self-configuring mobile nodes that are infrastructure less are known as the Mobile Ad-Hoc Networks. In these types of networks all the mobile nodes present are free to move as well as to communicate with each other simultaneously. Due to their highly advantageous mobile nature one main problem which occurs frequently is Link Breakage. The efficiency of the whole network is hampered a lot with this single concern. So in order to cater this problem of link failure or link breakage, an alternate path should be provided for the communication to continue. In this paper a new method is devised in order to cater the problem of link failure which will also increase the efficiency of the Mobile Ad- Hoc Network and the AODV protocol. This will also decrease the packet loss incurred during the communication or data transmission.

Keywords: MANET, AODV, link Failure, beacon frames.

I. INTRODUCTION

A Mobile Ad-Hoc Network is a group of Wireless and mobile nodes, which don't have any central controlling node in the network. Each mobile point in the network (often referred to as a node) has two functions to perform: one as a Router and second as a Packet forwarder. These nodes are free to travel in any desirable direction, thus making the network topology unpredictable. This unpredictability of the network make it hard to devise a certain method which can totally avoid the problem of link failure. MANET is a type of network which more oftenly have a configurable networking environment functioning on Link Layer of the Ad- Hoc Networks. All the routing protocols present in MANET are divided into two categories: Proactive and Reactive Routing Protocols. Proactive protocols establish a link between the source and the destination according to the predefined paths in the routing table which are present with each and every node. Whereas Reactive protocols establish a link between the source and the destination only when it is required for the data transmission or communication. The study of the simulation of both the protocols show that the Reactive protocols are more efficient and reliable than the Proactive protocols. In this paper, AODV routing protocol has been used. Security is the biggest issue in the ad hoc routing applications. In ad hoc networks it is quite challenging to cater to security needs of the network due to lack of central authority, topology changes because of node mobility, shared radio channel and limited availability of resources. There are many applications of the ad hoc networks both in commercial environment, military operations and other security purposes.

II.LINK FAILURE PROBLEM

Link failure problem is a common problem in MANET which is caused due the mobile nature of MANET nodes. When the nodes participating in communication move, they may move out of each other's coverage area. Thus causing link breakage. In the diagram below, link problem is shown where in first part of diagram A can communicate with B and B cam communicate with C so there is a link between A → B → C. but in second part of diagram node B moved towards C so B is out of range for A so there is a link failure occurred between A and C.

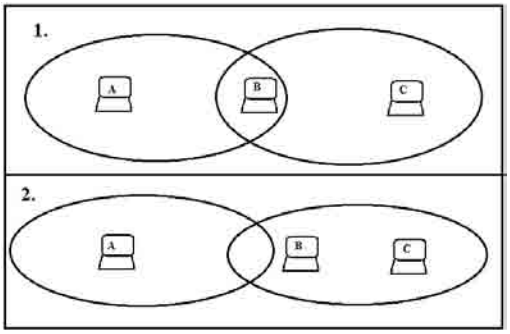


Fig 1**:** Link failure problem

III. LITERATURE REVIEW

Dimitri Marandin (2005), demonstrated the detection of broken links to nodes using hello messages and the feedback provided by Medium Access Control (MAC) layer. The reception of hello messages signifies link availability with the source of hello message. But this technique requires that each node transmits a hello message at regular intervals. MAC layer feedback works better than hello messages when the network load is low. When the load on the network is high, the number incorrect link failure decisions from MAC layer feedback also increases. This results in low throughput (High Packet Loss). Two performance metrics namely Good put and Energy Efficiency were used. Simulation results show that the average energy expenditure per packet received is less in the case of MAC feedback.

Khalid Zahedi *et. al.* **(2011),** proposed the link breakage prediction technique. In this, the Received Signal Strength Indicator (RSSI) value is used by a mobile node along a defined path that is active to predict the link failure. The availability of a link is evaluated and a packet named Soon Link Breakage Warning (SLBW) is generated if there is a possibility of link breakage. The simulation results show that the packet delivery ration is increased significantly. It is also seen that packet loss and end to end delay is decreased.

Mrs. Sunita Nandgave-Usturge (2012), laid emphasis on the routing in MANET. Congestion, mobility and interference being the main judgmental causes for the link failure. When the quantity of data being sent to a network exceeds the limit of the network to holds data at one time, congestion occurs. Congestion mainly occurs at Transport layer Due to congestion, the usage of buffer space at intermediate node increase, thus resulting in loss of data. It is the main culprit in performance degradation of the Transmission Control Protocol (TCP). The reliability of the TCP gained giving sequence number to each packet and by giving back the acknowledgement. Ability of a node to change location within its transmission range is referred to as Mobility. The main reason for packet loss ion the network are mobility and congestion. To improve the performance of TCP cross layer approach is used. Better congestion control techniques are devised in AODV. In this paper the author talks about the four different signal strength based mechanisms to control congestion: AODV, MAODV, Reliable AODV and CLS_AODV.

Parveen Yadav *et. al.* **(2012),** proposed a novel routing algorithm to maintain the route with the use of Link Failure Localization (DSR-LFL). The decisions in the algorithm are taken on the basis of where the link has failed along the source route. This particular algorithm helps in improving the scalability and route maintenance. There is an improvement seen in salvaging of packets and in delivery of packets as compared to the packets sent. A reduction is also seen in the number of error messages.

Humaira Ehsan *et. al* **[2012],** elaborated various kinds of attacks in MANET and simulation of these attacks was done using ns-2 simulator. Various attacks namely black hole attack, selfish node behavior, RREQ flooding and selective forwarding attack are used draw major inferences about the impact of these attacks on the network. If the attacker node is in between the destination and the source, then the malicious node would have a major role in performance degradation. Moreover, if the attacker node is in one part of the network, while the communication between source and destination takes palace in another part of the network, then the impact of the attacker node would be minimal.

K. Shanwaz *et.al.* **(2012),** proposed a modification to the existing DSR protocol by adding a link breakage prediction algorithm. The received packets send a signal power value which is used to predict the time when the link failure could take place. A warning is sent to the source node of the packet if the link is going to break soon. A

proactive route rebuilding is done by the source node to avoid disconnection. The intermediate nodes monitor the signal strength based on a threshold signal value to inform the source node about the likelihood of any route disconnection. This technique reduces dropped data packets.

Mr. S.A. Jain *et.al.* **(2012**), illustrated the different mechanisms used for link failure detection by using alternate route finding. In order to find the path from next to next node Ant colony Optimization algorithm(ACO) is used in mobile Ad-hoc network. In Ant colony optimization, overhead parameter will also improve as the control packets used are only forward ants and backward ants. It also avoids undesired re-transmissions from the source. Thus improving the throughput and end to end delay.

Abedalmotaleb Zadin *et. al.* **(2013), proposed** a stable connection of nodes in MANET by applying a node protection protocol. When a link failure occurs, a total of two nodes are switched off each from a different, this happens in the case of recovery of protection of node. In link protection technique, when a link failure takes place on a primary path, the backup path is not useful. A message is generated for the source which tells the source to again map the path to the destination. The node that was the last reachable uses the path that was designed to be the backup path that covered the unreachable node in order to prevent the mapping of the whole path again thus resulting in time efficiency. The number of packets delivered and the delivery rate is calculated by the Greedy Based Backup Routing Protocol Node Protection (GBR-NP).

IV. METHODOLOGY

According to the proposed solution, the link failure problem can be solved on the basis of beacon frame range concept. Maximum existence of beacon frames is found and dynamically shift the path so as to avoid link failure and enhancing the performance of the network.

The Adjacency matrixof given network is denoted by **A.**

The Number of Nodes is denoted by **n**.

Node **a** is the Source and Node **b** is the Destination.

Step I: Set all Elements outside the range of the given network node to 0.

Step II:.Identification of neighbours of all the nodes in the network present in between Node **a** and Node **b**.

Step III: The path between the Source and the Destination is mapped with high vicinity nodes in it and then stored in an array.

Step IV: The Neighbour list of each node is searched and a node with high vicinity is picked up from the neighbour list and placed in the array

Step V: Match this node with the other neighbouring nodes in the network. If node has the low vicinity, then replace this node with another.

Step VI: Then all the nodes in the array are matched with the neighbour list of the selected node otherwise, Select an arbitrary node with high vicinity and place it in the array. By doing this we get our safe path that would help us in data transmission.

All the above steps result in a network of the high vicinity nodes. In this network, the source node chooses the node which is in its vicinity, is with higher signal strength. Suppose if a node has the 45 percent vicinity, and the path that chooses by the source having the 50 percent vicinity. As the node of vicinity 50 moves from its position then its vicinity will also reduce. In that case the source node will shift the route to the node having the vicinity 45. Thus link failure can be contained by applying this method. The packet loss also reduces. Apath is generated, in which no node with low vicinity is included. The proposed algorithm provides a network having the secure and reliable data transmission.

V. RESULTS AND DISCUSSIONS

Simulation is done using NS-2 simulator. The figures shown below compare the proposed method with method (which adds an extra node when link failure occurs). The graphs show two lines: red line for the traditional approach, green for the proposed method.

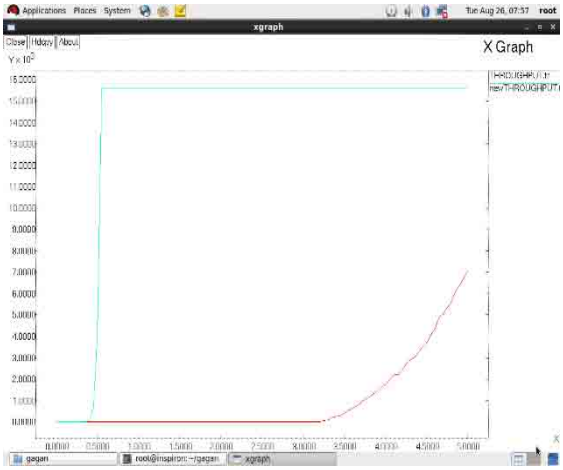


Fig 2: Throughput Graph

Figure 2 shows the graph for difference in throughput. The proposed method shows a considerable increase in throughput.

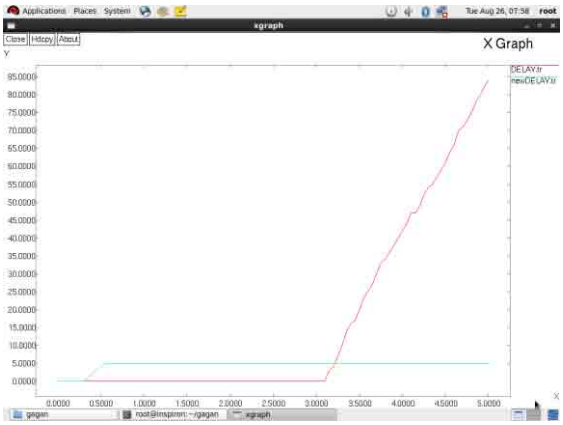


Fig 3: Delay graph

Figure 3 shows the difference in delay caused. The delay in proposed method is quite low.

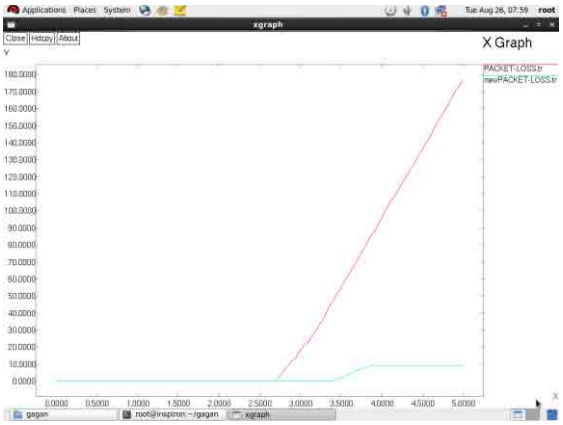


Fig 4: Packet loss graph

Figure 4 shows the Packet loss graph. Increase in throughput will result in decrease in packet loss and vice versa.

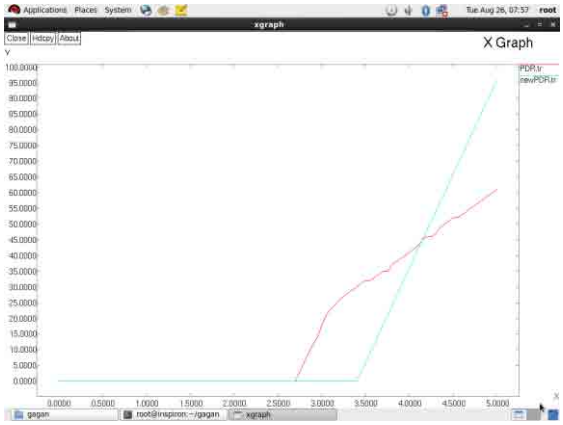


Fig 5: PDR graph

Figure 5 shows the difference in PDR. Packet delivery ratio increases when link failure problem gets eliminated by using the proposed method.

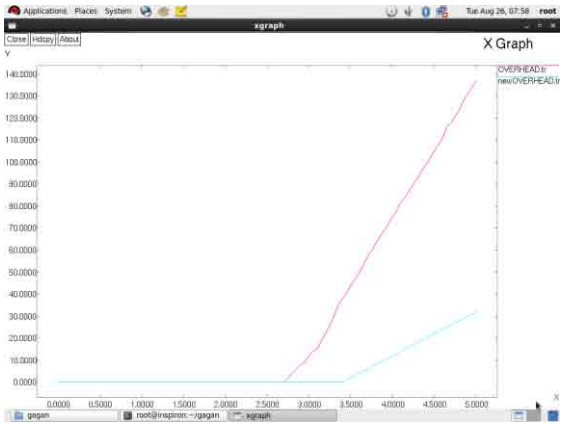


Fig 6: Overhead graph

Figure 6 shows the graph for overhead caused due to link failure problem. The overhead gets reduced when link failure problem is eliminated using the proposed method.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, the routing approaches in ad hoc networks from security view of point, are considered. It presented the requirements that need to be addressed for secure routing. The low vicinity nodes in the ad hoc routing are analysed. Existing routing algorithm for ad hoc networks are not much secure. The proposed algorithm presented in this paper considers the high vicinity between the nodes. These nodes are used for data transmission. The path that is chosen by the source node may consist large no. of nodes. Hence the path of network becomes large, so the future work can also be done to choose the lesser number of nodes with high vicinity. The Security research area is still

open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks.

REFERENCES

[1] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing Security in Wireless Ad-Hoc Network. *IEEE Communication Magazine* , 70-75.

[2]Ehsan, H., & Khan, F. A. (2012). Malicious AODV. *IEEE International Conference on Trust, Security & privacy and Computing and Communiaction* , 1181-1187.

[3] Jain, S. A., & Kadam, A. A. (2012). A Study of Congestion Control mechanism using Link Failure Detection in MANET. *International Journal of Engineering Research & Application* , 1009-1012.

[4] Marandin, D. (2005). Performance Evaluation of Failed link Detection in Mobile Adhoc network. *IEEE* , 398-404.

[5] Nandgave-Usturge, S. (2011). Study of Congestion Control using AODV & Signal Strength by avoiding Link Failure in MANET. *International Conference on Communication, Information and Computing Technology* , 1-5.

[6] Shanwaz, K., & Babu Rao, D. S. (2012). Reducing Link Failure in MANETs using Link Breakage Prediction Algorithm. *International Journal of Engineering Research & Technology* , 01-06.

[7] Yadav, P., Bhattacharjee, J., & Soni, R. (2012). A Novel Routing Algorithm based on Link Failure Localization for MANET. *International Journal on Computer Science & Engineering* , 1738-1748.

[8] Zadin, A., & Fevens, T. (2013). Maintaining Path Stability with Node Failure in Mobile Adhoc Networks. *Elsevier International Symposium on Intelligent Systems, Techniques for Ad hoc & Wireless Sensor Networks* , 1068-1073.

[9] Zahedi, K., & Ismail, A. S. (2011). Route Maintenance Approach for Link Breakage Prediction in Mobile Adhoc Network. *International Journal of Advanced Computer Science & Application* , 23-30.

A Review on Various Security Techniques in Vehicular Ad Hoc Network

Er. Harpreet Kaur
M-Tech Research scholar
Amritsar College of Engineering and Technology, Amritsar
harpreetkaur2555@gmail.com

***Abstract*- Vehicular Ad hoc Network is become more and more important now days. The life saving factor is a key issue in this network. It becomes intelligent transport system. It is a new form of mobile ad hoc network (MANET). In VANET vehicles are the nodes with mobility so there is not a fix infrastructure. It has several safe and non-safe applications in wireless medium which causes several attacks. Due to open access medium, security is the most important concern in VANET. The main objective of this paper is to study various attacks and security issues in VANET.**

***Keywords*- Vehicular Ad hoc Network, Wireless, Attacks, Security, DSRC**

I. INTRODUCTION

Vehicular Ad hoc network (VANET) consists of vehicles/mobiles nodes, which means every node can move freely in the network and stay connected. All nodes can communicate with each other through single hop or multi hop. It is the advance technology in network and wireless communication vehicular ad hoc network. In the year 1998, the team of engineers from Delphi Delco Electronics System and IBM Corporation proposed a network vehicle concept aimed at providing a wide range of application [3]. In the advancement of wireless technology, the concepts of network car attract the attention in all over the world. VANET is a intelligent transport system which provide vehicle to vehicle communication in which vehicles act as mobile node that aim to provide communication among nearby vehicles known as inter vehicular communication(V2V or IVC) and vehicle to infrastructure communication in which between vehicles and nearby Roadside units or RSU known as inter vehicular communication(V2I or RVL). The main goal of VANET is to provide information to passenger regarding their safety and security. Because of wide use of internet, now the aim is to provide commercial information to driver and passengers.

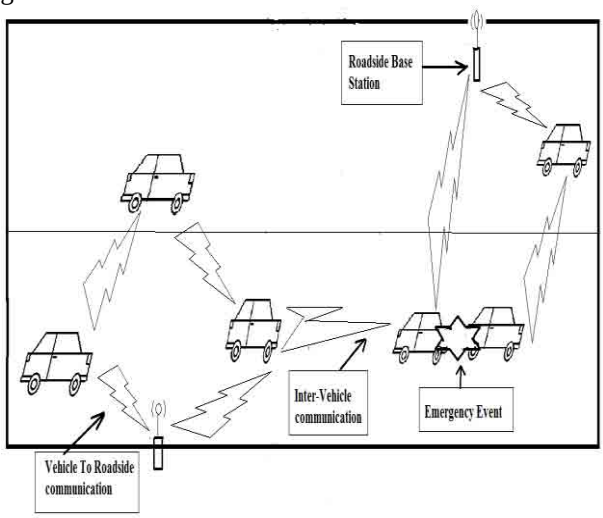


Fig1. VANET Infrastructure

Communication with Wireless Access in Vehicular Environment(WAVE) use IEEE 1609.2 standard known as DSRC 802.11p. A radio used for the communication is Dedicated to short-range Communication (DSRC) which means allocated as a new band in 1999 by the Federal communication commission (FCC)[4]. On-Board Unit (OBU), a device which is inside the vehicles which processes the data collected from various sensors fitted inside the cars and gives conditions of the vehicles is responsibles for communication with outside network i.e with other vehicles and infrastructure.

A) CHARACTERSTICS OF VANET

1) High Mobility

In VANET network, the nodes are usually moved at a high speed. This make difficult to predict the node's position and making the protection of nodes privacy.

2) Rapidly Changing Network Topology

Due to high mobility and random speed of vehicles, the node's positions make changes frequently. Because of this reason, topology in VANET's tends to change frequently.

3) Unbounded Network Size

The VANET network can be implemented in our city, more than one city or in our country. This means the size of VANET is geographically unbounded.

4) Frequency Exchange Of Information

In VANET network, the nodes gather the information from the other nodes and RSU (Roadside Base Unit). Hence exchange of information among the nodes frequently.

5) Wireless Communication

VANET is built in wireless network. Nodes are connected and exchange information via wireless, because of this some security measures are considered in exchange of information.

6) Time Critical

In VANET, the information must be delivered to the node with in time limit, so the node make the decision and perform action accordingly.

II. DATA AGGREGATION

Data aggregation topic will study in the sensor network. The reuse of wireless sensor network Secure Data Aggregation (SDA) mechanism is not possible in Vehicular Ad hoc Network, because of mobility nature of VANET and the fact that nodes moves in specific paths. The bandwidth utilization problem in VANET is solved by the Data Aggregation. Classifications of aggregation technique are: syntactic and semantic.

Syntactic Aggregation compresses or encoded the data after receiving from multiple vehicles and fit the data in a unique frame and record.

Semantic Aggregation means that data received from individual vehicle is summarized.

Some possible attacks on Data Aggregation are:

1) Forging of atomic reports

The station of attacker may forge its own messages and influence further aggregation.

2) Forging of aggregation

Aggregation with arbitrary data is directly created by the attacker and injects them into the network.

3) Suppression of aggregation

Attacker stations may suppression aggregates because of the large information value of aggregates, resulting in biased information dissemination.

III. SECURITY ISSUES OF VEHICULAR NETWORK

VANET face many attacks. These attacks are described as follow-

A) ATTACKS AND THREATS ON VANET

Threats to Authentication VANET are open network and can be easily accessed by attackers. So in the following paragraphs, we introduce the some important attacks in the VANET Domain.

1) Sybil Attack

Sybil Attack happens when large number of pseudonymous is created by the attacker, and act like it is more then hundred vehicles, to tell other vehicles that there is jam ahead and suggest them to take alternate route.

Scope of attack is measured by the area of nodes that have data of uncertain validity. Scope's limited if the area of affected node is small that is local or remote area and extended attack if large area of node is affected.

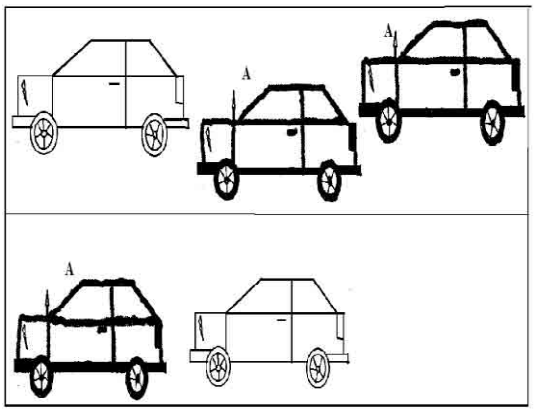


Fig2. Sybil Attack

2) Message Suppression Attack

In this, attacker selectively dropping packets from the network which may contain the critical information for the receiver, the attacker suppress these packets and can use them again in other time. For example an attacker might remove the congestion alter, and use it at another time so vehicle are prevented to select an alternative path to reach the destination and force them to wait in the traffic. The main objectives of the attacker to prevent the authorities and RSU to knew about the collision.

3) Reply Attack

This attack is used by the malicious user, who has the ability to capture the generated frame. As the name suggests, the attack happens when an attacker reply the transmission of previously generated frames in new connection. Malicious uses the previously generated frame in any other part of the network. Currently, we don't have any protection against this attack as it does not contain sequence and time stamp.

The main goal of this attack is to confuse the authorities and prevent the identification of vehicles in hit-and-run incidents.

4) Node Impersonation Attack

In VANET network, each vehicle has a unique identity that is id and with the help of this id vehicle is identified in the network. It becomes the most important in case of accident. In this attack, an attacker changes his/her identity and act like a real originator of the messages. The attacker receives the message from the originator and change the contents according to his/her benefits and then send the message to another vehicle.

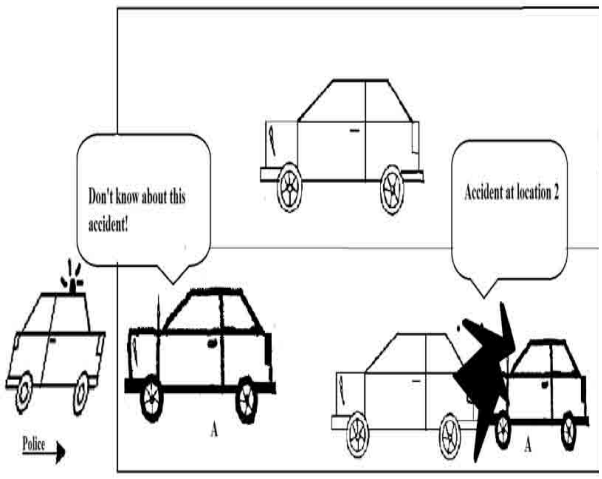


Fig3. Node Impersonation Attack

5) Tunnel Attack

In tunnel, GPS signals are disappear. An attacker may exploit this temporary loss of information and inject the false data once the vehicle leaves the tunnel and before it receive the updated information. In this example, the physical tunnel is replaced by an area jammed by the attacker, which result in the same effect.

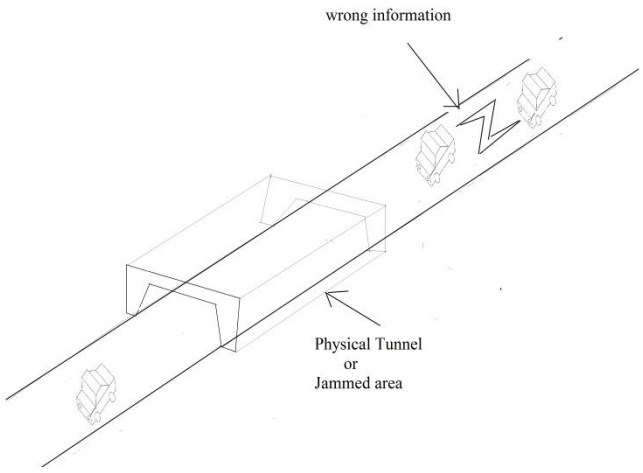


Fig4. Tunnel Attack

6) GPS Spoofing

The identity and the geographical location of all the vehicle is maintain on the network location table in GPS satellite. GPS satellite simulator is used by the attacker to generate the signals which are more powerful than the original signals. With the help of simulator, the attacker produces the bogus GPS reading to fool the vehicle it thinks that they are in different location.

7) Denial Of Service Attack (DOS)

This attack happens when the attacker take the control of all the vehicular resources and jam the communication channel of VANET network so that no authentic vehicle an access it. It is a very serious problem for the user to communicate in the network and prevents critical information to pass other vehicle. This problem put the driver in danger; if he is totally depend upon the application's information. Three different ways through attacker can achieve it-:

a) In the basic level, the attacker overwhelm the node resources so that it cannot perform other necessary tasks which results the node become busy continuously and not do anything else.
b) In extended level, the attacker jam the communication channel by generating high frequency so no vehicle can able to communicate with another vehicle.
c) Drop the packets

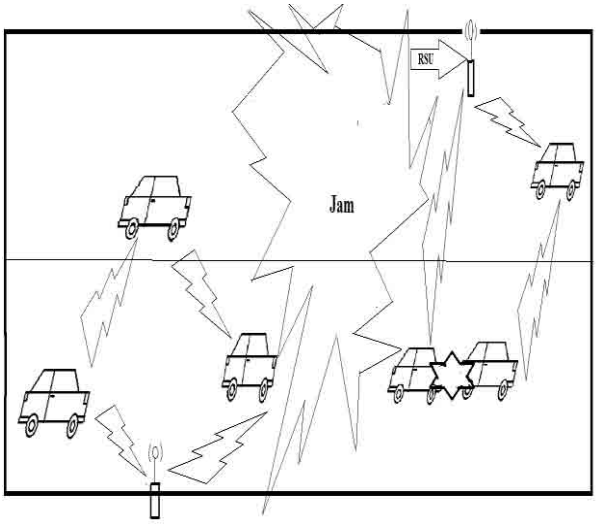


fig5. DOS Attack

8) Spamming

Attacker sends the spam messages to consume the bandwidth of network and to increase the transmission latency. This kind of message is difficult to control, due to lack of necessary infrastructure and centralized administration. Attacker can send spam messages to group of users. These messages are just like the advertisement messages and not concerned to the user.

9) Black Hole Attack

In black hole attack, node refuses to participate in the network or when an established node drops out. When the node is dropped out, all routes it participated are broken down leading to a failure to propagate messages.

10) Malware Attack

Malware attack is like a virus or worms in the VANET network which cause serious disruption to the operation. This attack injected in the VANET network when software is updated in VANET unit and RSU. This attack is carried out by a rogue insider rather than the outsider.

IV. SECURITY REQUIREMENTS

In order to make the vehicular network secure, the number of security requirements must be required. Some of the security requirements are same for all the networks and some are valid and specific only for the vehicular network.

1) Authentication

Network node must be authenticated to send messages through the network. A vehicle must verify the legitimacy of the message and sender before reacting on the messages and events. Without authentication, illegitimate and malicious user injected false messages in the network and make confusion in other vehicles by distributing false message. With authentication, nodes can simply drop the message from the unauthenticated user.

2) Authorization

Authorization is the highest level of implementation to access the control which itself is defined by the network policies. Authorization define the role of node which specifies the type of messages that the node can read or write on the network, it allow the action to be taken and generally the protocol that it can execute.

3) Data Verification

A regular verification of message is required to eliminate the false messages before the user react on it.

4) Confidentiality

To protect the privacy of each driver, the message should be encrypted to prevent the outside gaining the driver information.

5) Integrity

All the messages that are sends and received on the network must be protected from alternation attack. A network is secure if it provides protection against message alternation. There are number of ways which are used to alter the message during its transmission from source to destination and all possible attack must be considered.

6) Non-Repudiation

Non-repudiation has the ability to identify the attacker even after the attack happens. This is used to prevent the cheater to deny from their crimes. Any type of information related to the car like: the trip rout, speed, time, any violation will stored in the device called TPD (Tamper Proof Device).

7) Privacy

Privacy of driver is the important issue in vehicular communication. Drivers don't want that his personal and private information is accessed by the other user. Since the vehicle information like location, speed, time, and car data are transmitted through wireless communication, there should not possible to get driver identity from this information. The privacy must be achieved by

using temporary key. These keys will change frequently. Each key is expired after using only one time. The information of all key are stored in TPD (Tamper Proof Device) and will be reloaded again for the official check-up.

Table1. Security Requirements for each VANET Setting

VANET setting Sec. Requirement	V2V Warning Propagation	V2V Group Comm..	I2V Warning	V2I Warning
Entity Identification	Yes (all vehicles)	No	Yes (sender)	Yes
Entity Authentication	Yes (sender)	no	Yes (sender)	Yes (sender & Receiver)
Attribute Authentication	No	Yes (sender & Receiver)	No	No
Privacy Preservation	Yes	Yes	No	Yes
Non-Repudiation	Yes (sender)	No	Yes (sender & receiver)	Yes (sender & receiver)
Confidentiality	No	Yes	No	No
Data Trust	Yes	Yes	Yes	Yes

Table1 specifies the identified security requirements for VANET. I2v and V2V considered the same setting and have the different security requirement, so they have been distinguished here. Entity Identification specifies the each participated entity has different and unique identifier. However, identification does not mean that the entity proves that it is its actual identity- this is called as Entity Authentication requirement. V2V Warning Propagation required the identification of entity for message routing and forwarding, so identifiers are essential to build the routing table. In Group Communication, there is not required to identify or authenticate the communication peers. There is a need that both the participated entities become group members by using required attributes which is known as attribute authentication requirement. This requirement is only used in communication pattern. I2V warning required the both identification and authentication to send only the messages through infrastructure. Identification and authentication is not used by the receiver because infrastructure warning sends the messages to all the passing vehicles in the area. On the contrary, V2I warning required the emitting vehicles to be identified and authenticated. In this way, vehicles are trustworthy identity will be able to send such messages.

Privacy preservation is critical for vehicles because of two reasons, first vehicles actions should not be traced and second it is impossible for the unauthorized entity to link vehicle's identity with that of its driver. This requirement is present in all V2V communication and does not present in I2V warning because privacy is not used by the sender.

Non- Repudiation requirement means that entity is not able to deny after sending and receiving the messages. It is used by the sender in V2v warning. It is also used in I2V and V2I warning.

Confidentiality requirement is used to assure that message will only read by the authorized parties. This type of security requirement is only used in the group communication because only group members are allowed to read such information.

Data trust globally refers to the data integrity and accuracy which must be assured in the related information. At the stake, data should not be altered and it should be truthful. The receiver must be receives the fresh information. False and modified data should lead to the potential crashes and other safety problems of traffic. Because of this reason, data trust must be providing to all the VANET communication.

V. CONCLUSION

In future, users want safety and security on the roads and it become possible by implementing secure and safe VANET application with new technology. This technology is a fertile region for attacker who will try to change the contents of safe and non-safe applications to misguide the users of the network with their malicious attack. In this paper we present some possible attacks and their solutions. In the future work we want to expand our idea with their malicious attack. In this paper we present some possible attacks and their solutions. In the future work we want to expand our idea about the critical attacks and verifying it through simulation.

VI. REFERENCES

[1] Anderson R, Kuhn M. Tamper resistence- a cautionary note.In: Proceedings of the

second Usenix workshop on electronic commerce; November 1996.

[2] A. Fonseca, T. Vazao, applicability of position-based routing for VANET in highways and urban environment, j.Netw.Comput.Appl.36 (3) (2013) 961-973.

[3] Dietzel S, Schoch E, Konigs B,Weber M, Kerl F. Resilient secure aggregation for vehicular network. IEEE Network 2010; 24(1):26-31.

[4] Kumar Manish, et.al, "security challenges, issues and their network security", "*International Journal Of Network Security And its Application (IJMSA)",* vol-5, September 2013, pp. 95-105.

[5] Locert C., Scheuermann B., Mauve M., 2010. A probabilistic method for cooperative hierarchical aggregation of data in VANET s, AdHoc network, *journal of Vehicular Networks*, 8(5), p.518-30

[6] Mohanty Sagarika, Jeva Debasish, " secure data aggregation in vehicular-ad hoc network: a survey", "2nd International Conference Of Communication, Computing And Security (ICCCS), 2012, pp.922-929.

[7] Molina-Gil J., Caballero-Gil P., caballero-Gil C., 2010. Data Aggregation for Information Authentication in VANETs, Information Assurance and Security Leeters1, p.47-52.

[8] N. Maslekar, j. Mouzna, H. Labiod, M. Pai, Modified C-DRIVE: clustering based on direction in vehicular environment, in: IEEE Intelligent Vehicles Symposium, vol.4, 2011, pp.845-850.

[9] N. Maslekar, M. Boussedra j. Mouzna, H. Labiod, A stable clustering algorithm for efficiency applicationin VANETs, in: &th International Conference on Wireless Communication and Mobile Computing, Istanbul. 2021, pp.1188-1193.

[10] Rawat Ajay, et.al, "VANET: security attacks and its possible solution", "*Journal Of Information And operations Management"*, vol-3, 2012, pp.301-304.

[11] R.Lind et.al, .The network vehicle. A glimpse into the future of mobile multimedia, IEEE Aerosp. Electron. syst. Mag., 1999.

[12] Rivas Antolino David et.al, "security on VANET: privacy, misbehaving nodes, false information and secure data aggregation", "*Journal of Network and Computer Application*", vol-34, 2011, pp.1942-1955.

[13] Sun Y, Lu R, Lin X, Shen X, Su J. A secure and efficient revocation scheme for anonymous vehicular communication, In: IEEE international conference on communication (ICC), 2010; May 2010, p.1-6.

[14] S.Al-sultan, M.Moath, Al-Doori, H. Al-Bayatti Ali, H. Zedan, A comprehensive survey on vehicular ad hoc network, j.Netw. Comput. Appl. 37(1) (2014) 380-392.

[15] Verma,M,&Huang,D., "SeGCom: Secure Group Communication in VANETs", " IEEE Consumer Communication and Networking Conference (CCNC)" Las Vegas,NY,USA:IEEE, 2009,pp.1-5.

[16] Wiedersheim B, Ma Z, Kargl f, Papadimitratos P. Privacy in inter-vehicular network: why simple pseudonym change is not enough. In: seventh inter-national conference on wireless on-demand network systems and services (WONS); 2010. P.176-83.

[17] Wu HT., Wi-Shuo L., Tung-Shih S., Wen-Shyong h., 2010. A novel RSU-based Message Authentication Scheme for VANET, Fifth International Conference on System and Network Communication, IEEE, p.111-116.

[18] W. Fan, y. Shi, S. Chen, L. Zou, A mobility metric based dynamic clustering algorithm (DCA) for VANETs, in: International Conference on Communication Technology and Application, Beijing, 2011, pp.752-756.

[19] Qi H., Suguo D., Dandan R., Haojin Z., 2010.SAS: A Secure Data Aggregation Scheme in Vehicular Sensing Network, Proceedings of IEEE ICC.

A comprehensive survey on routing protocols in Vehicular Ad hoc Networks

1Anshu Joshi, 2Ranjeet Kaur Sandhu
1 anshujoshi240@gmail.com, 2 er.ranjeetsandhu@gmail.com
1 Research Scholar, Dept. of CSE,DAV University , Jalandhar, Punjab
2 Assistant Professor, Dept. of CSE, DAV University, Jalandhar, Punjab

***Abstract*-VANET (Vehicular Ad-Hoc Networks) is an emerging area of research focusing on reliable and efficient communication among vehicles. The V2V communication and V2I communication needs to be addressed with efficient algorithms. Due to dynamic topology and high mobility patterns the information routing becomes difficult in VANET routing protocols. This paper provides a review of protocols classified into six classes based on the nature of routing of information. The main motive is to overcome the network overhead, latency and optimal path for routing of data by these protocols.**

Keywords*: VANET, V2V, AU, V2I,*

Topology-based, Routing Protocol

I INTRODUCTION

Vehicular Ad-hoc Network is communication among vehicles to solve the issue of security, efficient routing, privacy and Quality of service. VANET establishes communication among V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). In V2I communication, RSU and OBU play an important role. RSU (Road Side Units) plays a centralized role to control the activities related to vehicles. They aid in exchanging messages between the vehicles and also forward it to other RSU for making communication reliable and efficient. The RSU may also act as a centralized authority to provide authenticated environment for secure communication. An OBU is on board unit that is a wireless communication device to felicitate communication among vehicles and road side units. The vehicles are the mobile nodes within the network and they communicate with V2V process. Dedicated short range communication is a communication medium used for VANET that operates on 75 MHz spectrum band around 5.9 GHz allocated by US Federal Communications Commission for vehicle safety applications. RSU's communicate with OBU's via DSRC radio signals.

VANET is derived from MANET (Mobile Ad-Hoc network) but it exhibits some characteristics that differ from other mobile ad-hoc networks: High mobility, self-organization, distributed communication, mobility restrictions, frequent disconnected networks and limited battery power and storage capacity. These characteristics pose great challenge for developing efficient routing protocols. This paper discusses some routing protocols classifications and illustrates challenges and issues in VANET routing. The routing protocol sets up an efficient route for communication between mobile vehicles in case of VANET. So, the routing protocols developed for VANET can be classified in accordance with different aspects like Qos, techniques used, depending on routing information and routing strategies. On classifying VANET protocols in different categories. Fig.1 shows the mentioned classification.

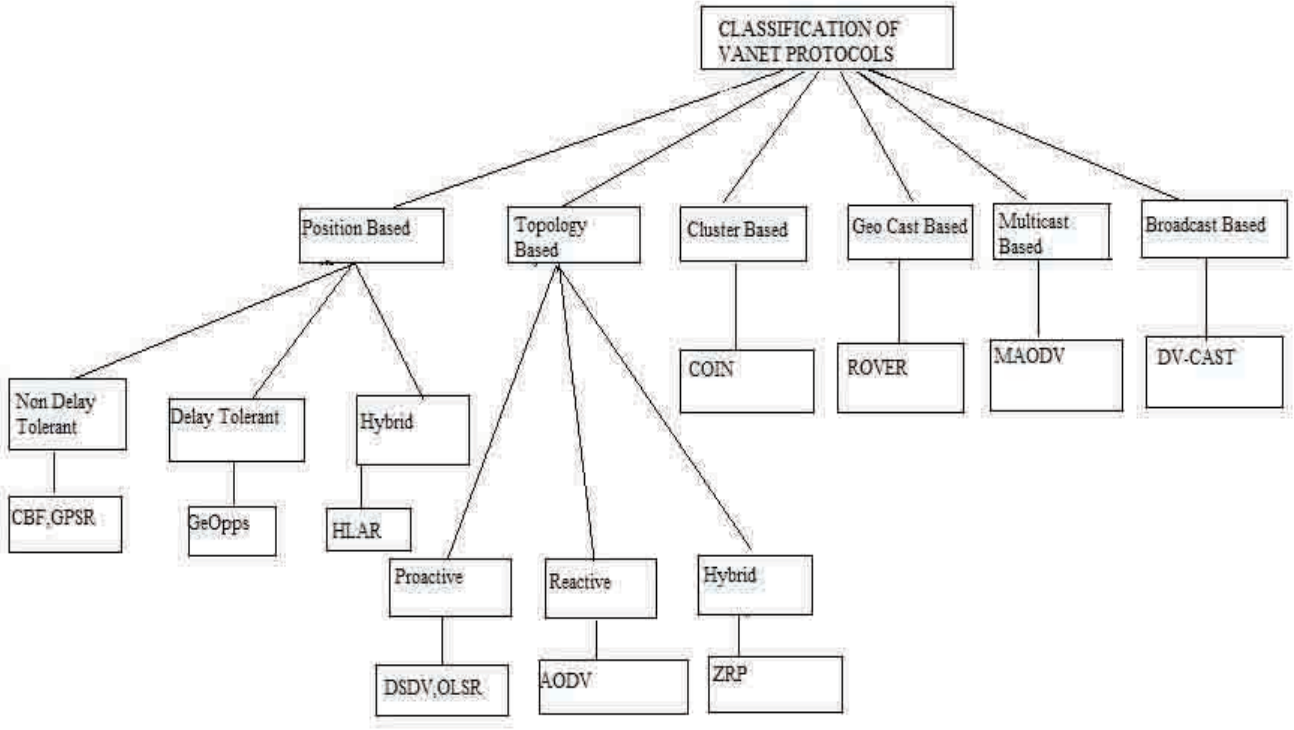


Fig.1 Classification of VANET Protocol

This paper discussed about the various protocols involved, architecture and issues associated with Vehicular Ad-hoc networks. The paper is divided into four sections. Section I is introduction, Section II discusses about the architecture of VANET, Section III discusses about topologies of VANET, Section IV deals with the Issues of VANET routing.

II ARCHITECTURE OF VANET

The main architecture of VANET is described in Fig.2 which describes the components in VANET.The V2V and V2I communication is done through these components . The Gateway present in the architecture provides a meduim to communicate among the RSU's and IEEE 802.11p. Fig.2 is a general overview of a VANET scenario in Urban Area.

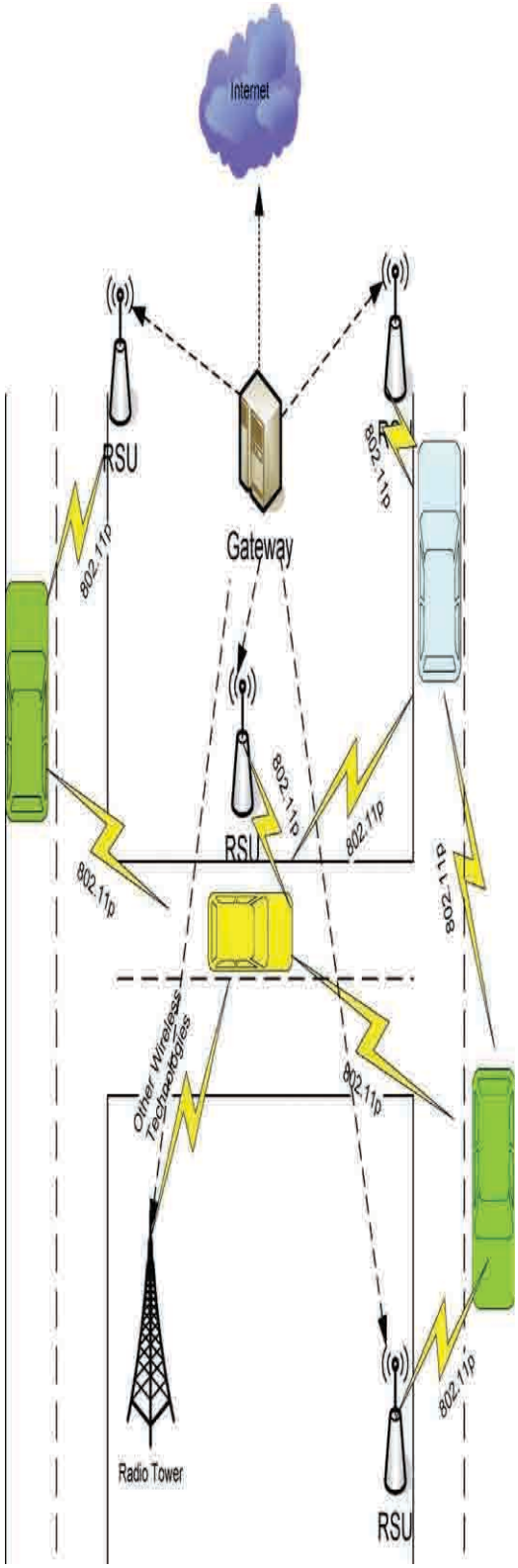


Fig. 2 Architecture of VANET

The Three main components of VANET according to the study are: Application Unit (AU), On board Unit (OBU) and Road side Unit (RSU). RSU acts an intelligent router which provides communication among vehicles by forwarding the messages from vehicle to vehicle, the vehicles which are in range of RSU's are able to communicate with each other through RSU's .RSU communicate via Dedicated short range communication(DSRC) with vehicles and with other RSU's and OBU's in architecture using IEEE 802.11p standard. RSU's are fixed components along the roadside. OBU's are On board units installed on the vehicles, they act as communication medium for communication among OBUS's or with Road side units. OBU's are also for communication with AU (Application Unit). The Application Units are basically used for safety applications and they are sometimes treated as integrated part of the OBU. The motive of routing in VANET is to provide security and efficient routing services to make users feel comfortable while they are travelling on road. An RSU is an intelligent router which provides services to OBUS's on Vehicles and AU's.

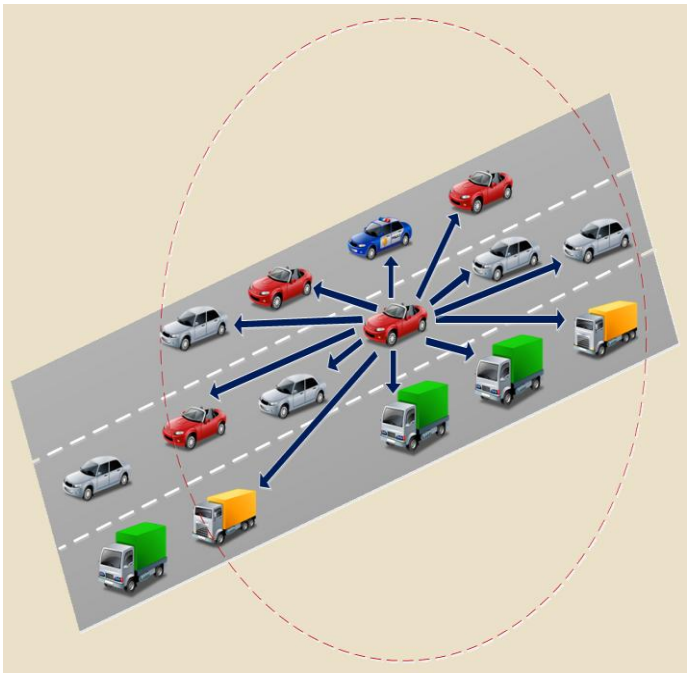


Fig 3. Simple VANET Network.

III ROUTING PROTOCOLS IN VANET

The routing protocols specified in the introduction are categorized into six categories: Position based, Topology based, and Geo-cast based, cluster based, broadcast and multicast based routing protocols.

A. Position based Routing

Position based routing protocol is based on positional information. In this case nodes come to know about their and neighbor's position using Geographic positioning system which aid in locating the nodes in geographic area. The node can identify other nodes if and only if the node is source nodes radio range. There is no requirement of route discovery and maintenance because in position based routing when the source needs to send a packet to the destination, source stores the address of the destination in the request packet header which helps in locating and forwarding the packet to destination. The position based protocols are further classified into three classes: Delay Tolerant Network (DTN) Protocols, Non Delay Protocols (Non DTN) and hybrid protocols.

1) Delay Tolerant network(DTN) protocols:

The DTN is a wireless network which involves mobile nodes which communicate with other nodes when they reach in transmission range of the node. DTN Protocols:

a) **Geographical Opportunistic routing (GeOpps):**

GeOpps uses store and forward technique but uses navigating system for packet transmission. The navigation system helps in collecting the geographical position information which aid in identifying the nodes which are in range of the source node and transfer those packets. The steps involved in the source to destination communication are:

Each neighboring node estimates the future

closest point to the destination to reach.
Every neighboring node calculates shortest

delay time to reach the destination node.

Using shortest time calculated by each neighbor node to reach destination and the shortest delay time taken by a node to reach the destination that node should be considered as the next hop carrier to transmit the packet to destination fast.

2) Non Delay Tolerant Network Protocols:

This geographic routing protocol uses nearest neighbor to forward the packet to the destination and in case if there is no nearest neighbor to the destination this approach may not be successful. There is no issue of dis-connectivity as there is available more number of nodes to achieve successful communication. The problem of nearest neighbor node to destination can be solved through routing strategies. GPSR and CBF are the Non Delay Protocols.

a) Greedy Perimeter Stateless Routing (GPSR):

In this protocol each node forwards the packet to the intermediate nodes which are nearest to the destination node constantly. This protocol follows approach of recording the first hop node's neighboring positions which aid in when there is no nearest node to the destination. The perimeter forwarding is done to decide to which node it delivers the packet so as it reaches to destination efficiently. This protocol is stateless routing protocol that utilizes greedy approach. GPSR could face link failure due to high mobility and frequent mobility pattern changes. This problem can be handled well by perimeter forwarding.

b) Contention based forwarding (CBF) :

CBF is not a beacon oriented protocol i.e. it saves the consumption of bandwidth. This transmits data packets to its neighbors and later identifies the node that will continue forwarding the packets. This node is selected using a distributed timer based contention and the rest nodes are suppressed to prevent forwarding the packets. Receivers compute and compare their distance with the destination to the last hops's distance with destination node. The more the computation results, shorter time to forward the packet.

3) Hybrid Position based routing

Position routing reduces the routing overhead and it does not focus on constructing and maintaining a routing table as it is location based protocol which fetches information about destination and source through geographical processing. Hybrid routing scheme includes characteristics of two or more position based routing protocols (non-DTN and DTN). This hybrid protocol was developed due to some limitations faced by position based routing

protocols:

Performance of position based routing decreases if position accuracy of source and

destination is not achieved.

This position based approach may fail if

node closer to the destination is not found.

This problem of nearest neighbor can be solved but it requires packet to travel large distance with loopy routes and may drop data packets. Hybrid approach is followed; protocol HLAR is example to this approach.

a) **Hybrid Location Based Ad-Hoc Routing**

protocol(HLAR) :

HLAR efficiently use all the available location information and to minimize the routing overhead. The interesting feature that this protocol shifts to on-demand routing whenit does not find sufficient location information . It works as reactive protocol in route discovery if there is no route to the destination then source adds his location information and location information about destination in route request packet and searches for nearest node, in case nearest node is found then packet is forwarded else request packet is flooded to all the neighbors. However HLAR minimizes routing overhead in comparison to on-demand routing protocols.

B. Topology Based Routing Protocol

Topolog y based routing protocol usually a traditional MANET routing protocol that utilizes information stored in a routing table for forwarding the packet to the destination node. The protocol can be classified in three classes: Proactive (Periodic/table driven), Reactive (On demand) and Hybrid protocols.

1. Proactive routing Protocols:

It uses routing table for forwarding the message packets from source to destination. The table stores the routing information for all other nodes, each entry in table contains the information about the next hop node used in the path to destination. The table is periodically updated with route information and should be broadcasted to all the neighbors. It may cause overhead problems in high mobility area.

a) Destination sequence Distance vector

routing(DSDV):

DSDV uses shortest path algorithm to implement only one route to destination which stored in routing table, a routing table contains information about all accessible nodes, as well as the total number of hops needed to reach these nodes and a sequence number is assigned to all the nodesinitiated by the destination. DSDV uses loop free routes reduces overhead and uses optimal route to every node. If large network is considered then it causes overhead reason being unnecessary updates in table even if there is no change in the toplology.DSDV does not provide multi routes to the destination but it periodically updates routing table to its neighbor. It utilizes single node link nearest to the destination.

b) Optimized Link State Routing(OLSR):

It implements link state strategy; it keeps a routing table which stores the information about the routes to nodes available in the network but if topology changes then each node must send its updated information to some selective nodes further these selective nodes transmit to other selective nodes used in communication. It is suitable for dynamic topology and better for applications that require low latency in the data transmission. OLSR causes congestion due to generation of packets to handle the topology changes. Advancement to OLSR is HOLSR (Hierarchical optimized link state routing protocol which decrease the overhead in large size networks.

2. Reactive routing Protocol

This is on- demand routing protocol that reduces network overhead by maintaining routes only when required. If there is no route available then source node floods route discovery process until destination is found and if message reaches destination then route reply back to source

node using unicast communication.

a) Ad-Hoc On-Demand Distance

Vector(AODV)

AODV uses RREQ, RREP and RREP packets for communications as thisalgorithm is on-demand based algorithm. When there is no path available then route discovery process starts until an intermediate node to the destination is found or the destination node is found. The route request packets follow the route to destination whereas route reply packet is reply from destination to setup a path from source to destination. RERR packet tells whether all the nodes in the link are connected or there is some breakage. AODV as compared to other proactive routing algorithms offers low network overhead by reducing messages flooding in the network and minimizes the routing table overhead only keeping active connections. It has loop free routes with use of sequence numbers. AODV is flexible to highly dynamic network topology and large scale network. The disadvantage or drawback

to AODV is a route failure causes a new route discovery process which decreases data transmission rate and increase in the network overhead.

3. Hybrid Routing protocol :

It is mixture of proactive and reactive protocols. With aim to minimize the control overhead caused in proactive routing protocols and delay in route discovery process in reactive protocols.

a) Zone Routing Protocol(ZRP)

In ZRP a network node divides the network into zones. ZRP uses reactive routing protocol for outside zones and proactive protocol for inside zones. Inside zone uses cache table to forward the packet to destination without delay. For outside zone, ZRP uses reactive routing to discover a route, the route request is sent to the border nodes of routing zone; the packet includes a unique sequence number, the source address and
destination address. The border node responds back to the route request packet by looking for destination inside the zone. If destination is found, it send route reply on reverse path to source node, if not able to find the destination node locally then border node adds its address in the packet and forwards to its own border nodes. Later the sources stores the path whether locally or outside to be used in data transmission to the destination.

C. Cluster based routing protocol

This protocol divides the network into clusters where nodes in the clusters possess same characteristics like they have same direction, velocity. Each cluster has cluster head that has focus on to manage communication process inside. The nodes inside the cluster can communicate with other nodes via cluster head. And this creates virtual infrastructure for networks.

1. Clustering For Open IVC Network

It is a clustering protocol focused on to improve the network scalability. Clusters are formed based on three parameters: mobility of nodes, nodes positions and behavior of nodes. Each cluster has time to live thus decreases control overhead. Inter vehicle communication system stabilizes the distance between the cluster member nodes and the cluster head node which communicates with other nodes outside the cluster. This purpose is solved by maintaining some characteristics such as mobility of node should be low to maintain the long communication among nodes.

D. Multicast routing Protocol

Multicast routing provides multiple paths from a source to destination in case a single path fails other path continues with the communication reducing route discoverytransmission. It stores multi paths to destination using single route discovery process. A new route discovery is required if all routes in multipath scenario fails. This enhancement causes low overhead due to frequent route discovery transmission by discovering multiple paths which decreases chance of retransmission. It also does not increase the delay in route discovery process.

1. **Ad-Hoc On demand Multipath distance**

Vector routing Protocol(AOMDV) :

AOMDV protocol is a multi path on-demand protocol that is extension to AODV; it discovers multiple paths from source to destination so in case of any single route failure other routes may become active. This strategy reduces the overhead of network due to no retransmissions of the route request. A single route discovery mechanism is used for multiple paths which causes uninterrupted communications for the packet transmission and provide lower overhead. AOMDV keeps all available paths in routing table and then shortest path among those paths are chosen for communication.

E. Broadcast Based Routing Protocol

The broadcast routing enables packets to flood into the network to all available nodes inside the broadcast domain. This routing allows packets to deliver via many nodes which may achieve a reliable packet transmission.

1. Distributed Vehicular Broadcast Protocol

(DV-CAST)

DV_ CAST is a broadcast routing that uses multi hop scheme. In this protocol, each node monitors the status of its neighbor nodes connectivity to them. It uses concept of beacon messaging to get information about the network topology. In a connected strategy the node can be rebroadcast along the nodes movingin the same way. In disconnected source node uses store and forward strategy if the node found the neighbor node in broadcast range then it forwards the packet stored else if the node could not found the neighbor among the broadcast region then the node discards the packet after some time to live for the packet. This protocol minimizes broadcasting overhead.

F. Geo Cast Based Routing Protocol

Geo cast belongs to multicast protocols which are based on sending packets from a source to a group of destinations. This protocol enables a single

source to communicate or send packets to other vehicles located in specific geographical area which is labeled zone of relevance (ZOR). The node if is in same geographic area are member of ZOR group if they move out of that group their membership changes and they drop packets when they move out of one ZOR group. Zone of forwarding is responsible for forwarding packets to other ZOR vehicles belonging to other ZOR groups . They attain reliable packet delivery in dynamic topology.

1. Robust Vehicular Routing(ROVER)

It permits each vehicle to deliver packets to vehicles which are inside a specific ZOR. It is similar to AODV uses on demand routing. It floods only control packets in the network and does unicast routing. The source node floods route request to its ZOR this packet includes unique source ID, its location, its recent ZOR and a sequence number assigned to the route. If the packet lies inside the ZOR and zone of forwarding then only it can reply with ID to one hop neighbor and records the routing information in routing table, else if it

does not lie then it cannot reply.
ROVER is different to AODV as it sends route request packet not to the source node but to the node that forwarded it the packet.

IV ISSUES IN VANET ROUTING

VANET face various challenges being among the most researched topics. It has high dynamic nature of topology and high in mobility pattern. Some of the open issues and challenges being faced by the VANET routing are described in this section. Listing some of the challenges and issues:

A. Dynamic topology and High Mobility

Vehicles are the mobile nodes in VANET and move according to road pathway which restricts mobility. Thus causes disruption in communication among the nodes due to varying topology and road pathway restriction. A solution to effective data dissemination is broadcast the packets among the nodes.

B. Fault Tolerance

VANET being a fast changing topology, several vehicles could enter and leave the network periodically. If during the communication a single node leaves the network then the route should be created by routing protocols immediately to avoid any route failure in absence of the node.

C. Security

This is the most important challenge issue in VANET. If no security is provided in routing protocols, a malicious node can enter the network and cause disruption in communication or may cause link failure which could in turn cause road accidents. So to protect the information from being trapped by malicious nodes authentication, integrity and non-repudiation must be achieved

CONCLUSION AND FUTURE WORK

VANET is a wide area of research. Routing, security and Quality of service are current issues that need coverage in research. Routing protocols discussed in the paper are general overview of various categories of protocols in VANET. The VANET has dynamic topology and high mobility patterns which has made designing of a VANET scenario a bit challenging. Using efficient algorithms which could aid in various challenges faced in routing could be solution for a better VANET scenario to felicitate communication among the V2V and

V2I.

The Future work focuses on addressing the challenges in VANET as mentioned.

REFERENCES

[1] Baozhu Li, Yue Liu and Guoxin Chu, ”Improved AODV Routing Protocol for vehicular ad-hoc networks”,2010, International conference
on Advanced Computer Theory and Engineering. [2] H. Yoo, D. Kim, “Repetition-based

cooperative broadcasting for vehicular ad-hoc networks”, comput. Commun.34(5) (2011) 1870-
1882.

[3] S.sultan, M.Doori, A. Bayatti,H.Zedan,”A comprehensive survey on vehicular ad hoc
networks, J.Netw, comput appl(2013)

[4]J. Toutouh, J.G Nieto, E. Alba, “Intelligent OLSR routing protocol optimization for VANET”,IEEE Trans. Veh.technol. 61(4)(2012)
1884-1894.

[5]V.Naumov, T.R Gross, “Connectivity Aware Routing(CAR) in vehicular ad hoc networks”, in: Proceedings of 26th IEEE International Conference on computer communications, INFOCOM 2007,Anchorage,Alaska,USA,May2007.

[6]P1609.0/D5, Sep 2012-IEEE draft guide for wireless Access in vehicular Environments(WAVE),http://ieeexplore.ieee.org/servlet/opac?punumber=6320593,2012,pp-1-74.

[7]M. Bakhouya, J. gaber, P.lorenz,"An adaptive approach for informationdisseminationin vehicular ad hoc networks, J.Netw comput 34(6)
(2011) 1971-1978.

[8] Amit Dua, Neeraj Kumar,Seema Bawa,"A systematic review on routing protocols forvehicular Ad hoc Networks, Vehicular communications 1 (2014) 33-52.

[9]Baara T. Sharef, Raed A. Alsaqour, Mahamod Ismail,"Vehicular communication ad hoc routing protocols" ,journal of network and computer applications 40(2014) 363-396.

Mobile Ad-Hoc Networks Characteristics, & Applications: A Review

Aneet Kaur[1], Anu Sheetal[2]
[1,2]Department of Electronics and Communication Engineering
Regional Campus, Gurdaspur
Email: [1]aneetkaur_ece_892609@yahoo.com,[2]anusheetal2013@gmail.com

***Abstract*- Revolution in the field of Mobile Ad Hoc Network (MANET) came with many research areas. In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. Security in mobile ADHOC network is a big challenge as it has no centralized authority which can supervise the individual nodes operating in the network. The attacks can come from both inside the network and from the outside. MANETs are susceptible to a variety of attacks such as active and passive attack. This situation may be precarious for confidential communication. In this paper, we are going to discuss MANET characteristics, structure, applications different types of attacks that can harm MANET and degrade network performance.**

***Keyword*–**MANET, Routing, Active and Passive Attacks

I. Introduction

A mobile ad hoc network (MANET) is generally defined as a network that has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. Mobile Ad-hoc Network is formed by a group of wireless nodes having no fixed infrastructure. These nodes are free to move anywhere, anytime according to need. That means they change their topologies very frequently [1]. Sometimes, these nodes act as a router as well to forward packets. Even, they can communicate easily with each other though there is no strictly define fixed structure or any centralized authority. MANETs are more popular than wired networks [1]. But due to mobility of nodes and dynamic topology, MANETs are more vulnerable to attacks. Therefore, security issues are more challenging in MANETs as compare to wired networks. Therefore, it is difficult to achieve security goals such as Authentication, Integrity, availability and Confidentiality. Also, ad hoc networks do not need to operate in a standalone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity [2,3].As a consequence, mobile ad hoc networks are expected to become an important part of the future 4G architecture, which aims to provide pervasive computer environments that support users in accomplishing their tasks, accessing information and communicating anytime, anywhere and from any device.

Some examples of MANET are as follow:

- In Classroom: Ad hoc network between student PDAs and workstation of the instructor.
- Large IT campus: Employees of a company moving within a large campus with PDAs, laptops, and cell phones.
- Moving soldiers with wearable computers: Eavesdropping, and impersonation attacks can be launched.
- Shopping mall, restaurant, coffee shops: Customers spend part of the day in a networked mall of specialty shops, coffee shops, and restaurants.

II. Security goals of MANET

In MANET, nodes within each other's wireless transmission ranges can communicate directly, however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism [5,7]. These mechanisms are used to prevent, detect and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

A. Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

B. Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

C. Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

D. Integrity: Message being transmitted is never altered.

E. Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

III. Characteristic features

MANET has many characteristic features that distinguish it from cellular and wired networks [2,6,8]. The specific characteristics and complexities, which are summarized below, they impose many design challenges to the network protocols. In addition, these networks are faced with the traditional problems inherent to wireless communications such as lower reliability than wired media, limited physical security, time varying channels, interference, etc. Various characteristics of MANET are as follow:

A. Dynamic topologies: Network topology may change dynamically as the nodes are free to move.

B. Bandwidth-constrained, variable capacity link*:* Realized throughput of wireless communication is less than the radio's maximum transmission rate. Collision occurs frequently.

C. Energy-constrained operation: Some nodes in the ad hoc network may rely on batteries or other exhaustible means for their energy.

D. Limited physical security: More prone to physical security threats than fixed cable networks.

E. Self-creation, self-organization and self-administration: Ad hoc networks can be rapidly deployed with minimum user intervention. There is no need for detailed planning of base station installation or wiring. Also, ad hoc networks do not need to operate in a stand-alone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users.

F. Network scalability: MANET is a highly scalable network. It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. Wireless ad hoc network can be build up where there is no support of wireless access or wired backbone is not feasible. All network services of ad hoc network are configured and created on the fly.

IV. Routing

In MANETs, there is different area in which research is going on like bandwidth utilization, power consumption; routing etc. but routing area is taking great importance by researcher because sometimes we have a confidential data to send between devices. Therefore, routing ensures secure data transmission between devices. In this paper, we are here to discuss about different types of attacks that can harm our confidential information during communication. At present, there are three types of routing protocols present in MANETs. First is Proactive, second is Reactive and Hybrid. In proactive routing protocols, it maintains table at node level [6]. Because of this, they provide fast responses to topology changes by maintaining routing information for all network destinations and react to changes in the network. The examples of proactive routing protocols are OLSR and DSDV.On the other hand, reactive routing protocols provide routing information on demand basis and they rely on frequent change in topologies. As compared to proactive, reactive routing protocols take more time in establishing communication path. The examples of reactive routing protocols are AODV and DSR. Hybrid protocols take the advantages of both proactive and reactive protocols. The example of hybrid protocols is ZRP.

V. Attacks in MANET

Due to mobility in nature, mobile ad hoc networks are highly susceptible to different attacks. Those who performed these attacks are called attacker. Sometimes if a node performs one of attacks is called malicious node. If we talk about domain or terrain, these Attacks are divided into two groups, first internal attack and second external attack. In Internal attack, an attacker captures a node to gain access to encrypt and authenticate keys. This type of attack can be start by a compromised node that fit in to the network. This compromised node will ready to forward data packets but not allow doing so because the compromised node might be overloaded, selfish or broken. An overloaded node lacks CPU cycles, buffer space or available network bandwidth to forward packets [1]. In external attack, Attackers assume that there is no knowledge of keys is required to encrypt the data. These attacks are called external attack because attacker node does not belong to the network. These attacks may involve in transmission of false routing information or bogus data packet, generation of routing loops, partitioning of the network and congestion [2].

In these attacks, attacker can work with the collaboration of compromised nodes that belong to network. Therefore they can make routing loops or many other false routes to disrupt the normal transmission. Out of both attacks, internal attacks are more dangerous than external attack because malicious node will be the part of selected route. If we see the behavior of attack, attacks can be categorized as passive attack and active attack. In passive attack, malicious nodes involve in eavesdropping of transmitted data. This gathered information can further used for malicious deeds by attacker. In this, attacker does not disrupt the normal transmission but try to discover valuable information by listening to the routing transmission. It is very difficult to guard against such types of attack. If we are using wireless environment, it is

almost impossible to spot Eavesdropping. Gathered valuable information can expose their IP addresses and connections between nodes or we can say over structure of the network. Sometimes, it is seen that if a path to a meticulous node is asked for more often to other nodes, the attacker will be able to guess that the node is important for the network and removing it could bring the entire network down [3, 4, 5]. Active attack has totally different qualities than passive attack.

On the other hand, in active attack, attacker involve in alter information to disrupt the normal transmission of the network. Attacker can alter data packets, change route to wrongly forward data packet to wrong node. To implement active attack, malicious node must be part of network [6, 7]. Now, we want to combine passive attack, active attack with internal and external attack. Therefore, we can say that internal and external attack can belong to active attack only [1].

VI. Passive Attacks in MANETS

In passive attack, malicious nodes involve in eavesdropping of transmitted data. This gathered information can further used for malicious deeds by attacker. In this, attacker does not disrupt the normal transmission but try to discover valuable information by listening to the routing transmission. It is very difficult to guard against such types of attack. If we are using wireless environment, it is almost impossible to spot eavesdropping.

Gathered valuable information can expose their IP addresses and connections between nodes or we can say over structure of the network. Sometimes, it is seen that if a path to a meticulous node is asked for more often to other nodes, the attacker will be able to guess that the node is important for the network and removing it could bring the entire network down. There are different types of passive attacks present in MANETs:

Traffic Analysis: This attack is network based attack. In this, attacker only observes patterns of data packets. There is no need to compromise a legitimate node or break encrypted data packet. During transmission, encrypted message can show a lot of analysis communication pattern. This can enable malicious node to harm network [8, 13].

Monitor and Eavesdropping- In this, attacker snoop the number of data packets during data transmission. The motive is to know the communication contents. Most of the time malicious nodes are intended to grasp control information about network [9].

Camouflage Adversaries- In this, attacker can add malicious node in the network or compromise the nodes resided in the network. They try to have the properties of the legitimate node in the network [8]. Attacker hides its real IP address or MAC addresses and takes IP address of member of the network [10].

Selfish Node Behaviour - in this, malicious nodes drop packets with a self-centred inspiration to prioritize its traffic [11]. These passive attacks can also be used to launch active attacks that can make havoc in the network.

VII. Active Attacks in MANET

On the other hand, active attacks are those who disrupt the normal operation of the network. They can modify the sending message, inject the invalid messages, make the loop with the collaboration of other nodes, flood the channel, replicate and deletion of exchanged data so that routing procedure can be confuse. All these can be responsible for degrading the network performance [12]. Active attacks include dropping attacks, replay attacks, collusion attacks, and tampering attacks [13].

Different types of active attacks are as:

Wormhole or Tunneling: This attack takes place when a malicious node present in a network makes a tunnel with a malicious node present in another network. By using this tunnel, attackers can drop packets to the different network, change the direction of transmission, make confusion for shortest route etc. This attack will only occur with the collaboration of more than one malicious node [14]. The tunnel is created either using a wired link or by having a long range high bandwidth wireless link operating at a different frequency band.

Spoofing or Impersonation: In this attack, the attacker steals access rights of authorized users. An attacker may hack the credential's information to imitate the legitimate node [15]. By doing so, attacker examine, modify and include data in the hi-jacked communication.

Packet Dropping Attacks: In this attack, attacker discards route error packets leading legitimate nodes to forward packets in broken links [14].

Flooding Attack: The malicious node broadcasts forged Route Request packets randomly to all nodes every 100 ms in order to overload the network [15].

Black Hole Attack: In this attack, when transmission is initiated by source, a malicious node advertises that it has the shortest path to any other nodes of the network to attract all packets sent by the source node. As soon as, malicious node receives packets towards other nodes, it drops all the packets instead of forwarding to the final destination [13].

Forging Attack: A malicious node modifies and broadcasts to the victim node route error packets leading to repeated link features [15].

Fabrication: Instead of modifying the existing routing packets in the network, malicious node generates the incorrect information about the route between devices [15].

Modification: in this attack, attacker not only hi-jack the data packets but also do some modification in data packet before forwarding the packet to another nodes in the network. By doing so, attacker confuse the transmission [15].

Denial of Service (DOS): the aim of the attacker is to consume bandwidth by injecting a large number of fake packets like route request. So that network can be flooded with these wasteful packets to prevent channel access to authorized users [13].

Selective Forwarding Attack: for attracting more traffic, malicious node can either selectively drop the received data or collect sensitive information. Attacker makes believe that all nodes in the network are reliable to forward data packets. After receiving packets, attacker drops certain packets instead of forwarding every message. This attack can make havoc in network if malicious node is closer to source node or destination node, attacker can attract most of the traffic. Another thing that can make network paralyzed, if attacker drops more packets and forwards less [11, 14].

VIII. Applications

MANET provides various services to various users some of them are listed as below:

Tactical networks: MANET provides various tactical network services thus possible scenarios/services provided by this are in Military communication and operations and in Auto-mated battlefields.

Emergency services: MANET provides various emergency services such as thus possible scenarios/services are Search and rescue operations, Disaster recovery, Replacement of fixed infrastructure in case of environmental disasters, Policing and fire fighting, Supporting doctors and nurses in hospitals.

Commercial and civilian: MANET provides various commercial and civilian services such as E-commerce: electronic payments anytime and anywhere Environments, Business: dynamic database access, mobile offices, Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks, Sports stadiums, trade fairs, shopping malls, Networks of visitors at airports and etc.

Home and enterprise**:** MANET provides various services for home and enterprise such as Home/office wireless networking, Conferences, meeting rooms Personal area networks (PAN), Personal networks (PN), Networks at construction sites networking.

Education: MANET provides various services in feild of education such as Universities and campus settings, Virtual classrooms, Ad hoc communications during meetings or lectures.

Entertainment: MANET provides various services in field of entertainment such as multi-user games Wireless P2P networking, Outdoor Internet access, Robotic pets, Theme parks etc.

Coverage extension: MANET provides various services in field of coverage extension such as Extending cellular network access, Linking up with the Internet, intranets, etc.

XI. Benefits of MANET

- Multi-hop ad-hoc networks can reduce the power consumption of wireless devices. More transmission power is required for sending a signal over any distance in one long hop than in multiple shorter hops.
- Self-creating network, Self-organizing network, Self-administering wireless network.
- Intrinsic flexibility
- Reduced interference levels, increases spectrum reuse efficiency, and makes it possible to use unlicensed unregulated frequency bands
- No expensive infrastructure must be installed
- Use of unlicensed frequency spectrum
- Quick distribution of information around sender
- Use of ad-hoc networks can increase mobility and flexibility, as ad-hoc networks can be brought up and torn down in a very short time.
- Ad-hoc networks can be more economical in some cases, as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes.
- Because of multi-hop support in ad-hoc networks, communication beyond the Line of Sight (LOS) is possible at high frequencies.

X. Conclusion

The rapid evolution in the field of mobile computing is driving a new alternative way for mobile communication, in which mobile devices form a ad hoc network. Its intrinsic flexibility, lack of infrastructure, ease of deployment, auto-

configuration, low cost and potential applications make it an essential part of future pervasive computing environments. As a consequence, the seamless integration of mobile ad hoc networks with other wireless networks and fixed infrastructures will be an essential part of the evolution towards future fourth generation communication networks. In this survey paper, we tried to inspect the security threats in the mobile ad-hoc networks, which may be a main disturbance to the operation of it. As a result, the security needs in the MANET are much higher than those in the traditional wired networks.

References

[1] Basagni, S., Conti, M., Giordano S., and Stojmenovic,I. Ad Hoc Networking. IEEE Press Wiley,New York,Vol.1, No.2, 2003.

[2] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, Vol.1 No.8, pp. 13–64, 2010.

[3] Freebersyser, J. A., and Leiner, B. A DoD perspective on mobile ad hoc networks. In: Perkins, C. (Ed.) Ad Hoc Networking, Addison Wesley, Reading, Vol.2, No.3, pp. 29–51, 2009.

[4] Corson, S., and Macker, J. Mobile Ad hoc.Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC-2501, IETF,Vol.1, No.2, 1999.

[5] Abolhasan, M., Wysocki, T., and Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, Vol. 2, No.1, pp. 1–22, 2004

[6] Royer, E., and Toh, C. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, Vol.6, No.2, pp. 46–55, 2009.

[7] Hoebeke, J., Moerman, I., Dhoedt, B., and Demeester, P. Towards adaptive ad hoc network routing. International Journal of Wireless and Mobile Computing: Special Issue on 'Wireless Ad Hoc Networking', to be published.

[8] Kozat, U. C., and Tassiulas, L. Service discovery in mobile ad hoc networks: an overall perspective on architectural choices and network layer support issues. Ad Hoc Networks, Vol. 2, No.1, pp. 23–44, 2008.

[9] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Vol. 4, No.3, pp. 334-340, 2009.

[10] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science Vol.5, No. 6, pp. 22 - 24, 2008, San Francisco, USA.

[11] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.), Vol.1, No.8, pp. 23-34,@2006 Springer.

[12] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, Vol.9, No.8, August 2009.

[13] N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technology.

[14] V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks ," Journal of Computer Science Vol. 4, No.3, pp. 245-251, 2008.

[15] Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06,Vol.1, No.2, pp.231-240, 2006.

Implementation Of MANET Network Using Various Routing Protocols

Harminder Singh[1] **Atul Mahajan[2]**

[1] Research Scholar, E.C.E. Department, A.C.E.T. Amritsar. E-mail: harmindersingh.ece@gmail.com

[2] Associate Professor, E.C.E. Department, A.C.E.T. Amritsar. E-mail: mahajan271@gmail.com

***Abstract* –** Mobile Ad Hoc Network i.e. MANET is a temporary, infrastructure less, self organized, multi hop network. In this the nodes(devices) are moving without any intermediate infrastructure. There are many parameters which are taken into consideration while research, that are routing protocols, power consumption, bandwidth utilization etc. For different network scenarios such as network size and topology there are different routing protocols which make it difficult to select a particular routing protocol. There are different strategies which claim to prove high efficiency and improved performance.This paper provides an overview of existing routing protocols with their introduction, characteristics and usability proposed in literature.

***Index Terms* –** MANET, Literature Review, Routing Protocols, Future Applications and Challenges.

I. INTRODUCTION

MANET is in research from 20 years due to its dynamic nature. It is characterized by low bandwidth and low power consumption due to absence of a centralized mechanism. All the nodes in this are moving i.e. a single node acts as a host and a router. This type of infrastructure less establishment is very usefull in situations like battlefields, emergency, natural disasters etc. It is a group of wireless moving nodes that transmit and receive directly without any connection to an intermediate device which means all nodes are having autonomous nature. For example, Basu et al.[1] advocate the vision of *power-up-n -play*, in which no predefined infrastructures are installed and, when powered up, the devices "intelligently" configure and connect themselves to other devices. Bhagwat et al.[2] also focus on the interoperability of sensor devices and present three research issues: (1) distributed algorithms for self-organizing devices, (2) packet forwarding, and (3) internet connectivity.

II. LITERATURE REVIEW

i. "Review of Various Routing Protocols for MANETs" by Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma published in International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011. In this developers of all reactive, proactive and hybrid routing protocols was named with the need to develop and upgrade the protocols.

ii. "A Novel Review on Routing Protocols in MANETs" by Robinpreet Kaur & Mritunjay Kumar Rai in Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012. In this a brief summary about all MANET's routing protocols was given with the difference between them on the basis of performance characteristics.

iii. "Implementation Experience with MANET Routing Protocols" by Kwan-Wu Chin, John Judge, Aidan Williams and Roger Kermode in ACM SIGCOMM Computer Communications Review Volume 32, Number 5: November 2002. Under this the history and background of MANET is published with the implementation of AODV and DSDV using Seen Metric.

iv." Ad Hoc Wireless Networks Routing Protocols- A Review" by Geetha Jayakumar and G.Gopinath in Journal of Computer Science 3 (8):574-582-, 2007 ISSN 1549-3636 © 2007 Science Publications. In this design constraints were specified by considering various characteristics.

v. "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations" by S. Corson and J. Macker in Network Working Group Request for Comments: 2501 Category: Informational. Emphasis was on applications, characteristics, ip layer mobile routing, security and efficiency.

vi. "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" by Elizabeth M. Royer and Chai-Keong Toh in IEEE Personal Communications April 1999. In this Signal stability mechanism and comparison of different characteristics was done.

vii. "Mobility Models, Broadcasting Methods and Factors Contributing Towards the Efficiency of the MANET Routing Protocols: Overview by Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Alirview in Paper ID 123. Mobility models, performance evaluation and efficiency of MANET was discussed in this publication.

viii. "Future Application Scenarios for MANET-based Intelligent Transportation Systems" by C.K. Toh in Proceedings of IEEE FCGN Conference, 2007. In this future Ad Hoc applications with their challenges are enclosed. Major emphasis was on traffic system, localised stolen vehicle recovery mechanism, ITS enabled car navigation system.

III. ROUTING PROTOCOLS

Routing protocols is a set of rules that governs a packet to travel along the transmission line in accordance to the parameters of the receiving device. A routing protocol is responsible for successfull and faithfull delivery of the packet. There are three main types of routing protocols in Mobile Ad Hoc Network (1) Reactive – ON Demand, (2) Proactive – Table Driven and (3) Hybrid. Figure 1 depicts various routing protocols used in Mobile Ad Hoc Network.

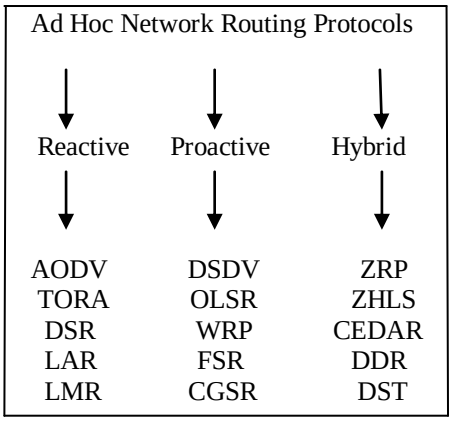


Figure 1: MANET Routing Protocols.

i. Reactive Routing Protocols

Reactive Routing Protocol is known as on demand routing protocol, it is called so because route is established only when the need arises. The principle behind this protocol is Query-Reply topology in which the network does not require to maintain up-to-date. The major advantage of this protocol is that it reduce network traffic overhead. This protocol has two components[3]:

Route Discovery: In this stage the source node initiates the route discovery. The mechanism behind route discovery is that the source node transmits a request or query message, requesting a route to the destination node. This message is flooded i.e. relayed by all the nodes until the request reaches the destination node, the whole route is stored in the request message and is sent back to the source node as reply to the query. There are multiple routes to a single destination but the shortest is selected.

Route Maintenance: Due to dynamic topology environment of the network, route failure arises between nodes due to link breakage etc, so route maintenance is necessary. Reactive Protocols has acknowledgement mechanism due to which route maintenance is possible. If one route fails then new route is implemented as there are multiple paths to send a single packet.

A. AODV

Ad Hoc On Demand Distance Vector[4] is a widely accepted on-demand routing protocol which works on the principle that the sender only includes the address of the neighbouring nodes thus performing hop-by-hop routing, it creates routes on demand. This protocol reduces overhead in the network, and provides moderate mobility in the network performance.

B. TORA

Temporally-Ordered Routing Algorithm is a highly adaptive, loop-free, bandwidth efficient and distributed routing algorithm. It is fairly complicated algorithm but its feature of propagation of control message around the link breakage, makes it a unique and prominent protocol. Optimization of routes is done here by providing new heights to nodes to improve the links.

C. *DSR*

Dynamic Source Routing algorithm uses link state algorithm in which the transmitting node has address of all the nodes in the network. Designed for multi hop networks, every node maintains a cache to store newly discovered routes. It increases overhead as the transmitting node has to maintain addresses of all intermediate nodes also.

D. LAR

Location Aided Routing Protocol[5]. In this Route-Request and Route-Reply packets are sent similar to DSR and AODV. This uses location information to diminish routing overhead in the network.

E. LMR

Light Weight Mobile Routing algorithm is based on link reversal mechanism. It follows two procedures i.e. link establishment and link maintenance. Link maintenance is done by sending failure messages to detect route failure in the network.

ii. Proactive Routing Protocols

Proactive Routing Protocols are known as table-driven routing protocols. This is called so because every node maintains routing table of the whole network topology, even when it is not required and necessary. This protocol is not suitable for larger networks as the nodes has to maintain a large number of information. Although latency is reduced but overhead is increased.

A. *DSDV*

Destination Sequenced Distance Vector[6], in this case each node contains a routing table having information regarding next hop, number of hops to reach the destination. Each node has a large overhead.

B. OLSR

Optimised Link State Routing Protocol is based on link state algorithm.. It performs hop-by-hop routing i.e. each node uses its most recent information to route the packet. It is based on three mechanisms: neighbourhood sensing, efficient flooding of packets and implementing the shortest route by using shortest-path algorithm.

C. *WRP*

Wireless Routing Protocol[7] not only maintains information of nodes in the routing table but also recognise and store the shortest distance between the source node and destination nodes. It is basically a path finding algorithm and converges fast routes in case of link failure at nodes.

D. FSR

This protocol is based on the Fisheye Technique[8] i.e. each node maintains a accurate distance and path quality information about its immediate neighbour. But the amount of information goes on decreasing with increase in distance from the node. The nodes lying outside the fisheye scope receives smaller size update messages as compared to nodes lying in the fisheye coverage.

E. CGSR

Cluster Head Gateway Switch Routing Protocol is different from other protocols because it prefers hierarchical network topology. It divides nodes into clusters which establishes coordination among the members of each cluster related to a special node called as cluster head. Routing performance is increased as packets are routed through both cluster heads and gateways.

iii. Hybrid Routing Protocols

Reactive routing protocols has less network overhead and high network latency, whereas proactive routing protocols has less network latency and high network overhead. So, a trade off is required to overcome the limitations of these two routing protocols. Hybrid Routing Protocol is combination of these two as it uses route discovery mechanism of reactive protocols and table-driven procedure of proactive protocols.

A. ZRP

Zone Routing Protocol[9], as the name suggests it is a algorithm associated with zones. At the initial stage in route discovery mechanism it is checked that whether the destination node is within zone or not. If destination node is within the zone then proactive routing is preffered to speed up communication and if it is outside the zone then inter-zone phenomenon of reactive protocols is used.

B. ZHLS

Zone Hierarchical Link State Routing divides the network in non-overlapping zones. Each zone is assigned with unique zone ID and node ID. There are two types of link state updates: node level LSP(Link State Packet) and zone level LSP. Due to network division there is low overhead.

C. CEDAR

Core Extraction Distributed Ad Hoc Routing, as the name suggests there is a core node in each partition called as dominator node. It is a partitioning protocol which integrates routing with QoS support. It follows three steps: (1) establishment and maintenance of core, (2) propagation of link-states in the core, (3) execution QoS route computation algorithm at core node.

D. DDR

It is a tree based routing protocol without the need of root node or cluster head to handle data between different nodes and zones. In this trees i.e. information regarding different routes of a packet are constructed using periodic messages, which are exchanged by neighbouring nodes only.

E. DST

Distributed Spanning Tree performs node division into number of trees[10]. It follows two strategies:

Hybrid Tree Flooding(HTF): In this the source node sends control packets to all neighbours in the tree. Each packet remains there for a particular holding time.

Distributed Spanning Tree Shuttling: In this the source node sends packet to all tree nodes until the packet reaches its destination leaf or node.

The limiting problem of this mechanism is that if the root node breaks down then the whole tree will be out of function

.*Handoff in MANET:* In convention cellular networks, handoff occurs when signal-to-noise ratio decreases below threshold value. But in case of Mobile Ad Hoc Network there is no concept of signal-to-noise ratio, rather the absence and presence of neighbourhood nodes determines the occurance of handoff from one node to another in case of link breakage.

IV. COMPARISON OF ROUTING PROTOCOLS

Reactive Routing protocols provide less overhead and high latency i.e. packet is delivered to destination node with a delay. Proactive Routing Protocols provide speedy delivery of packet but network overhead is increased as each node has to maintain table of neighbouring node. Hybrid Routing Protocols increases the efficiency by accurate and speedy delivery of data i.e. it contains different routes to destination with speedy delivery.

Table 1. Comparison between Ad Hoc Network Routing Protocols

Parametes	**On-Demand (Reactive)**	**Table-Driven (Proactive)**	**Hybrid**
Overhead	Less	High	Intermediate
Latency	High	Low	Intermediate
Route Availability	On-Demand	Always Available	Depends on destination location
Storing capacity	Depends on number of nodes	High	Depends on number of clusters and zones
Routing tables	No	Yes	Yes

Traffic Control	Low	High	Low than these two
Updates	No	Yes	Yes

V. CONCLUSION

In this paper an effort has been made on comparative study of different routing protocols. Each protocol is unique and has its own characteristics and features. As reactive protocols are suitable for longer distances and proactive are preferred over smaller distances, so there is a trade off between these two and it is hard to make a choice. According to the network establishment and type of application the routing protocol can be implemented. Due to lack of centralized mechanism, absence of infrastructure and dynamic topologies, an additional challenge is introduced i.e. network security. As this field is widespreading with course of time and the need arrises to overcome the challenges to meet the future requirements.

VI. FUTURE APPLICATIONS AND CHALLENGES

i. Security Systems

Ad Hoc System enabling cameras could be installed at hot spots of a city. Whenever a high speed vehicle crosses then this information could be passed to security management team.

Challenge is to make this system perfect in order to curb the high speed vehicles.

ii. Traffic Management.

Potential application of MANET in traffic is that, if a car faces falling trees, road blockage, heavy rain, land slide etc, then it can inform to other cars by transmitting message hop-by-hop. In this way time and life can be saved.

Challenge here is to broadcast message to all other nodes(cars) efficiently without skipping a single node.

iii. Accident Avoidance

Another future application is to install Ad Hoc Network in cars to avoid collision on roads i.e. if someone has to change the lain then it can do this by collecting information about number of other cars on the same lane as well as on the new lane. It will avoid accidents caused due to overtaking and reckless driving.

Challenge is to install the system in all cars.

VIII. REFERENCES

[1] P. Basu and T. D. C. Little. Task-based self-organisation in large smart spaces:issues and challenges. In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999.

[2] P. Bhagvat, C. Bisdjikian, P. Kermani, and M. Naghshineh. Smart connectivity for smart spaces. In DARPA/NIST/NSF Workshop on Research: Issues in Smart Computing Environment, Atlanta, USA, 1999. `

[3] Tarek Sheltami and Hussein Mouftah "Comparative study of on demand and Cluster Based Routing protocols in MANETs", IEEE conference, pp. 291-295, 2003.

[4] C. E Perkins, E. M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[5] Y.-B. Ko and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," "in Mobile Computing and Networking *(*MOBICOM'98*)*", Dallas, TX, USA, 1998, pp. 66–75.

[6] S. Murthy, C. Siva Ram and B.S. Manoj, "Ad Hoc Wireless Networks:Architectures and Protocols," Prentice Hall, Chapter 7, 2004.

[7] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," "ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks*"*,
Oct. 1996, pp. 183–97.

[8] G. Pei, M. Gerla, T.-W. Chen, "Fisheye state routing in mobile ad hoc networks," in: "Proceedings of IEEE ICDCS Workshop on Wireless Networks and Mobile Computing*"*, April 2000, pp. D71– D78.

[9] Z. J. Haas and M. R. Pearlman, .ZRP: a hybrid framework for routing in ad hoc networks, pp. 221.253, 2001.

[10] S. Radhakrishnan, N. Rao, G. Racherla, C. Sekharan, and S. Batsell, "DST – a routing protocol for ad hoc networks using distributed spanning trees," in: "Proceedings of IEEE WCNC*"*, September 1999, pp. 100–104.

Analysis of Sybil Attack Detection Mechanism-Footprint in Vehicular Ad Hoc Networks

Harpreet Singh
Student, Dept. ofCSE
Amritsar College of Engineering and Technology,
PTU, Jalandhar, Punjab
harpreetmoda@ymail.com

Dr. TanuPreet Singh
Professor and HOD, Dept. of ECE
Amritsar College of Engineering and Technology,
PTU, Jalandhar, Punjab
tanupreet.singh@gmail.com

ABSTRACT

In vehicular networks, where privacy, especially the location privacy of nameless vehicles is highly concerned, anonymous verification of vehicles is absolutely necessary. An attacker who succeeds in creating multiple hostile identifies can easily launch a Sybil attack, gaining anextremely large influence. In this paper, we analyze Sybil attack detectionmechanism, Footprint that uses the trajectories of vehicles for identification while still preserving their location privacy. More precisely, when a vehicle approaches a road-side unit (RSU), itasks for an authorized message from the RSU as the proof of theappearance time at this RSU. We design alocation-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous which means RSU is anonymous when signing a message; second is the temporary linkable property which means two authorized messages issued from same RSU are identifiable if they are issued within same period of time. With the temporal limitation on the linkability of two authorized messages, authorized messages used for long-term identification are illegal. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages.

GeneralTerms—Sybil Attack, signer-ambiguous signature, temporary linkable trajectory.

1. Introduction

Vehicular Ad Hoc networks are emerging new technologies to integrate the capability of new generation wireless networks to vehicles. The idea is to provide:

- Connectivity on the road to mobile users
- Efficient vehicle to vehicle communications that enable the intelligent transportation system (ITS).

Therefore vehicular Ad Hoc networks are also called inter vehicle communications (IVC) or vehicle to vehicle communications (V2V).

In the last few years we have seen a large increase in research and development in this area. Several factors have led to this development including the utilization of IEEE 802.11 [1] [2] technologies, manufacturing of vehicles to address the safety, environmental and comfort issues of their vehicles. Although cellular networks enable convenient voice communication and simple infotainment services to drivers and passengers, they are not well suited for certain direct vehicle to vehicle and vehicle to infrastructure communications. However, vehicular Ad Hoc networks which offers direct communications between vehicles and to and from roadside units (RSU's) can send and receive hazard warnings and information on the current traffic situations with minimal delay.

A wide spectrum ofapplications in such a network relies on information aggregation among participating vehicles. Without identities of participants, such applications arevulnerable to the Sybil attack where a malicious vehicle masquerades as multiple identities [3]. The consequence of Sybil attackhappening in vehicular networks can be critical. For example,in safety-related applications such as hazard warning,collision avoidance, and passing assistance, biased resultscaused by a Sybil attack can lead to severe car accidents. Therefore, it is of great importance to detect Sybil attacksfrom the very beginning of their happening.

Sybil Attacks in VANETs –Sybil attacks have been regarded as serious security threats to ad hoc networks. In these attacks a malicious vehicle claims to be at multiple locations with multiple identities and thus creates an illusion of traffic congestion. A malicious vehicle can manage to get identities of other vehicles by stealing or by eavesdropping.

Challenges in detecting Sybil Attacks-

- Vehicles are anonymous. There are no chains of trust that links claimed identities with the real ones.
- Location information of vehicles in very confidential
- Conversation between vehicles is very short due to high mobility of vehicles
- Difficult to establish trustworthiness among vehicles in such short period of time

These lack of qualities in the network enables the malicious vehicles to generate a hostile identity which is very difficult to validate in short time conversations between vehicles

Thepaper is organized as follows. Section 2 introduces various techniques to remove Sybil attack problem. In Section 3, we describe the Footprint technique, attack models in vehicular networks. Section 4 elaborates the design of Footprint. Finally, we give concluding remarks and outline the directions for future work in Section 5.

2. Techniques to remove the threat of Sybil Attacks-

- **PKI Based Signature-**it is straightforward to openly bind a distinct authorized identity (e.g. PKI-based signatures) [4], [5], [6] to each vehicle so thateach participating vehicle can represent itself only onceduring all communications. Using explicit identities ofvehicles has the potential to completely avoid Sybil attacksbut violates the anonymity concern in vehicularnetworks.
- **Resource Testing-** resource testing [7],[8], [9] can be conducted to distinguish betweenmalicious and normal vehicles, where the judgment ismade whether a number of identities possess fewerresources (e.g., computational and storage ability) thanwould be expected if they were different. This scheme fails inheterogeneous environments where malicious vehicles caneasily have greater no. of resources than normal ones.
- **Global Positioning System (GPS)-**It is aimed to provide locationinformation of vehicles which can be exploited to detect hostileidentities. However, these schemes often fail in complicatedurban settings (e.g., bad GPS signals due to urban canyons,inaccurate localizations due to highly dynamic wirelesssignal quality).
- **Group-signature-basedschemes** [10], [11]- Using group signatures can provide anonymity of vehicles and suppress Sybil attacks by restrictingduplicated signatures signed by the same vehicles.
- **SybilGuard**[12]- In this scheme, human-established real-world trust relationship among users isused for detecting Sybil attacks. Since even the attacker cangenerate as many as Sybil identities, building relationshipbetween honest users and Sybil identities is much harder.Thus, there exists a small "cut" on the graph of trustrelationship between the forged identities and the real ones.However, this scheme cannot be used in vehicular net-works, since it is very challenging to create such trustrelationship among vehicles. This is because vehicles arehighly mobile. Communications often happen amongtemporarily met and unfamiliar vehicles.
- **Received Signal Strength Indication(RSSI)**- In this scheme, by successively calculating the RSSIvariations, the relative locations among vehicles in surroundingscan be estimated. Identities with the same estimatedlocations are considered as Sybil vehicles.Xiao et al. [13] have proposed a Sybil attack detectionscheme where the location of a particular vehicle can bedetermined by the RSSI measurements taken at otherparticipating vehicles. In addition to the inaccuracy of RSSImeasurements, this scheme also needs all neighboringvehicles to act as a team which may suffer a Sybil attackagainst the detection scheme itself

3.Introduction to Footprint-Sybil Attack eradication scheme-

In this paper, we study a novel Sybil attack detectionscheme **Footprint** that uses the trajectories of vehicles foridentification whileconserving the anonymity andlocation privacy of vehicles. Specifically, in Footprint, whena vehicle meets an RSU, upon request, the RSU issuesan authorized message for this vehicle as the proof of itspresence at this RSU and time. Intuitively, authorizedmessages can be utilized to identify vehicles since vehicleslocated at different areas can get different authorizedmessages. However, straight usage of authorized messageswill leak location privacy of vehicles because knowing anauthorized message of a vehicle signed by a particular RSUis equivalent to knowing the fact that the vehicle hasshowed up near that RSU at that time. In Footprint, wedesign alocation-hiddenauthorized message generationscheme for two purposes-

- RSU signatures onmessages aresigner-ambiguouswhich means an RSU isanonymous when signing a message. In this way, the RSUlocation information is concealed from the final authorizedmessage.
- Authorized messages aretemporarilylinkablewhich means two authorized messages issued fromthe same RSU are recognizable if and only if they are issuedwithin the same period of time.

Thus, authorized messagescan be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the linkability of twoauthorized messages, authorized messages used for long-term identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harmanonymity of vehicles.To be uniquely identified, a vehicle collects a consecutiveseries of authorized messages as it keeps traveling. Such asequence of authorized messages constitutes atrajectory ofthis vehicle. In Footprint, a vehicle is free to start a newtrajectory by using a new temporary public key. Further-more, a malicious vehicle can abuse this freedom toelaborately generate multiple trajectories, trying to launcha Sybil attack. Based on the observation that Sybiltrajectories generated by a malicious vehicle are very alike,Footprint establishes the relationship between a pair oftrajectories according to our definition of similarity. Withthis relationship, Sybil trajectories generated by the samemalicious vehicle form a "community." By finding andremoving "communities" of Sybil trajectories, Footprintcan detect and defend against Sybil attacks.

Advantages of Footprint-

- Footprintdoes not need the identities of vehicles, which ensures theanonymity of vehicles.

- Second, no geographical informationis leaked in Footprint, which guarantees the locationprivacy of vehicles.
- Third, Footprint only needs each vehicleto be equipped with a cheap commercial GPS receiver andDSRC wireless communication module.
- Sybil attackdetection can be online independently conducted by aconversation holder (e.g., an individual vehicle or an RSU)which initializes a conversation among vehicles.

Limitation of Footprint-Footprint requires an infrastructure of RSUs and a trustauthority (TA) existing in the system in order to generatetrajectories and establish trust among entities, respectively.

Attack model and assumptions in Footprint-

Assumptions:

- The TA and all RSUs are fully trustworthy.
- The RSUs are synchronized.Synchronization among RSUs is easy to attain since allRSUs are unified by the RSU backbone network.
- The mobility of vehicles is independent.This means individual vehicles should move independently and therefore would not travel along the same routefor all the time.

Attack Model-

In order to launch a Sybil attack, a malicious vehicle musttry to present multiple distinct identities. This can bedone by either generating legal identities or byimpersonating other normal vehicles. With the followingcapabilities, an attacker may succeed to launch a Sybilattack in vehicular networks:

Heterogeneous configuration: malicious vehicles canhave more communication and computation resources than honest vehicles. For example, amalicious vehicle can mount multiple wireless cards,physically representing different communicationentities. Furthermore, having more powerful resources can also fail those resource testing schemesfor detecting Sybil attacks.

Message manipulation:due to the nature of openwireless channels, the attacker can eavesdrop onnearby communications of other parties. Thus, it ispossible that the attacker gets and interpolatescritical information needed to impersonate others.In any decision-making procedure based on reports sentfrom a number of individual vehicles, if an attackersucceeds in presenting multiple independent identities, itcan launch Sybil attacks against honest vehicles where theattacker can inject multiple false reports via multipleidentities into the final decision.

4. SYSTEM DESIGN

In general, Footprint chains threetechniques namely, infrastructure construction, location-hidden trajectory generation, and Sybil attack detection.Incremental methodology is usedfor deployment of RSUs. In the end, a limited number of available RSUs can get the maximum service coverage in termsof served traffic amount as well as good fairness in terms of geographical distribution. After the deployment of RSUs, a vehicle can require authorized messages from each RSU it passes by as a proof of its presence there. We adopt an event-oriented linkable ring signature scheme [14] for RSUs to issue authorized messages for vehicles. Such authorized messages are location hidden which refers to that RSUsignatures are signer ambiguous and the authorizedmessages are temporarily linkable. Furthermore, a set of consecutive authorized messages issued for a vehicle are tightly chained together to form a location-hidden trajectory of the vehicle, which will be utilized for identifying this vehicle in future conversations. During a conversation which is started by a vehicle or an RSU, called aconversation holder, a participating vehicle should provide its trajectory for verification. With the trajectories sent from all participating vehicles, the conversation holder can conduct online Sybil attack detection according to the similarity relationship between each pair of trajectories. Among alltrajectories, Sybil trajectories forged from the same attacker are sure to gather within the same "community." By treating each "community" as one single vehicle, Sybil trajectories can be largely eliminated.

Infrastructure Construction

Deployment of RSU

In Footprint, vehicles require authorized messages issued from RSUs to form trajectories, which should be statically installed as the infrastructure.RSUs are deployed at all intersections. This can result good trajectories with aadequate number of authorized messages which will assist the recognition of a vehicle. However, deploying such a huge number of RSUs in one time is prohibitive due to the high cost. In contrast, we take an incremental deployment strategy in Footprint, considering the compromise between minimizing the number of RSUs and maximizing the coverage of traffic. Specifically, in the early developing stage with a limited number of RSUs, an intersection is chosen if it satisfies two requirements: first, it is geographically at least definite distance away from all other RSU-equipped intersections; second, it has the maximum traffic volume among all rest intersections without RSUs.

Initialization of System

After deployment of RSU, the system needs to be initialized. The initialization process includes three steps:

1. Setting up TA: TA first chooses a set of public parameters required for the ring signature scheme which is used for RSUs to sign messages and establishes a pair ofpublic/private key pair Kpub, Kpri. The public key of the TAKpub can be obtained by all RSUs and vehicles in the system through a secure channel. It is used to verify whether a message is authorized by the TA

2. Setting up RSUs: When a new RSU R is added to the system, the TA issues a pair of public/private key pair KpubR, KpriRfor R and sends the public parameters to R as well. After all RSUs are recorded in the system, the Public Key List (PKL) of all RSUs is broadcasted to all RSUs from the TA via the RSU backbone network. In addition, the IPaddresses of its

neighboring RSUs of Rare also notified to R. Complying with the incremental deployment of RSUs, version control is taken by the TA in managing the PKL. More specifically, when new RSUs enroll in the system, the TA updates the PKL and rises its version number. Then, the newest PKL can be disseminated to all RSUs in the system via the RSU backbone network.

3. Setting up vehicles: For a vehicle to join in the system, it only needs to get the PKL of all RSUs and the public parameters. It can get such information when meeting any RSU or a vehicle with the information. After that, it can construct its own trajectories in the system.

Generating Location-Hidden Trajectory

Location-Hidden Authorized Message Generation-One possible implementation of a location-hidden authorized message generationscheme is by utilizing linkable ring signature [15]. Linkable ringsignature is signer-ambiguous and signatures are linkable(i.e., two signatures can be linked if and only if they areissued by the same signer) as well. Particularly, we choosethe linkable ring signature scheme introduced by Dodis et al.[16] and Tsang and Wei [17] for two reasons: first, it has beenproved to be secure; second, it has constant signature size.To meet the requirement of temporarily linkable property,we extend the scheme to support theevent-orient linkabilityproperty [14] which guarantees that any two signatures arelinkable if and only if they are signed based on the sameevent by the same RSU.In our signature scheme, we define aneventas a periodof time within which two signatures issued from the sameRSU are linkable. In **Footprint**, when avehicleviapproaches an RSUR, it demands a time stampfromR,using a generated key pairKpub, Kpri.Upon request,Rgenerates a messageMforvi,which includesKpub and a time stampindicating the timewhen this message is generated. Then,Rksigns on themessageMand sendsMtogether with the signature,denoted asM ||SR (M) backtovi.

Trajectory-Encoded Message

Intuitively, an authorized message issued from an RSU canbe used to identify a vehicle. However, it is often the casethat two or more authorized messages may have the samelink tag. In this case, it is hard to tell whether thesemessages belong to different vehicles.With the independent mobility assumption, as twovehicles move along, the probability for the pair of vehicleshaving exactly the same trajectories is slim. Therefore, it isfeasible to use trajectories to exclusively represent corresponding vehicles as long as those trajectories are sufficiently long. With authorized messages, a straightforwardmethod for a vehicle to present its trajectory is to sort all itsauthorized messages into a sequence according to time.Thus, in future conversations, the vehicle can use thissequence of authorized messages to identify itself. Thismethod is simple but inefficient because each time when thevehicle needs to be identified in a conversation, allmessages in the sequence should be sent to the conversationholder for verification. This will cost tremendous wirelessbandwidth and computational resources. Furthermore, amalicious vehicle can easily forge a huge number of faketrajectories by arbitrarily picking a subset of authorizedmessages as long as these messages are in the right order oftime. Since authorized messages are location hidden, theconversation holder cannot tell whether a providedtrajectory is an actual one or a forged one.In Footprint, we embed the trajectory of a vehicle into anauthorized message. Specifically, upon the starting of a newevent, besides computing the new event id and link tag forthe new event, an RSU also informs all its neighboring RSUswith the new generated link tag.

Sybil Attack Detection

During a conversation, upon request from the conversationholder, all participating vehicles provide their trajectory-embedded authorized messages issued within specified event for identification. With submitted messages, theconversation holder verifies each trajectory and refusesthose vehicles that fail the message verification. After that,the conversation holder conducts online Sybil attackdetection before further proceeding with the conversation.

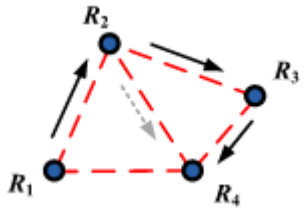


Fig1: RSU neighboring relationship

Figure showing RSUs connected with dash line where solid arrows show the actual sequence of RSU and dash arrow shows possible forged trajectory.

Message Verification-As the proof that a vehicle vi was present near certain RSU R at certain time, an authorized message allotted for vi can be verified by any entity (e.g., a vehicle or an RSU) in the system. In the case that an entity needs to verify vi, vi will sign onan authorized message M || SR (M) generated by RSU R using Kpri and then send the message to the entity. The message verification process consists oftwo steps:

1. Ownership verification:

Since any other Kpriwill fail the test, an authorized message cannot be misused by other vehicles because only vi knowsKpri which is pairwise with Kpub contained in M. Therefore, if the test stands, it meansMisexclusively generated forvirather than for other vehicles.

2. Legitimacy verification: If the authorized message passesthe ownership verification, the entity further examineswhether the signature contained in the authorized messageis signed by a legitimateRSUinthesystem. In the case thatvifails in either step, the entity will considervias a malicious vehicle and ignore any furtheractions ofvi.

Problem Definition

Recall that, in Footprint, vehicles have wide freedom tomake their trajectories. For example, a vehicle is allowed torequest multiple authorized messages from an RSU usingdifferent temporary key pairs. Thus, a vehicle can usedifferent authorized messages for different conversations.This capability, however, can be used to maximum advantage by a maliciousvehicle that tries to launch a Sybil attack by using multipledifferent messages in a single conversation.

In Fig. 1, an attacker can legally generate multipletrajectories which appear distinct from each other evenunder a very simple RSU topology. Assume the real path ofthe attacker is {R1, R2, R3, R4} (indicated by solid arrows). Itcan start a new trajectory at any RSU by using a differenttemporary key pair. Therefore, besides thetrajectory {R1, R2, R3, R4}, trajectories like{R1, R2, R3}, {R2, R3, R4}, {R1, R2}, {R2, R3}, { R3, R4}, {R1}, { R2}, {R3}, {R4} are all legitimate. In addition, knowing the neighboring relationship ofR2 andR4, the attacker can generate forged trajectorieslike{R1, R2, R4}, {R1, R4}, {R2, R4}(indicated by thedash arrow). Note that the attacker cannot generate atrajectory like {R1, R3} since R1 is not a neighbor ofR3.In the case of this example,R3 expects signatures signedbyR2 andR4.

Eliminating Sybil Communities

the Sybil attack detection problem can be well resolved by finding an efficient algorithm to remove all possible "communities" of Sybil trajectories. However, the problem of finding all Sybil "communities" within a given set of trajectories is very hard. Assume each trajectory in the set is a vertex in anundirected graph. We define an edge between two vertices if the corresponding trajectories have a non-negative similarity value. To find all "communities" in the trajectory set is equal to find all complete subgraphs (called cliques). Finding all cliques in a graph is a well-known NP-complete problem.

In Footprint, we take an iterative procedure to get all Sybil "communities." Specifically, we first generate a corresponding graph.Then, iteratively, we pick a maximum clique each time in the graph and remove all vertices in the clique andall corresponding edges from the graph until there are no more vertices present in the graph. The reason that we pick the maximum clique each time is twofold: First, in order to launch a Sybil attack, a malicious vehicle presumes to achieve multiple identifications, which requires the attacker to issuea sufficient number of forged trajectories. This will form a big-sized clique in contrast to those cliques made up of honest vehicles; Second, because the order in which we remove cliques from the graph does not change an original clique from being a clique in the left graph, removing the max clique each time helps contract the size of the graph, whichimproves the Sybil attack detection performance. If there are multiple maximum cliques found, we choose the one with the largest sum of similarity associated with all edges. The reason is that a larger similarity means two trajectories are more alike, which are more likely from a malicious vehicle.With each picked maximum clique, we choose the trajectory with the longest length as a legal trajectory and remove all other trajectories in the clique.

5. Conclusion and Future Work

In this paper, we have studied a Sybil attack detection scheme Footprint forvehicular networks. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme.Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories.Footprint can largely restrict Sybilattacks and can enormously reduce the impact of Sybilattacks in urban settings (above 98 percent detection rate).With the proposed detection mechanism having muchspace to extend, we will continue to work on severaldirections. First, in Footprint, we assume that all RSUs aretrustworthy. However, if an RSU is compromised, it canhelp a malicious vehicle generate fake legal trajectories (e.g. by inserting link tags of other RSUs into a forged trajectory).In that case, Footprint cannot detect such trajectories.However, the corrupted RSU cannot deny a link taggenerated by itself nor forge link tags generated by otherRSUs, which can be utilized to detect a compromised RSUin the system. In future work, we will consider the scenariowhere a small fraction of RSUs are compromised.Improvements will be made based on the realistic studiesbefore it comes to be deployed in large-scale systems.

References

[1] IEEE 802.11p Amendment, "Wireless Access in Vehicular Environments," v. D3.0, 2007, work in progress.

[2] Harpreet Singh, Tanupreet Singh, GovindSood, "A Review Of Vehicular Ad Hoc Networks, Applications, Challenges, Attacks and Security Measures,"ISBN NO: 978-81-924867-3-4 , June 2014.

[3]J.R. Douceur, "The Sybil Attack,"Proc. First Int'lWorkshop Peer-to-Peer Systems (IPTPS '02),pp. 251-260, Mar. 2002.

[4]M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks,"Proc. Symp. Operating Systems Design and Implementation (OSDI '02),pp. 299-314, Dec. 2002.

[5]B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust,"Technical Report SRI-SDL-04-02, SRI Int'l, Apr. 2002.

[6]S. Capkun, L. Buttyan, and J. Hubaux, "Self-Organized Public KeyManagement for Mobile Ad Hoc Networks," IEEE Trans. MobileComputing,vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[7]C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack inMobile Ad Hoc Networks,"Proc. Securecomm and Workshop,pp. 1-11, Aug. 2006.

[8]N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. SixthIEEE Int'l Conf. Peer-to-Peer Computing (P2P '06),pp. 171-176, Oct.2006.

[9]P. Maniatis, D.S.H. Rosenthal, M. Roussopoulos, M. Baker, T.Giuli, and Y. Muliadi, "Preserving Peer Replicas by Rate-LimitedSampled Voting,"Proc. 19th ACM Symp.Operating SystemsPrinciples (SOSP '03),pp. 44-59, Oct. 2003.
[10]Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "BalancedTrustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications,"IEEE Trans. Vehicular Technology,vol. 59, no. 2,pp. 559-573, Feb. 2010.
[11]L. Chen, S.-L. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs,"IEEE J. Selected Areas in Comm.,vol. 29, no. 3, pp. 1-11, Mar. 2011.
[12]H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard:Defending against Sybil Attacks via Social Networks,"Proc.SIGCOMM,pp. 267-278, Sept. 2006.
[13]B. Xiao, B. Yu, and C. Gao, "Detection and Localization of SybilNodes in Vanets,"Proc. Workshop Dependability Issues in WirelessAd Hoc Networks and Sensor Networks (DIWANS '06),pp. 1-8, Sept.2006.
[14]P.P. Tsang, V.K. Wei, T.K. Chan, M.H. Au, J.K. Liu, and D.S.Wong, "Separable Linkable Threshold Ring Signatures," Proc. Int'lConf. Cryptology in India (INDOCRYPT '04), pp. 384-398, 2004.
[15]J.K. Liu, V.K. Wei, and D.S. Wong, "Linkable SpontaneousAnonymous Group Signature for Ad Hoc Groups (ExtendedAbstract),"Proc. Ninth Australasian Conf. Information Security andPrivacy (ACISP '04),pp. 325-335, 2004.
[16]Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "AnonymousIdentification in Ad Hoc Groups,"Proc. Int'l Conf. Theory andApplications of Cryptographic Techniques (EUROCRYPT '04),pp. 609-626, 2004.
[17]P.P. Tsang and V.K. Wei, "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation,"Proc. Information Security Practiceand Experience Conf. (ISPEC '05),pp. 48-60, 2005.

Performance Evaluation of DSR and DSDV Routing Protocols by using NS2 Simulator

Sandeep Singh
M.tech Scholler
ACET AMRITSAR

Monika Jyoti
M.tech Scholler
BCET GURDASPUR

Soubti saini
M.Tech Scholler
SSI PATHANKOT

Abstract- **Ad Hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration, in which individual nodes cooperate by forwarding packets to each other to allow nodes to communicate beyond direct wireless transmission range.Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power. Ad Hoc routing protocols can be divided into two categories: table-driven (proactive schemes) and on-demand routing (reactive scheme) based on when and how the routes are discovered. In Table-driven routing protocols each node maintains one or more tables containing routing information about nodes in the network whereas in on-demand routing the routes are created as and when required. Some of the table driven routing protocols are Destination Sequenced Distance Vector Routing protocols (DSDV), Clusterhead Gateway Switching Routing Protocol (CGSR), Hierarchical State Routing (HSR), and Wireless Routing Protocol (WRP) etc. The on-demand routing protocols are Ad Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing Algorithm (TORA). There are many others routing protocols available. Zone Routing Protocol (ZRP) is the hybrid routing protocol In this paper for evaluation purposes, we have considered 500m x 500m, terrain area which compare the performance in terms of the packet delivery fraction and throughput for DSR and DSDV routing protocols. The simulation is done by using NS-2 simulator and results shows that DSR performs better in both cases packet delivery fraction and throughput over DSDV routing protocol.**

Keywords – ***DSDV, DSR, Packet Delivery Fraction, Throughput.***

I. INTRODUCTION

There are currently two variations of mobile wireless networks infrastructured and Infrastructureless networks.The infrastructured networks, also known as Cellular network, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs).

The other type of network, Infrastructureless network, is known as Mobile Ad NETwork (MANET). These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.As mobile ad hoc network does not have any fixed infrastructure and so also called as infrastructure-less network because nodes establish communication among themselve by adapting the dynamically changing network environment. Dynamic and infrastructure-less, wireless ad-hoc networks implies that any computation on the network needs to be carried out in a decentralized manner. Further, in a wireless ad hoc network, channel bandwidth and node energy, are two important constrain factors [11] and hence it is a good idea to use reactive routing, where routing is performed only on demand.This paper discuss in detail the functioning of DSR and DSDV routing protocols.we compare these two routing protocols with real experimental results by using Network Simulator-2(NS-2).

Section 2 will explain a proactive protocol, DSDV (Destination Sequence Distance Vector), and a reactive protocol, DSR (Dynamic Source Routing). Section 3 covers our experimental setup for performance evaluation of DSR and DSDV routing protocols using NS-2. In Section 4, the result analysis is presented.

Section 5 concludes this paper . **TYPES OF ROUTING PROTOCOLS**

In this section we will briefly study types of routing protocols.These routing protocols are classified into two main categories:(i) Table Driven Routing Protocols(proactive protocol)(ii) Source Initiated On Demand Routing protocol(reactive protocol).

Table Driven Routing Protocols:Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast.

Source Initiated On Demand Routing:A different approach from table-driven routing is source-initiated on demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired

2.1 DSDV(Destination Sequence Distance Vector)

Destination Sequence Distance Vector is proactive routing protocol in which a every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the nexthop neighbor to reach the destination node, the timestamp of the last update received for that node.This Routing Algorithm is based on the idea of the Distributed Bellman Ford (DBF) Routing Algorithm with certain improvements.In case of failure of route of upcoming hop,the sequence number is updated and information is broadcasted to neighbours.The routing table is checked when a node receives routing information.If such entry is not found in the routing table then routing table is updated with new routing information.If the new found entry is already present in the routing table then the sequence number of the received information is compared with the entry in the routing table and information is updated.If the sequence number is less than received information then information is rejected with the least sequence number.if the two sequence numbers are equal then hop with short routing data is preserved.

2.2Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is a reactive protocol of type Source Initiated On Demand Routing protocol.The main concept of this type of protocol is source routing.It is mainly used for multi hop adhoc networks present in mobile nodes.this protocol allows network to become completely self –organizing and self-configuring and there is no need of previous network or infrastructure.this protocol does not uses periodic messages like used in AODV protocols which reduces network bandwidth.DSR protocol also save battery power and large routing updates is not done in this type of protocol. The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the mobile has not yet seen the request and if the mobile's address does not already appear in the route record. A route reply is generated when the route request reaches either the destination itself, or an intermediate node, which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. illustrates the formation of the route record as

the route request propagates through the network. If the node generating the route reply is the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator. If it has a route to the initiator in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record. If symmetric links are not supported, the node may initiate its own route discovery and piggyback the route reply on the new route request shows the transmission of the route reply with its associated route record back to the source node.

I. EXPERIMENTAL SETUP

For performance evaluation of the DSR and DSDV routing protocols the simulation environment is created. It calculates the performance of protocols in dynamic network topology changes while continous delivery of packets from source to the destination. To calculate the performance ability, different possible set of future events are generated by changing the number of hops. We use following scenario generation commands for generating scenario file for 20, 50, 80 and 100 nodes:

./setdest –v 1 –n 20 –p 2.0 –M 10.0 -t 200 -x500-y 500;
./setdest –v 1 –n 50 –p 2.0 –M 10.0 -t 200 -x50 -y 500;
./setdest –v 1 –n 80 –p 2.0 –M 10.0 -t 200 -x50 -y 500;
/setdest –v 1 –n 100 –p 2.0 –M 10.0 -t 200 -x50 -y 500.

Similarly, for connection pattern generation we use, cbrgen.tcl file. Following commands are used for creating the connection pattern

ns cbrgen.tcl -type cbr -nn 20 -seed 1.0 -mc 16 –rate 4.0;
ns cbrgen.tcl -type cbr -nn 50 -seed 1.0 -mc 16 –rate 4.0;
ns cbrgen.tcl -type cbr -nn 80 - seed 1.0 -mc 16 –rate 4.0;
ns cbrgen.tcl -type cbr -nn 100 -seed 1.0 -mc 16 rate 4.0;

The trace file is created during each execution and is evalulated using a no of different scripts , particularly one called file *.tr and this .tr file counts the number of successfully packets that are successfully delivered and the length of the route taken by the packets, and also additional information about the internal functioning of each scripts executed. This trace file is evaluated by using AWK file and graphs are created by using Ms Excel.

Simulations are done by considering DSR and DSDV routing protocol. To get actual performance, the mean of results are calculated for number of scenarios. We measure the protocols performance on a terrain area of 500m x 500m from real life scenario at a fix speed of 10 m/s. The time of simulation was taken 200 seconds for Constant Bit Rate (CBR) traffic type with a packet size of 512 Byte. All the nodes are considered with Omni-Antenna and Two Ray Ground Radio Propagation method. Simulation parameters are in shown below in Table-1.

SIMULATION PARAMETERS

Parameter taken	Value
Simulator used	NS-2.2
Used protocols	DSDV and DSR
Time of simulation	200 sec
Area of simulation	500 x 500
Range of transmission	250 m
Node movement	Random waypoint
Type of traffic	CBR (UDP)
Data payload	512 bytes/pkt

Table: 1. Simulation Parameters

II. PERFORMANCE METRICS AND RESULT ANALYSIS

The Packet Delivery Fraction (PDF) and throughput are considered in Kilo bits per second (Kbps) for evaluation of DSR and DSDV routing protocols. The simulation results that are obtained with above simulation parameters are ashown in Table-2. The comparison between DSDV and DSR is shown in Figure.1 by using graph comparision.

4.1 Packet Delivery Fraction (PDF).

It is the ratio of the data packets delivered to the packets that are generated by host..

Packet Delivery Fraction (PDF) = Packets Received by the destination node / Total Packets Sent by the source.
Mathematically, it can be expressed as:

$$P = \frac{1}{c} \sum_{f=1}^{e} \frac{R_f}{N_f}$$

Where, P is the fraction of successfully delivered packets, C is the total number of flow or connections, f is the unique flow id serving as index, R_f is the count of packetsreceived from flow f and N_f is the count of packets transmitted to f.

Node: 20, Pause Time: 2.0 Sec., Max Speed: 10 m/s.

Routing protocols	Total Packets Send	Total Packet Received	Packet Delivery Ratio
DSDV	8855	7598	0.858046
DSR	8910	8902	0.999102

Node: 50, Pause Time: 2.0 Sec., Max Speed: 10 m/s

Routing protocols	Total Packets Send	Total Packet Received	Packet Delivery Ratio
DSDV	8820	7528	0.853514
DSR	8870	8858	0.998308

.

Node: 80, Pause Time: 2.0 Sec., Max Speed: 10 m/s.

Routing protocols	Total Packets Send	Total Packet Received	Packet Delivery Ratio
DSDV	8896	7678	0.863084
DSR	8847	8799	0.994574

Node: 100, Pause Time: 2.0 Sec., Max Speed: 10 m/s.

Routing protocols	Total Packets Send	Total Packet Received	Packet Delivery Ratio
DSDV	8831	8169	0.925036
DSR	8887	8867	0.997749

Table.2 Packet Delivery Fraction with varying number of Nodes.

4.2 Throughput

In case of routing protocols throughput means that the the total size of useful packets that received at all the destination nodes. The basic unit of throughput is MB/s, however we have taken it in Kilo bits per second (Kb/s). The throughput values obtained for the simulation parameters of table -1 is tabulated in table-3. The graph shown in below figure-2 indicates the throughput comparison of these two routing protocols, DSDV and DSR.

Throughput in Kbps with varying number of Nodes				
DSDV	1730.16	1723.69	1971.17	2042.04
DSR	6845.53	7935.53	8141.34	7306.86
No. of Nodes	20	50	80	100

Table.3 Throughput with varying number of Nodes.

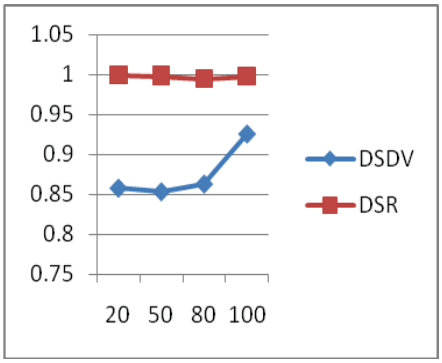


Figure 1 Packet Delivery Ratio Vs No of nodes

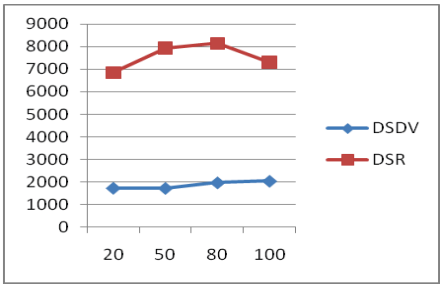


Figure 2 Throughput Vs No of nodes

III. CONCLUSION

Figure 3. Simple MANET Network

In this paper we have calculated the performance of DSDV and DSR routing protocols for mobile ad hoc networks using event simulator NS-2 by taking packet size of 512 Byte**.** DSDV protocol works on proactive table-driven routing strategy whereas DSR works on the reactive on demand routing strategy with different routing mechanisms. Experimental results that arrives showed us that DSR perform much better in case of Packet Delivery Fraction as well as Throughput. Also, DSDV apply the sequence numbers and contains one route per destination in its routing table whereas DSR works on source routing and route caches and maintains multiple routes per destination. The other observation comes from the experiments on DSDV and DSR protocols is that the behavior of these routing protocols changes when there is increase in number of nodes for a fixed area of 500m x 500m illustrates that even if the terrain area of the network scenario is kept constant, the behavior of these routing protocols changes.

At last it has been found that the overall performance of DSR routing protocol in case of performance matrices, Packet Delivery Fraction as well as Throughput is better than that of DSDV routing protocols. In our experimental evaluation we have taken up comparison of DSR and DSDV protocols with varying number of nodes. We shall consider the comparison of DSR and DSDV by varying packet size and speed of nodes.

REFERENCES

[1] Azzedine Boukerche. Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks. *Kluwer Academic Publishers, Netherlands, Mobile Networks and Applications Vol.9,* No.4. pp 333-342, 2004,

[2] C. Cheng, R. Riley, Srikanta P. R. Kumar, J. J. Garcia-Luna Aceves. A Loop free Bellman-Ford reouting protocol without bouncing effect. *In ACM SIGCOMM'89,* September 1989, pp 224-237.

[3] The Network Simulator - ns-2, Website : *http://www.isi.edu/nsnam/ns/*

[4] Charles E. Perkins and Pravin Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In *Proceedings of the SIGCOMM '94 Conference on Communications Architectures,* Protocols and Applications, pages 234–244, August 1994.

[5] The CMU Monarch Project's Wireless and Mobility Extensions to ns, Website: *http://www.monarch.cs.cmu.edu/*

[6] Charles E. Perkins, Pravin Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In *Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, August 1994. A revised version of the paper is available from *http://www.cs.umd.edu/projects /mcml/papers/Sigcomm94.ps Dynamic Source Routing Protocol Internet Draft http://www.ietf.org/html. charters/manet-charter.html*.

[7] D. Johnson, D. Maltz. Dynamic source routing in ad hoc wireless networks. In T. *Imielinski and H. Korth, editors, Mobile computing,* Chapter 5. Kluwer Academic, 1996.

[8] Josh Broch, David Johnson, and David Maltz. The dynamic source routing protocol for mobile ad hoc networks. *IETF Internet Draft*

http://www.ietf.org/internet-drafts/ draft-ietf-manet-dsr-01.txt, Dec 1998.

[9] D. Johnson, D. Maltz and J.Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad hoc networks, *Internet Draft, draft-ietf-manet-dsr-07.txt*, 2002.

[10] Azzedine Boukerche, Athanasios Bamis, Ioannis Chatzigiannakis, Sotiris Nikoletseas. A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks. *The International Journal of Computer and Telecommunications Networking, Vol. 52*, Issue 1, pp 130-154, Jan, 2008.

[11] Rajeshwar Singh, D K Singh, Lalan Kumar. Ants Pheromone for Quality of Service Provisioning In Mobile Adhoc Networks. *International Journal of Electronics Engineering Research, Vol. 2*, No 1 pp 101–109, Apr 2010.

[12] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin. Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment. *IJCSNS, VOL.9* No.7,pp 261-268, July 2009.

Various Types of Attacks in MANETs(Mobile Ad-hoc Networks): A Review

Er.Manpreet kaur
M.Tech Research Scholar
Amritsar College of Engineering and Technology ,Amritsar
Email:manu.uppal26@gmail.com

***Abstract*-MANET (Mobile ad hoc network) is an autonomous system in which mobile nodes are connected by wireless world. To forward packets ,each node operates as end system as well as router. The nodes are move freely and in a network all nodes organize themselves. The position of these nodes change frequently. One of the type of ad hoc network is MANET that can configure and change locations itself. Because MANET consists number of mobile users over slow wireless links to communicate. Since nodes are mobile, to connect to various network they use wireless connections. The main concern of the routing protocols of MANET is to establish efficient route between the communicating parties. Any attack in routing phase may destroy the entire network. Thus, security of the whole network mainly concern with security in network layer. This paper discusses the number of attacks in MANET.**

Keywords-Mobile ad hoc network (MANET),attacks, Jellyfish, Wormhole, black holes.

I.INTRODUCTION

MANET is a type of Wireless ad hoc network ,on the top of link layer it contains routable networking environment .In contrast to a mesh network ,MANET consist of a self configuring ,peer-to-peer network has a central administrator When mobile user is used, the session may not hold good and the communication may get hand-off. When the user is moving, the MANETS have main concern .To connect with different networks the MANETS use wireless networks. LANs are used to connect some of the MANETS and some MANETS are connected based on the application of the network to the internet. When they are not connected to any wireless routers even though these networks configure themselves. .Since MANET is a fixed infrastructure less, a number of attacks have been identified. To control the network traffic flow, an attacker can resolve the traffic by inject themselves between the source and destination into the path. Example of MANET

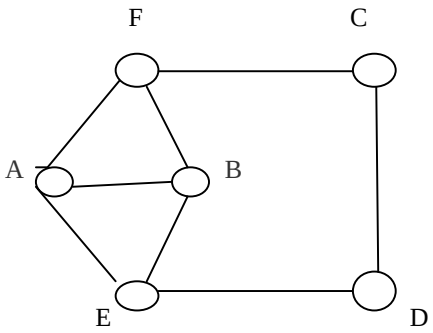


Fig.1. Example of MANET.

II. CHARACTERISTICS OF MANET

Various distinct characteristics which are provided by MANETs are as follow:

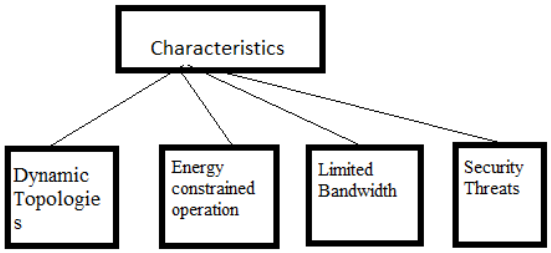


Fig.2. Characteristics

1. **Dynamic Topologies:** The variations in the structure of the network takes place when the nodes of the network keep on moving with different speeds.
2. **Energy-constrained Operation:** In the modern electronic world the devices mainly depend on batteries. In order to conserve the energy consumed by the mobiles, the design of the network is to be optimized.
3. **Limited Bandwidth:** Wireless network has very much limited bandwidth and within the limited bandwidth to perform with the

maximum efficiency the networks are to be optimized.

4. **Security threats:** Wireless communication is more affected than the wired communication for security. For secured transferred information the security of the MANET is to be optimized.

III. APPLICATIONS OF MANETs

- When Personal Area Networks (PAN) are taken into account, coverage need by them is less. MANETs serves the purpose where they need the very limited coverage
- It is easy to develop a wireless network rather than a wired network, at the time of disaster. MANET can be implemented, where wired network may be affected by the disasters.
- The MANET plays an important role in wireless communication and provides effective communication when there is a group effort required

IV. ATTACKERS

In mobile ad-hoc network, the nodes need restricted power supply, through which several problems will cause. When it is find that there is only limited power supply, a node may behave as a selfish node in mobile ad-hoc network. There are different types of attacker present in MANETs, which tries to reduce the performance of network. In this paper we study about various attackers, which are classified in the figure 2

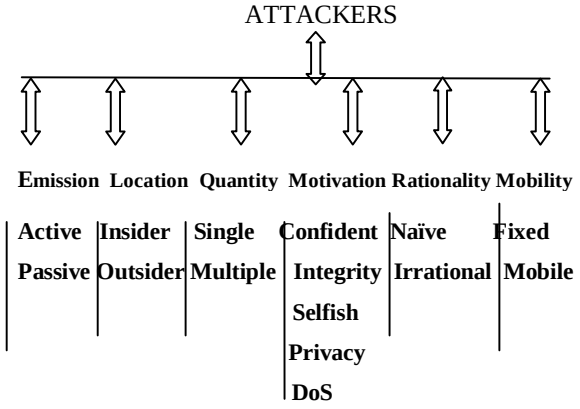


Fig.3. Attackers

V.ATTACKS IN MANETS

Mobile Ad hoc networks subject to various attacks from outside as well as from within the network itself. These attacks are mainly classified as two different levels. The first level of attacks are based on Internet connectivity Whereas the second level of attacks are based on mobile ad hoc networks . The attacks in MANETs are divided into two major types:

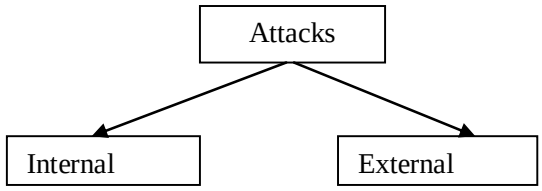


Fig.4. Attacks

A. Internal Attacks

The attacks that leads to nodes presents in network and links interface between them are called Internal attacks . Wrong type of routing information may broadcast to other nodes due to this type of attacks. As an internal attack occurs due more trusted nodes because of this sometimes these are difficult to handle. Compromised nodes or malicious nodes generated wrong routing information that is difficult to identify. Because by using their private keys, compromised nodes have the capability to generate the valid signature.

B. External attacks

Congestion in the network can be caused by these types of attacks like , advertising wrong routing information and denial of services (DoS). From normal communication external attacks are used to prevent the network and producing additional overhead to the network.

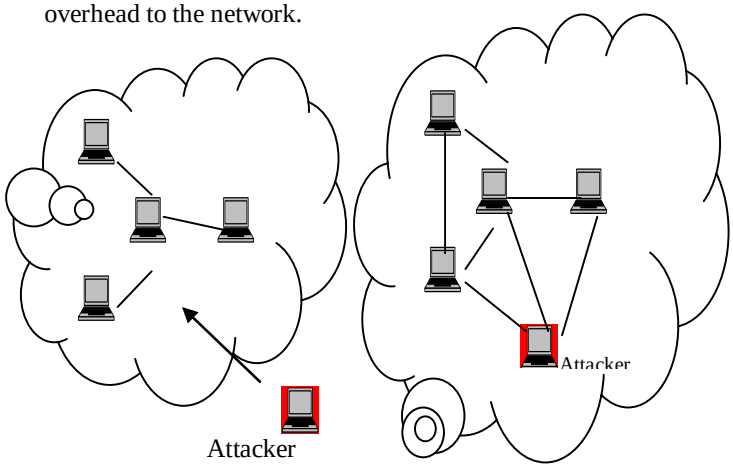


Fig.5. External and Internal attacks

External attacks can be divided into two categories:

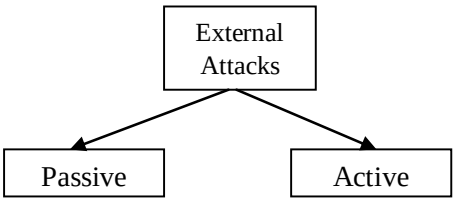


Fig.6. External Attacks

1) Passive Attacks: In passive attack to take idea about what communication is going on in the channel, the attacker silently listens the communication channel. There is no change or modification takes place in the message. Thus, in the network the confidential information that is being transferred through channel is known by the attacker. Powerful encryption algorithms are used to overcome this type of attacks by encrypting the data being transmitted.

2)Active Attacks: In active attack the attacker can modify, drop and destroy the original data. Active attacks can be of either internal or external. Internal attacks are carried out from malicious nodes which are inside of the network. Outside sources produced Active external attacks that do not belong to the network. External attacks are easy to detect than internal attacks. Compromised nodes or malicious nodes generally introduced the active attacks. Routing information can be changed by malicious nodes by introducing shortest path to the destination.

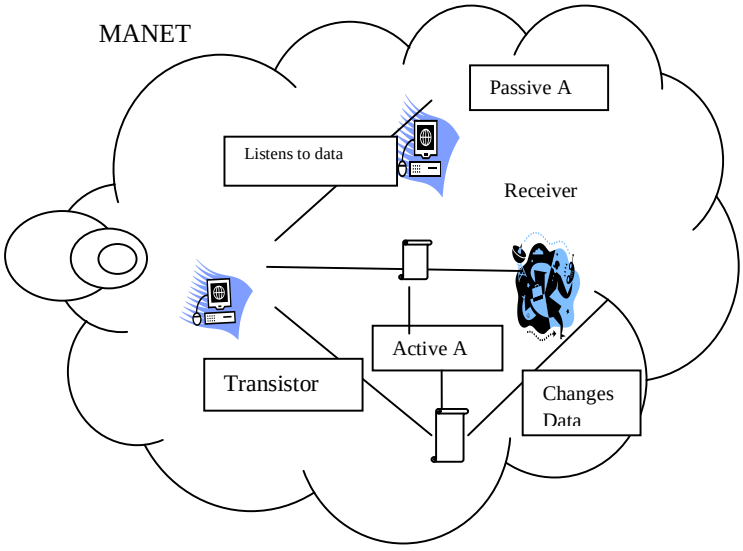


Fig.7. Active and Passive Attacks

Some of the Active attacks are as follows:

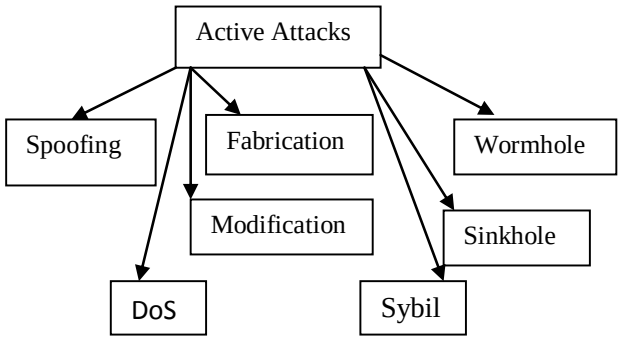


Fig.8. Active Attacks

a) Spoofing Attack: To alter the vision of sender, a malicious node absent his identity and sender change the topology.

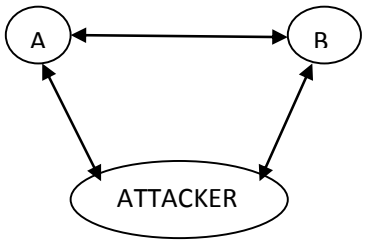


Fig.9. Spoofing Attack

b) Fabrication attack: The word "fabrication" refers to attacks performed by generating false routing messages. As they come as valid routing constructs, these type of attacks can be difficult to identify mainly in fabricated routing error messages, which clearly defines that a neighbor can no longer be contacted

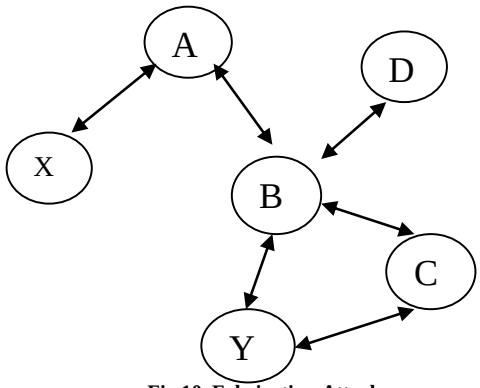


Fig.10. Fabrication Attack

c) Modification Attack: In these attacks the nodes modify routing, so that sender sends packets using

long route and may disrupt the overall communication network. Example of this attack is Sinkhole attacks.

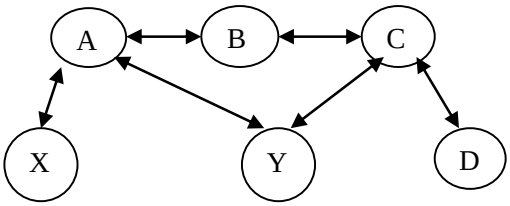


Fig.11. Modification Attack

d) Denial of Services: The aim of these attacks is to completely destroy the routing information. In this type of attack, to consume the bandwidth of the network malicious node sending the message to the node. The aim of malicious node is to be busy to the network node. When a message from the authorized node will come, the receiver will not able to receive the message because the network node is busy and sender has to wait for the receiver response**.**

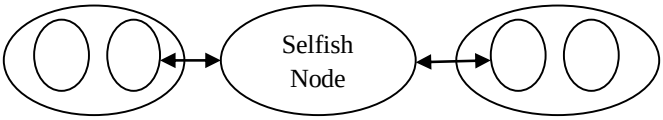


Fig.12.Denial of Attack

e)Wormhole Attack: Wormhole Attack is also known as tunneling attack. At one point an attacker receives packets and "tunnels" them to another point, in the network, in this attack. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole. The path which is used to send information is actually not the part of the actual network because of this wormholes are difficult to detect. Without knowing the network they cause damage so Wormholes are dangerous.

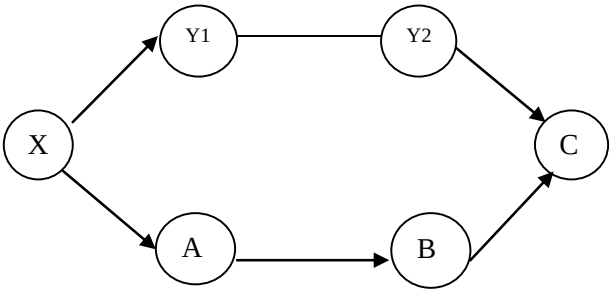


Fig.13. Wormhole attack

f)Sinkhole Attack: In sinkhole attack, the malicious node introduces that it has shortest path to the destination. Malicious node capture important routing information to use it for further attacks like dropping.

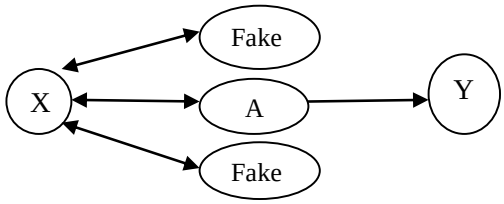


Fig.14. Sinkhole Attack

g)Sybil Attack: It pretends to be consisting of multiple malicious nodes with multiple fake identities in the network. So one node act as multiple nodes and can monitor multiple nodes at the same time. By this way number of nodes are increased that leads to increase in number of attacks. The Sybil attack mainly contained at distributed system environments.

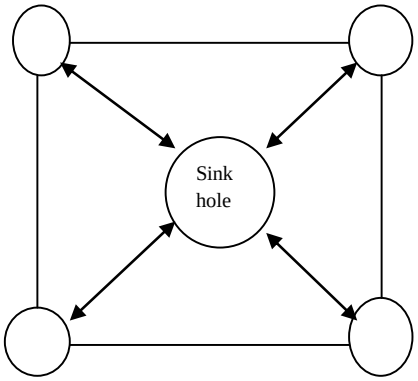


Fig.15. Sybil Attack

Some of Passive Attacks are as follows:

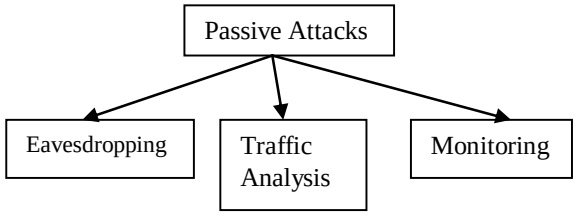


Fig.16. Passive Attacks

a)Eavesdropping: In Mobile ad-hoc network, one of the passive attack called eavesdropping occurred. In this attack during the communication the main concern is to know the confidential information that should kept secret. The sender and receiver may have

this confidential information as public or private key or any password.

b)Traffic Analysis: In this attack, to know the amount of data an attacker tries to understand the communication path between the sender and receiver. By traffic analysis no alteration is takes place in data..by destroying nodes traffic analysis can also be conducted as active attack to collect important information.

c) Monitoring: In this attack ,the attacker can read the confidential information but not able to change or modify this information.

Some other advance attacks are:

Rushing Attack: In this attack, an attacker takes the place between the path of the sender and the receiver. When sender transmits packets, the attacker firstly receives the packets and then forwards it to the receiver. The attacker creates duplicity by sending duplicate packets again and again and receiver receives these packets as original one .As the receiver continuously receives the packets so it remains busy .Due to this the efficiency of receiver is reduce.

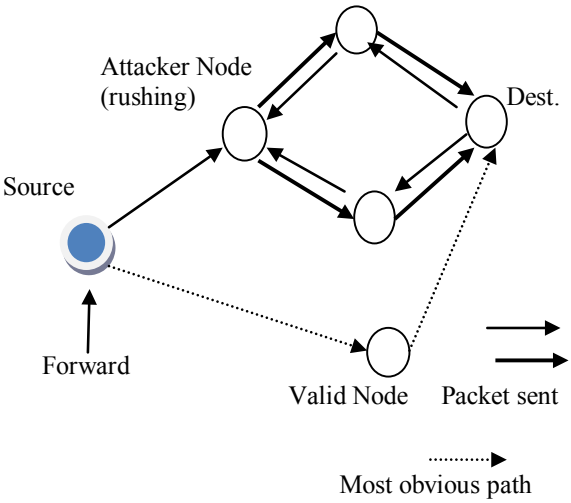


Fig.17.Rushing Attack

Jellyfish Attack: It results to end-to-end delay that affects the performance of the network. In this attacker attacks on the network by producing unwanted delays. In this attack, to become a part of the network the attacker first tries to take the access of the network. Once it get the access then it introduce the delays in the network by sending the packets with delays that it receive. Packets become free when delays introduced in the network.

Gray-Hole Attack: It is a type of an active attack. It is also known as misbehaving attack. The attacker in this attack, misguide the network by giving the permission to forward the packets. The attacker drops the packets that it receives from its nearby nodes then introduce DoS attack. The behavior of this attack is different in number of ways. While forwarding the packets, it drops the packets i.e. Node dependent. In other way it drop packets based on the predetermined time while behaving normal i.e. Time dependent

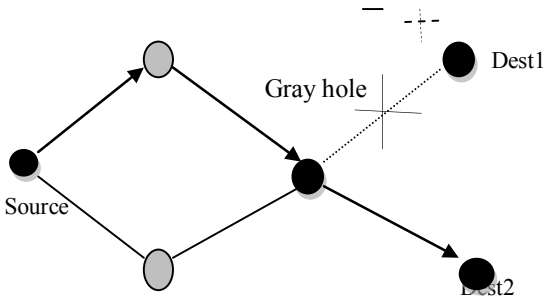


Fig.18. Gray-hole Attack

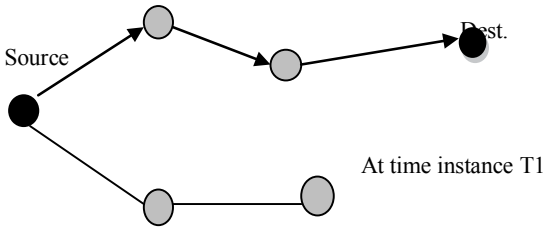


Fig.18a. Gray-Hole – Node dependent

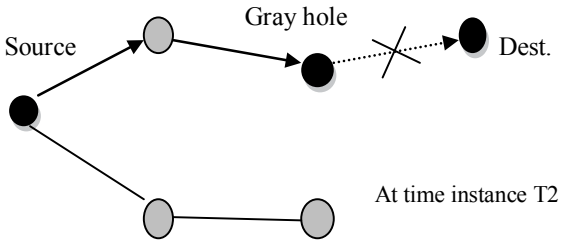


Fig.18b. Gray-Hole – Time dependent

Replay Attack: A node may repeat the data or delayed the data, in this attack. In this, originator receive the data and retransmit it. For example: A want to transmit data to B. It can only be done when A prove his identity to B and for identification A

sends his password to B. At that time, an attacker receive the password of A and introducing itself as A. When asked for the proof of identity. C sends A password from the last sessions, which B accepts.

Byzantine Attack: A compromised with set of intermediate, or intermediate nodes that working alone between the sender and the receiver within network and perform some changes such as creating routing loops ,forwarding packets through non – optimal paths or selectively dropping packets that leads to disruption or degradation of routing services within the network.

Jamming: It is a class of DoS attacks. Jamming attacks would reduce the performance of network. As the mobile hosts in MANET use wireless medium, a radio signal can be interfered or jammed due to which messages can be corrupted or lost. Thus if the attacker has a powerful transmitter .a strong signal will be generated to overcome the targeted signals and disrupt communication. A jammer can perform some attack strategies to interfere with other wireless communication are(constant jammer, deceptive jammer, reactive jammer and random jammer).

Black Hole Attack: It is one of the important attacks that introduce packet dropping that leads to packet loss. The black hole exits itself as a node that has shortest path to the destination node and as compare to all other nodes, sends its reply as early as possible. The source node consider this fake node as the path to destination and transmits all packets that are drained into the fake node creating an empty hollow.

Classification of Different Types of Attacks on Different Layers of the Protocol Stack

Table1: Classification of different types of attacks on different layers of the protocol stack[45]

Layer	Attacks
Application Layer	Repudiation, data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole, black hole, Byzantine, flooding, Resource consumption, location disclosure attacks
Data link Layer	Traffic analysis, monitoring, disruption MAC(802.11), WEP weakness
Physical Layer	Jamming, interceptions, eavesdropping
Multi layer attacks	DoS, impersonation, replay, man-in-the-middle

VI.CONCLUSION

Table2: Mapping the attacks (active or passive) with the layers [48]

Attacks	Active attack	Passive Attack	Layer
Spoofing	✓		Network Layer
Fabrication	✓		Multi Layer
Modification	✓		Multi Layer
Wormhole	✓		Network Layer
DoS	✓		Multi Layer
Sinkhole	✓		Network Layer
Sybil	✓		Network Layer
Eavesdropping		✓	Physical Layer
Traffic Analysis		✓	Data link Layer
Monitoring		✓	Data link Layer
Black hole	✓		Network Layer
Rushing	✓		Multi Layer
Replay		✓	Multi Layer
Location Disclosure	✓		Network Layer
Byzantine	✓		Network Layer

The ad hoc network is error free network, wireless, dynamic so they are prove to various kinds of vulnerable attacks. These networks have vast potential .in this we conclude network layer is most vulnerable than all other layer in MANET. We pay attention towards the potential countermeasures currently used and designed especially for MANET .nodes can be attached and removed at any time .this network is very much sensitive towards various attack out of which black hole attack is described by knowing the trust and threshold value black hole node is identified.

VII.REFERENCES

[1] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, 1996.
[2] A. Tanenbaum, *Computer Networks*, PH PTR, 2003.
[3] L. Zhou and Z. Haas, Securing Ad Hoc Networks, *IEEE Network Magazine*

Vol.13 No.6 (1999) pp. 24-30.
[4] S. Yi, P. Naldurg, and R. Kravets, Security Aware Ad hoc Routing forWireless
Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.
33
[5] H. Luo and S. Lu, URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks, *IEEE/ACM Transactions on Networking* Vol.12 No.6(2004) pp. 1049-1063.
[6] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. *Ad Hoc Wireless Networks*, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364, 2003.
[7] S. Burnett and S. Paine, *RSA Security's Official Guide to Cryptography*, RSAPress, 2001.
[8] M. Ilyas, *The Handbook of Ad Hoc Wireless Networks*, CRC Press, 2003.
[9] S. Yi and R. Kravets, Composite Key Management for Ad Hoc Networks. *Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services* (MobiQuitous'04), pp. 52-61, 2004.
[10] M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.
[11] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks. *Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA'02), pp. 3-13, 2002.
[12] A. Perrig, R. Canetti, J. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol. Internet Draft, 2000.
[13] P. Papadimitratos and Z. Haas, Secure Routing for Mobile Ad Hoc Networks. *Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference* (CNDS 2002), 2002.
[14] W. Mehuron, Digital Signature Standard (DSS). U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL). FIPS PEB 186, 1994.
[15] Y. Hu, A Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks inWireless Ad Hoc Networks. *Proc. of IEEE INFORCOM*, 2002.
[16] H. Deng, W. Li, and D. Agrawal, Routing Security in Wireless Ad Hoc Networks. *IEEE Communications Magazine*, vol. 40, no. 10, 2002. 34
[17] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. *Proceedings of the ACM Workshop on Wireless Security*, pp. 21-30, 2002.
[18] P. Papadimitratos and Z. Haas, Secure Data Transmission in Mobile Ad Hoc Networks. *Proc. of the 2003 ACM Workshop on Wireless Security*, pp. 41-50, 2003.
[19] Y. Hu, A. Perrig, and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. *Proc. of the ACM Workshop on Wireless Security* (WiSe), pp. 30-40, 2003.
[20] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. *Proc. of MobiCom 2002*, Atlanta, 2002.
[21] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communications*, pp. 38- 47, 2004.
[22] C. Perkins, *Ad Hoc Networks*, Addison-Wesley, 2001.
[23] R. Oppliger, *Internet and Intranet Security*, Artech House, 1998.
[24] B.Wu, J.Wu, E. Fernandez, S. Magliveras, and M. Ilyas, Secure and Efficient Key Management in Mobile Ad Hoc Networks. *Proc. of 19th IEEE International Parallel & Distributed Processing Symposium*, Denver, 2005.
[25] L. Buttyan and J. Hubaux, Report on Working Session on Security in Wireless Ad Hoc Networks. *Mobile Computing and Communications Review*, vol. 6, 2002.
[26] S. Ravi, A. Raghunathan, and N. Potlapally, Secure Wireless Data: System Architecture Challenges. *Proc. of International Conference on System Synthesis*, 2002.
[27] W. Stallings, *Wireless Communication and Networks*, Pearson Education, 2002.
[28] N. Borisov, I. Goldberg and D.Wagner, Interception Mobile Communications: The Insecurity of 802.11. *Conference of Mobile Computing and Networking*, 2001.
[29] P. Kyasanur and N. Vaidya, Detection and Handling of MAC Layer Misbehavior in Wireless Networks. *Proc. of the International Conference on Dependable Systems and Networks*, pp. 173-182, 2003. 35
[30] A. Crdenas, S. Radosavac, and J. Baras, Detection and Prevention of MAC layer Misbehavior in Ad Hoc Networks. *Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 17-22, 2004.
[31] C. Kaufman, R. Perlman, and M. Speciner, *Network Security Private Communication in a Public World*, Prentice Hall PTR, A division of Pearson Education, Inc., 2002
[32] S. Capkun, L. Buttyan, and J. Hubaux, Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. *Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.
[33] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M. "An Overview Of security Problems in MANET".
[63] Wenjia Li and Anupam Joshi. "Security Issues in Mobile Ad Hoc Networks- A Survey".
[34] Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006
[35] Shobha Arya1 And Chandrakala Arya2, "Malicious Nodes Detection In Mobile Ad Hoc Networks", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.
[36] YihChun, Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad -Hoc Network Routing Protocols", *WiSe 2003*, September 19, 2003, San Diego, California, USA.Copyright 2003 ACM 1581137699/03/0009
[37] V. Palanisamy1, P.Annadurai2, "Impact of rushing attack on Multicast in Mobile Ad Hoc Network", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009
[38] S. Albert Rabara1 and S.Vijayalakshmi2, "Rushing Attack Mitigation In Multicast MANET (RAM3)", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 4, December 2010
[39] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay**, "**Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3)
[40] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless, Sensor Networks; the Intruder Side". Athens Information Technology, 19002 Peania, Athens, Greece.
[41] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, **"**A survey on attacks and countermeasures in mobile ad hoc networks**",** Springer, 2006.
[42] Ms.Supriya and Mrs.Manju Khari, "MANET security breaches: Threat to a Secure communication platform", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012
[43] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", *International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.*
[44] Sheenu Sharma, Roopam Gupta, "Simulation study of blackhole attack In the mobile ad hoc networks", Journal of Engineering Science and Technology Vol. 4, No. 2 (2009).

[45]Joshi Parveen , "Security issues in routing protocols in MANETs at network layer", WCIT 2010.
[46]Chandrasekar.A.Manoranjini, "Hybrid Detector for Detection of Black Holes in Manets",International Conference on Electronic and computer Science 2013.
[47]Wu Bing ,Chen jianmin , Wu jie, Carderi Mihaela, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks",Springer 2006.
[48] Jain Sonali , "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc Network", Satyam Shrivastava et al./ International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 03 Mar 2013.
[49] Manjeet Singh, "A Surveys of Attacks in MANET ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

""""

Multi-Hop Routing Optimization Method for Vehicle to Roadside Network

Er.Kuljeet Kaur

M.Tech Research Scholar

Amritsar College of Engineering & Technology, Amritsar

Email-id:-petra.nikhanj@gmail.com

ABSTRACT

A route optimization method to improve the performance of route selection in Vehicle Ad-hoc Network(VANET).Based on the analysis of movement characteristics of vehicles and according to the relationship between the vehicles and roadside units.When the vehicle moves into the range of several different roadsides, it could build the route by sending some route testing packets as ants,so that route table can be built by the reply information of test ants, and then the node can establish the optimization path to send the application packets.Most hierarchical routing and clustering protocols are designed to be efficient when the data is sent from the sensor nodes to their cluster-head but not when it is sent the opposite way.Multi-hop and fault-tolerance routing protocol able to transport data from sensor nodes to their cluster-head and vice versa in an energy-efficient way is also presented.

***Keywords*:**Multi-hop routing optimization,VANET,Wireless sensor and actor networks

I. Introduction

With the rapid development of automotive electronics, more and more electronic equipments are adopted in automotive applications.A wide variety of the applications which are aimed to improve road safety or provide comfort for passengers in Vehicles are intended to be delivered in Vehicle Ad-hoc Networks(VANET) in the future.The VANET is characterized by high node speed,which rapidly changes topologies,multi hop, and self-organization.As a matter of fact,the VANET can be envisioned as a mobile platform for road traffic monitoring which Will replace more roadside sensor network devices.The vehicles can use the roadside gateway to connect the data server and collect the data which regard the local observed traffic, such as the state of highway in bad weather, real-time traffic information;even GPS map information updated online and so on.Every driver can collect data and share the necessary information with the public sever through

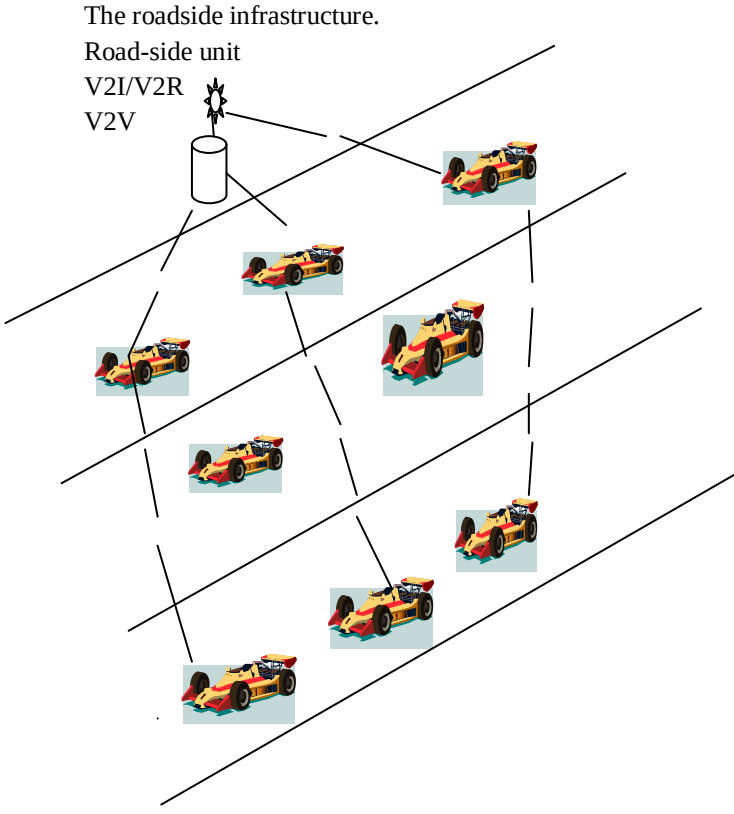


Fig.1.Vehicle to roadside communication

A new way of distributed computing where hundreds of small devices are able to collaborate in a wireless way is more and more present in our daily life.Sensor nodes,also known as "motes", are able to practically sense and monitor any kind of environment thanks to the fact that any kind of sensor can be attached to these devices.In addition, special devices, called "actors" , can take advantage of the collected information in order to act and modify the environment.WSANs(Wireless sensor and actor networks) allows us to develop a variety of interesting applications which were very difficult to carry out.WSANs are formed by devices with poor resources such as storage, energy, computation, memory, communication and so on.Another important topic is the use of routing mechanisms for clusters.Efficient routing protocols are needed in order to transport the data within a cluster in both directions, from the nodes to the cluster-head and vice versa.Normally, within a cluster the most frequent communication is carried out from the nodes to the cluster-head.Our work is a contribution to the WSAN research field in the sense that it effectively provides the following innovations:

- Cluster formation is carried out without using energy-inefficient protocols like flooding or multicast thanks to meta-data stored in the nodes before they are deployed.
- Developers will be able to specify the desired level of reliability between sensor nodes and their cluster heads, and viceversa in a quantitative way.
- To make this kind of communication more efficient we propose two concepts: memory path and clue-node.
- As overall contribution, the approach presents a powerful, efficient and robustness protocol which can be easily integrated with the application to carry all the communication process.
- Most papers published so far only have as the main goal achieving an efficient communication when the packets are sent from the sensor nodes to their cluster-head.We also provide an efficient mechanism to carry out this kind of communication, but we also consider important the communication carried out from the cluster-head to the sensor nodes.
- Clue-node helps the cluster-head to estimate the zone where the packets have to be sent

II. HERO protocol

HERO is the hierarchical routing protocol designed to allow an efficient, reliable and multi-hop bidirectional communication among nodes which belong to different tiers, so that the developers can organize a WSAN with as many tiers as they need.The most used architectures are those based on 2-tiers so, there is one tier where the sensor nodes are grouped in clusters and recollect information which is transmitted to the cluster-head and there is another tier formed by cluster-heads which aggregate the data received from the sensor nodes which is transmitted to the base station.HERO is a general and scalable solution which allows us to communicate nodes of a WSAN in a multi-hop way independently of the number of desired tiers.

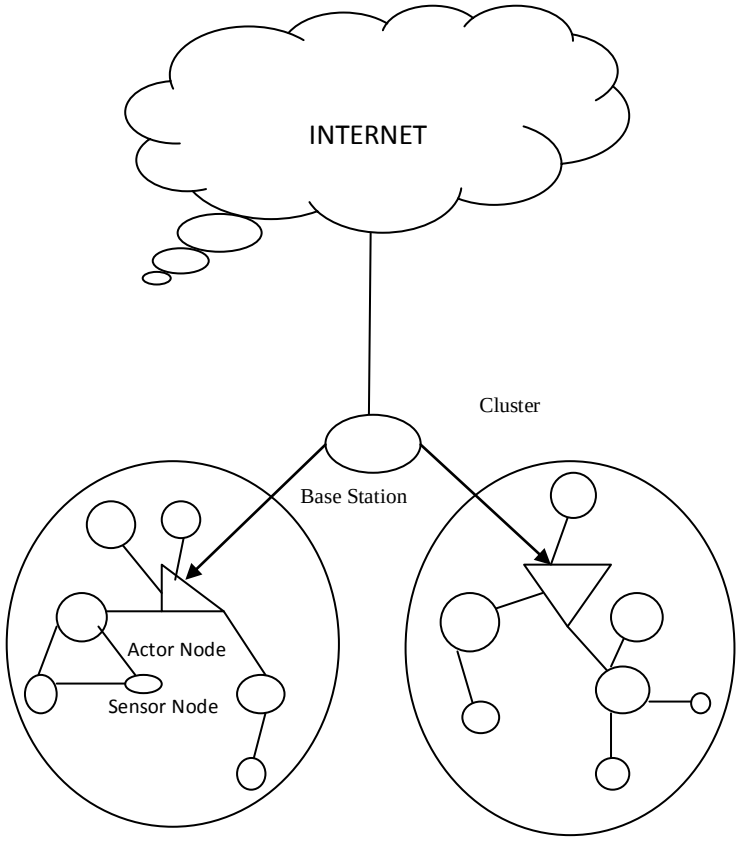


Fig.2 Wireless sensor and actor network.

Throughout this section the proposed protocol to achieve the two main communication patterns between nodes

and the cluster-head will be explained in details. Both communication patterns are known as event-driven and query-driven.In the former, the direction communication is carried out from the sensor nodes to their cluster-head.This model is used by all the WSAN applications as it is the suitable model to carry out any type of monitoring owing to the fact that during this activity sensor nodes collect information from the environment where they are deployed and they send it to the cluster-head.

III. PIACO algorithm in AODV

How to find the optimal path to avoid the routing handoff if possible is an important problem in the VANET. So we propose the modified PIACO-AODV algorithm to improve the performance of the packet delivery fraction, end-to-end average delay, and routing overhead. The algorithm flowcharts are shown in Fig.3 and Fig.4.

Fig.3 is the flowchart of source node initiating route discovery.It starts when the vehicle moves into the range of the roadside unit.

As shown in Fig.3 and Fig.4, the main steps of the PIACO-AODV algorithm are explained as below.

Step 1: Initialize the parameters in the system at the start time, such as the initial pheromone, the speed and the direction of vehicle, the source node and destination node, and other necessary information.

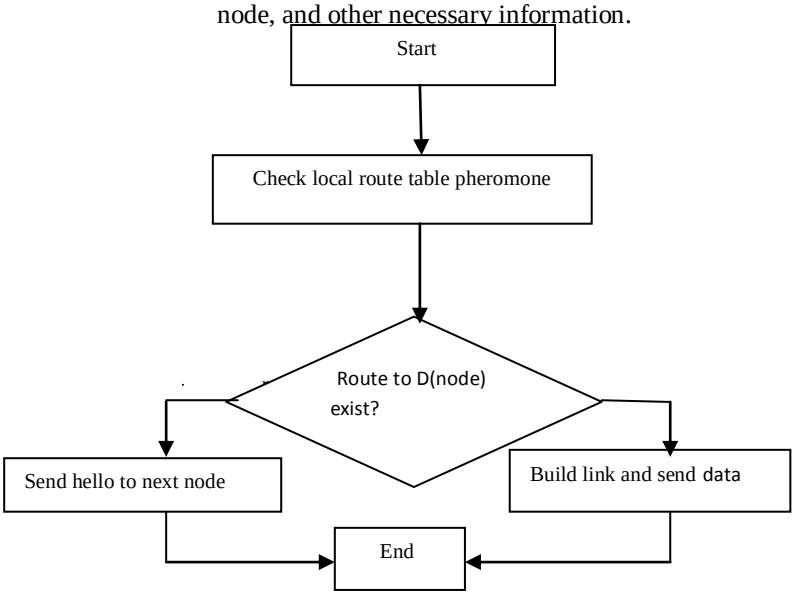


Fig.3. The flowchart of source node initiating route discovery

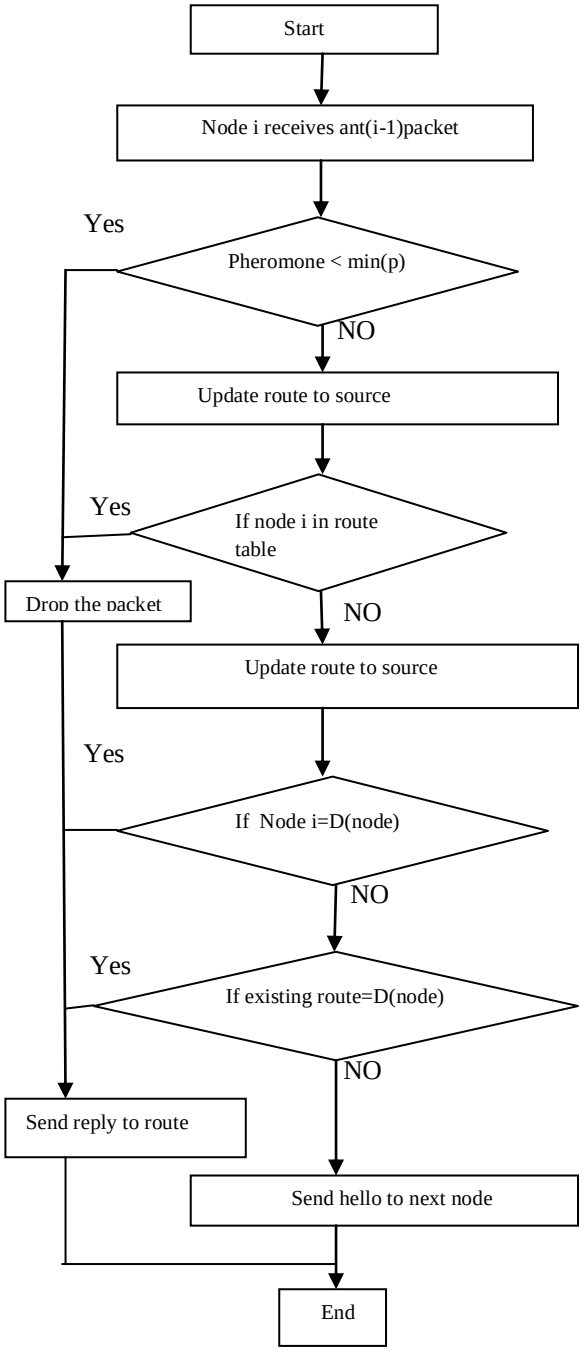


Fig.4.Flowchart of route searching of the middle node

Step 2: Start from the source node, and every node begins to choose the route according to the pheromone which is decided by the PIACO-AODV algorithm.

Step 3: Update the pheromone on every path after the cycle time.

Step 4: Generate the route for the ants.

Step 5: Send the optimal route to the source.When the optimal route is found in limited periods, the route will be sent to the source and the route information will be maintained.If the route information is changed, the path should be rebuilt.

Step 6: According to Step 5, all the nodes choose the optimal route from the source node to the destination node.

IV. Related work

Owing to the fact that both clustering and routing res two really important issues in the WSANs field, a large number of papers have been published trying to address them.

Almost all routing protocols can be classified as flat, data- centric, hierarchical and location-based protocols.Maybe the most proper kind of approach to organize and establish communication between the nodes of a WSAN is that based on hierarchical protocol.

V. Ant Colony Optimization

ACO algorithm is biologically inspired from the behaviour of colonies of real ants, and in particular how they forage for food. This algorithm proposed by Dorigo M and co-workers in 1996 is a novel heuristic evolutionary optimization algorithm.It can point out a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality.ACO has been applied to many problems, e.g. Traveling Salesman Problem(TSP), Sequential Ordering Problems(SOP), and Open Shop Scheduling(OSS) problem.The ACO algorithm are the effective ways to solve the feature selection problems.

The ants in ACO algorithm can be represented as some special packets in the vehicle ad-hoc network, and we configure some rules according to the algorithm for the packets.These packets can be sent in Internet Protocol level.

VI. Routing attacks

We use an attackers framework implemented in ns-2 to launch four types of scout and forager related attacks on iBeeAIS.In each attack scenario, we monitor the routed traffic at three points in the network-node2,node5 and node 7- and then generate traffic maps to indicate the success or failure of the attack.we now discuss the details of each attack.

Attack-1:Forging Forward scout: This attack is launched 100s after the start of simulation, when initial route discovery is complete.The attacker node 4 launches fake forward scouts to install a forged route 0-1-2-3-4-8. The attack rate is approximately 12-13 fake scouts per second.The fake packets have node 0 as source and node 8 as destination.

Attack-2:Forging Backward Scout:

The attack involving spoofed backward scouts is launched by Node 2 at time t=100s. Forged backward scouts are generated at the rate of approximately 11-12 scouts per second with Dsct as node 8.

Attack-3:Forging Spoofed Forager:

At t=50s, the attacker node 5 sends forged foragers to install a forged path 0-1-2-3-4-8 at node 0. The attack packet rate is approximately 4 forgers per second.The routing information is also modified in forged packets;delay value carried in packet header is artificially reduced to misrepresent the shortest path.

Attack-4:Modifying Forager Route Information: In this attack, the malicious node 7 artificially increases the route delay values in the foragers returning from node 8 to node 0; thus making the path 0-7-8 undesirable.The attack is launched at simulation time t=100s.

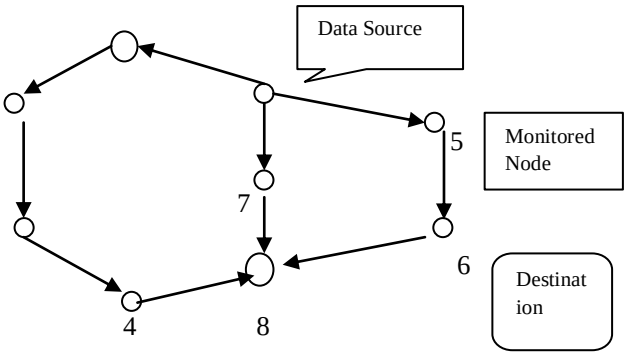


Fig.5. Node topology selected for attacks

VII. Results and discussion

After the model was built, a simulation was carried out to test performance of PIACO-AODV and the traditional AODV with NS-2.The test field was 1000 m multiply 1000m. The number of artificial ants in the colony is 30. The cover range of roadside device is 200m, and the test time is set to 300 s. CBR is the data source, and every packet is 512 bytes.In order to reflect the better performance of the modified AOC in the experiment, we tried many different combinations of parameters.

The end-to-end average delay at different speeds of the node is tested.The number of nodes is set to 50.The PIACO-ADOV algorithm has better performance than AODV.

VIII. Conclusion

In this paper, we present an improved AODV protocol with ACO algorithm in VANET.The proposed algorithm changes the route selection method in the AODV protocol.By modifying the value of the pheromone evaporation rate, the node could choose the better route in two main route discovery steps with higher possibility.In addition, we employ the position information in the new protocol, so that node could maintain a more stable routing.The experimental results show that the new protocol has more effective performance of than AODV.By changing the parameters in ACO, the algorithm could find the optimal route more quickly, which enchances the efficiency of the whole system.The results also represents that the new algorithm can reduce the handoff frequency in a given time,improve the routing path duration, and the transmission efficiency of merssage.In this we presented HERO, a novel hierarchical protocol that,thanks to its design and features is a fault-tolerance,energy-efficient and reliable protocol in the context of wireless sensor and actor networks

IX. Future Scope

The important contribution of this paper is to demonstrate the benifits of combining relevant features of the innate and adaptive immune systems.

iBeeAIS, can be further enchanced by utilizing more signal types-PAMPs danger signals, safe signals, etc- to develop a sophisticated signal processing algorithm to determine the context of a DC.A system with these features can scale to a number of heterogeneous network environment

Research in this direction will be the subject of our forthcoming publications.

X. References

[1] I. Akyildiz, I. Kasimoglu, Wireless sensor and actor networks: researchchallenges, Ad hoc Networks 2 (4) (2004) 351–367.

[2] J. Gehrke, L. Liu, Guest editors' introduction: sensor-network applications, IEEE Internet Computing 10 (2) (2006) 16–17. <http://doi.ieeecomputersociety.org/10.1109/MIC.2006.31>.

[3] G.W. Kirsten West, K. Hall, Research and markets: wireless sensor network technology trends report Q4 2010, 2010.

[4] A. Abbasi, M. Younis, A survey on clustering algorithms for wireless sensor networks, Computer Communications 30 (14–15) (2007) 2826–2841.

[5] E. Felemban, C.-G. Lee, E. Ekici, Mmspeed: multipath multi-speed protocol for qos guarantee of reliability and timeliness in wireless sensor networks, IEEE Transactions on Mobile Computing 5 (6) (2006) 738–754.

[6] C. Schurgers, M. Srivastava, Energy efficient routing in wireless sensor networks, Military Communications Conference, MILCOM 2001, Communications for Network-Centric Operations: Creating the Information Force, vol. 1, IEEE, 2001, pp. 357–361. http://dx.doi.org/10.1109/MILCOM.2001.985819.

[7] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, in: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, MobiCom '00, ACM, New York, NY, USA, 2000, pp. 56–67. http://dx.doi.org/http://doi.acm.org/10.1145/345910.345920.

[8] W. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive protocols for information dissemination in wireless sensor networks, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, New York, NY, USA, 1999, pp. 174–185.

[9] M. Younis, M. Youssef, K. Arisha, Energy-aware routing in cluster-based sensor

networks, in: Proceedings of the 10th IEEE International Symposium on
Modeling, Analysis, and Simulation of Computer and Telecommunications
Systems, MASCOTS '02, IEEE Computer Society, Washington, DC, USA, 2002, p.
129. <http://dl.acm.org/citation.cfm?id=882460.882620>.
[10] K. Iwanicki, M. van Steen, On hierarchical routing in wireless sensor networks,
in: Proceedings of the 2009 International Conference on Information
Processing in Sensor Networks, IPSN '09, IEEE Computer Society,
Washington, DC, USA, 2009, pp. 133-144. <http://dl.acm.org/citation.cfm?id=1602165.1602179>.
[11] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient
communication protocol for wireless microsensor networks, Proceedings of
the 33rd Hawaii International Conference on System Sciences HICSS '00, vol. 8,
IEEE Computer Society, Washington, DC, USA, 2000, p. 8020. <http://
dl.acm.org/citation.cfm?id=820264.820485>.
[12] S. Muruganathan, D. Ma, R. Bhasin, A. Fapojuwo, A centralized energy-efficient
routing protocol for wireless sensor networks, IEEE Communications Magazine
43 (3) (2005) S8–13, http://dx.doi.org/10.1109/MCOM.2005.1404592.
[13] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, An application-specific
protocol architecture for wireless microsensor networks, IEEE Transactions on
Wireless Communications 1 (4) (2002) 660–670, http://dx.doi.org/10.1109/
TWC.2002.804190.
[14] S. Lindsey, C. Raghavendra, Pegasis: power-efficient gathering in sensor
information systems, Aerospace Conference Proceedings, vol. 3, IEEE, 2002,
pp. 3-1125–3-1130. http://dx.doi.org/10.1109/AERO.2002.1035242.
[15] M. Khan, G. Shah, M. Ahsan, M. Sher, An efficient and reliable clustering
algorithm for wireless sensor actor networks (wsans), in: 53rd IEEE
International Midwest Symposium on Circuits and Systems (MWSCAS),
2010, pp. 332–338.

Handling of Mobile Adhoc Network Problems Using Different Techniques

Er. Name Sahil Sharma

MTECH Research Scholar

AMRITSAR COLLEGE OF ENGINEERING AND TECHNOLOGY, AMRITSAR

E-mail:- meetsahil2811@gmail.com

Abstract

As with the Increase of the use of the Mobile phones (Smart phones), the various types of the new applications are being developed day by day.

Also along with this, the various problems are also increasing such as HTTP attack, Black hole attack distributed node exhaustion attacks and various other epidemics. We will basically detect the affected system using the T-cover problem which is basically the NP complete. We process through the simulations using the NS-3 simulators. The three n-grem technique to the problem of HTTP attack detection is applied in the terms of the accurecy and the problems.

These techniques are applied to the highly realistic dete set consisting of various mager attacks. But results indicate the byte level analysis is basic as well as prectical approach.

In order to teckle the black hole attack, the path and rooute of AODV routing protocol is selected in the way that the most trusted nodes get involved. The not trusted node can be easily excluded from the path. The Simulation results are shown through the

OMNET++ Simulations where the higher threshold valuesresponsible for less packet drops and releible communication network.

The pattern recognition for detecting distributeted node exhaustion attack is evaluated through simulation experiments in terms of participation in detection process for achieving a level of attack detection accurecy.

A Study of defence against clock skew replication contributes to issue by realizing a replication attack of a fake clock skew and developement od counter measure in wireless senscr environment. This basically caluclates the time difference between the attacker node and imitated one, which is measured by the victim node. This approach is applicable when packets are send at the fixed time intervals. The time period of synchronisation changes frequently.

Keywards:

HTTP attack, ngrem analysis epidemics, Black hole attack, AODV pattern recognisation Introduction

(I) Introduction

Round about 4500 new web based attacks were found. Web application servers gets commonly tergeted for these attacks.

Most of HTTP traffic contains only printable ASCII charectors. Any executable code in incoming HTTP packets is not expected. The byte distribution of printable ASCII is restricted then executable code. So the amalysis of bytes distribution in HTTP packets can be used to setect various classes of attacks.

The techniques are basically based on hidden markov models and ngrem analysis n grem model is applicable to raw bytes in HTTP packets. It was applicable to problem of file type classification used to classify files as execuitable, text or multimedia.

The basic objective is to determine the strength and weaknesses of relatively straight forward n-grem analysis as compared to HMM based technique.

As with the introduction of Android, the wireless devices with complex capabilites and open source of operating system has increased with the introduction of a new propagation vector for mobile melware. The basic focus is an propagation melware in the context of wired networks also various short renge communcationsuch as Wi-Fi and Vluetooth uisng the mean field compartmntal Models.

The basic concept of healers to mimic the recovery process in a standard epidemic model is also introduced.

A novel healer placement stretegy using blue noise distribute is also proposed.

Three families of healer protocols: rendomized (RH), profile (PH) an prediction (PDH) are also designed to allow for the trade off between energy consumed for sending petches and time taken to recover full system.

As the MANET has no fixed infrestructure so it gets affected from various attacks such as passive attacks and active attacks.

In passive attacks, the attackers silently listens the communication chennel to know the confidential information being transfeerd from chennel.

In active attacks, the attackes destroys, drop and can modify the original data.

The black hole attack is responsible for the packetloss.

So according to AODV routing protocol, a high so sequence no. is assigned to node that can takes part in rout discovery process of AODV routig and source and destination of the actual route is estaiblished so as to transmit data safely.

As the wireless sensor network have emerged as a magcr source of collection of data based on sensing of the environment of sensor nodes.

It is necessary to protect these networks from various attacks.

Basically the distributive node exhaustion attacks are launched from various ends of a network to the set of victim node with the exhaust of limited resouces.

A distributed patern recognition scheme for distributed node exhaustion attack detection in wireless sensor network is defined.

An alforithm to imitate a nodes's clock skew under the time stamp's unproteched and eavsdropped is also provided with an approach to launch a replication attack on clock skew based node identification.

(II) Detectio techniques

x2 Distance

The x2 distance between the n grem relative frequency distribution of a given packet and expected relative frequency distribution of benign traffic is considered.

The traning phase consists of collection of n-grem statistics from benigntraffic.

We compute

$$D^2(X,Y) = \sum_{i=1}^{N} \frac{(X_i - Y_i)^2}{Y_i} \quad \text{(i)}$$

Where X is relative n-grem frequency of incoming packet

Y is relative n grem frequency distribution of benign treffic.

N is no of distant n-grems.

Suspect packet frequencies

Byte B1	Frequency
B_1	6
B_2	0
B_3	11

Ad-hoc n gram

Ad-hoc technique is similar to the x2 distance with a modified scoring function where x2 test is closely related to Euclideen distance. This approach can outperform x2 test in some cases here, firstly the relative n-grem frqencies y of benign traffic is introduced.

$$d(X,Y) = \left(\sum_{i=1}^{N} |X_i - Y_i| \right)^2 \quad \text{(ii)}$$

x, y, n are same as previous

(III) Pattern counting

Patterm counting is used to distinguish between executable files and text files. It is trained by determining distinct n- grem of bytes which appear in benign HTTP raffic. It attarective featue is that it can be implemented in an extremely efficient manner even for large values of n.

Effective Healer Placement

The healer placement puts effect on defense protocols and their coverege areas depends on their placement stretegy. A naive placement using uniform rendom distribution results in a scenario where many healers ended up covering the same region leaving a lot of uncovered area.

For healer placement strategy basically we need a type of a constreint which rejects various configurations those place healers very close to eachother. This can be directly reduced to the problem from field of computer vision which involves sampling pattern with a blue noise fourier spctrum. This problem can be defined as the limit of a uniform sampling with minimum rejection criterion. Successive points can be independently collected from the uniform distribution. If a point is at distance of at least R from all points in the accepted points, it is added to that set oherwise refected.

(IV) Family of Random Ized Healers

A healer have to decided to send a patch of the no. of nodes in its vicinity. It contains an initialization phase and an execution phase wherehealers prepares to deliver a patch. It picks a random time from the interval (o.T) where T is epoch length and used to schedule a broadcast called the patch timer.

It may send more patches then needed since thay decided to send patches regerdless of how many infected nodes are present in proximity.

(V) Family of Profile Healers

The healer attempts to learn the arrival distribution od nodes and subsequently determine if or not it is cost effective to deliver a patch.

An initialization phase prepares the healer passively records the number of neighbours it is observing during each epoch and an execution phase utilizes information learnt during the previous phase to decide whether or not to deliver the patch.

Its limitations are as it require to wait until the end of learning phase to start healing of system.

The healers lern and estimate the threshold only once.

To address these limitations, we adopt a hybrid approach where healers perform online and had the system simultaneously.

This approach is an extension of PHB algouithem.

(VI) Clock Skew Terminology

The clock skew of every physical device differs and so is suitable for device identification network communications. This study contributes to this issue by realizing a replication attack of an indistinguishable fake clock skew and by developing its countermeasure in a wireless sensor network environment. Our method calculates the time difference between the attacker node and the imitated one, which makes the biased timestamps of the attacker node's packets, when measured by the victim node. Clock skew is the difference between the clock frequencies of two clocks. The terminology used to represent the clock characteristics, therefore, can be defined as follows:

1. Offset: The difference between the time reported by C_r and by C_s, e.g., the offset of the receiver clock Cr relative to the sender clock C_s *is* $C_r(t)$-$C_s(t)$.
2. Frequency: The rate at which a clock progress, e.g., the frequency at time *t* of C_r is $C_r(t)$. The frequency of true time is then 1.
3. Skew: The difference in frequency of two clocks, e.h., the skew of C_r *relative to* C_s *at time t is* $C_r(t)$-$C_s(t)$

(VII) Clock skew-based node identification

The clock skew of any clock is stable under normal temperature; second, every stable clock skew is considered unique and thus there exists a distinguishable relative clock skew between any two physical devices. Clock skew can be used as a fingerprint of any device with a digital clock.

Clock skew can be used to provided an end to-end method to detect virtual sensor nodes, wormholes and Sybil-attacks in WSNs.

Only the sink node can execute the clock skew-based identification method the sink node itself does not send out its time information to others.

In-network: every node can use the clock skew to check the identity of its neighbor nodes as proposed. The in-network method can be used to identify sensor nodes in WSNs by utilizing a two-tier clock skew filter. The clock skew can be a practical tool to represent the identity of a device. The results of previous analysis confirmed that clock skews can be used to represent the fingerprints of sensor nodes and

that the method be used to defend against a Sybil attack.

(VIII) QoS of MANet Through Trust Based AODV Routing Protocol

The 'trust value' is calculated against all the intermediate nodes. This trust value is calculated depending upon the ability to forward packets and the RREQ forwarding ability of a node. Two weight factor W1 and W2 are introduced. W1 is the ratio of number of packets sent from a node to the number of packets received to that node. W2 is the ratio of number of RREQ received to number of RREP sent. This trust value is saved in the routing table of that node. And in the route discovery step of AODV routing protocol the path is established according to that trust value rather than the shortest Path.

Algorithm

Step 1

Count the number of packet received at each node.

Count the number of packet sent by each node.

Count the number of PREQ received at each node.

Count the number of PREP sent by each node.

Step 2

Calculate the threshold value: $W_1 = \frac{Number\_of\_packet\_sent}{Number\_of\_packet\_received}$

Calculate the weight factor: $W_2 = \frac{Number\_of\_Rout\,Re\,ply\_sent}{Number\_of\_Routequest\_received}$ (iv)

Step 3

Increase the ptrust value when threshold value is greater than the threshold value. Otherwise descrease the ptrust value.

Step 4

Calculate Trust Value=W_1 *W_2* ptrust

Step 5

Insert Trust Value into routing Table.

Step 6

Route establishment according according to Routeing Table

Rest of the part is similar to the traditional AODV Routing Protocol.

(IX)Threshold pattern modeling

The analytical model of a network undergoing an attack consists of two types of network traffic, namely, normal and attack. Each node in the network is considered to bear a single queue, with average time for packet processing and transmission at node I being si (actual value is computed in section 7). The intensity of the arrive traffic at node r is thus given by

$$\rho_r = s_i\left(\sum_{i=1}^{f} I_{r,i}^{i} + \sum_{j=1}^{k} I_{r,j}^{j}\right) \quad \text{(iii)}$$

I'_r defined as normal traffic intensity, whereas is defined as the attack traffic intensity for all attack nodes k E A. I consider the case of attack detection by means of studying the overall traffic intensity towards a set of target nodes in the network. Attack detector nodes are defined as nodes which observe traffic flow of the network towards the target node set T. These nodes are notated as: G={ g_0, g_1, gd=1) where {G}=d_2. These threshold values are defined as the maximum numbers of packets a node r is willing to accept from a particular network region, during a constant time interval, from the region of operation of the observer (detector) node.

A network spanning a large geographic area with fewer numbers of nodes , will have a low node deployment density, and a network covering a smaller geographic area, with large numbers of deployed nodes. Will have a higher node deployment density. the observable threshold value, is high for denser networks , implying that a larger set of target

nodes can be lost before an lost before an alarm can be raised.

$$th_r^d = \left[Pk_r + nw(density) + \frac{1.0}{d_{G(d)}(r)} \right] \quad \text{(v)}$$

Where nw (density) is the normalized node deployment density of the network, $d_{G,(d)}$(r) the normalized Euclidean distance from detector node d to the target node r, and pk is the normalized number of expected packets by node r in a fixed interval of time, In a cluster-based network topology, the cluster heads are considered to be critical nodes. The threshold subpatterns for this network topology are generated from the following equation:

$$th_r^d = \left[Pk_r + num\_ch + \frac{1.0}{d_{G(d)(r)}} \right] \quad \text{(vi)}$$

Where *numch* is the normalized number of clusters in the network and $d_{G(d)(r)}$ is the normalized Euclidean distance from detector node *d* to the target node *r*.

In a data aggregation topology, the data aggregation nodes in the network are significant in the aggregation and forwardingof sensory data up the tree hierchy. The pattern generation equation for a data aggregation topology is

$$th_r^d = \left[Pk_r + \frac{1.0}{d_{G(d)(r)}} \right] \quad \text{(viii)}$$

Where *dG(d)(r)* is the Euclidean distance from detector node *d* to the target node *r*.

After the expected initial threshold values for a set of target nodes are generated and stred in the detector nodes, the attack detection scheme, proposed in the following section. The features to be extracted from the traffic constitute the vectors that need to be compared during the pattern matching process of the detection scheme. These traffic features are given by:

- Percentage of packets with destination address –*d*, where d e T. This feature facilitates collection of statistics for packets destined for sensor nodes labeled as potential victims by the base station at network initialzation time.
- Percentage of packets with source address = {s-v Euclidean (s,r) . thr euc} where thr euc is the thereshold on maximum permissible distance between the detector and the target nodes.
- Percentage of packets with source address = {s-s cluster d, where d T, s N). Packets orginating from outside the cluster of a cluster head based sensor network, are labeled as potentially malicious from statstics obtained throw this traffic feature.

A packet internded for a target node, at a higher than threshold Euclidean distance, is analyzed by other detector nodes. With-in the target node's vicinity. Similarly, packets orginating from outside the cluster of operation of a decetor node, in a cluster based network topology, need to be analyzed by other detector nodes.

For each of the r target nodes, a pattern vector, pr, will be reconsitituted at the base station based on the receipt of individual sub-patterns from each og the n detector nodes. The pattern vector for a target node *r* is given by: $p_r = \{p_1, pe_1, p_2, ..., p_n, pe_n\}$, where p_n is the percentage of packets destined for target node *r*, observed by detector node *n* as to possessing a source address outside the education thershold defined by thr_{euc}, as

satisfying the second rule for feature ectraction defined above.

Fir cluster-based wirelss sensor networks, the pattern vector for a target node *r* is gioven by: $p_r = \{p_1, pc_1, p_2, pc_2 ...., p_n, pc_n\}$, where p_n is the same as the previous scenaric. These pattern vectors are compared with the threshold subpattern values, generated and stored in each of the attack detector nodes. i.e. traffic flow values, toweards a target node duting a given time period.

(X) Experiments and Results

In this section, the results of there preliminary are described. The first experiment was to check the properties of the clock skew; the second was to realize a replication attack on clock skew based identification; and the third experiment studied the effect of changing the period and how the proposed algorithm defended against the clock skew replication attack.

In these experiemnts, Taroko motes (Lau et al.,2006), Tmote Sky compatible products, were used. A Taroko mote has 8MHz Taxas Instruments MSP430 microcontroller, 10KB RAM and 48 KB external flash memory.

To evaluate the performance we apply the above approach/technique at difference threshold values. A threshold value 0.8 means that the node is considered as trusted it can forward at least 80% of the received packet. The trust value of a node falls below this threshold value, it is identified as black hole node and that node is excluded from the route discovery process.

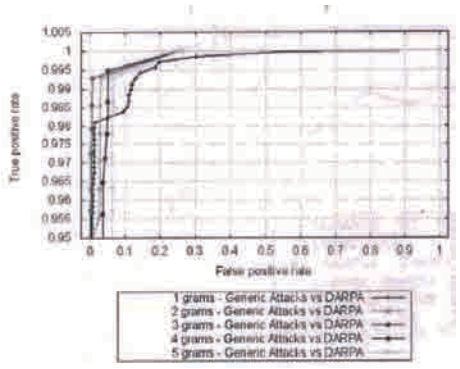
Wireless sensor networks are deployed for specfic sensing and reporting applications. The areaof sensor node deployment depends in the deployed depend on sevral charactistics of the application, namely, expected node lifetimes, expected per-node load and node sensing ranges.

The simulation experiments are performed for two injected nodes and laptop—calss nodes.

There is delays in communication computed at network at network initialization time based on the broadcast and receipt of 1Byte-length messages between the GN, mGN nodes as well as the based station. These values very based on the density of node deployment, i.e. value of *N*, in the network.

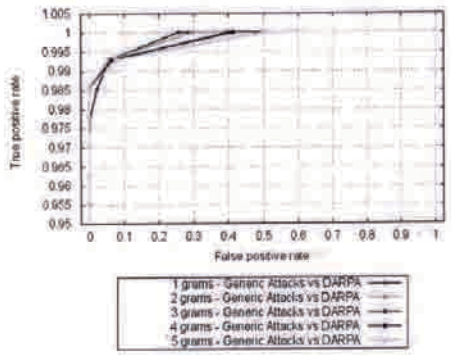
The energy consumption rates of the mGN nodes of the detection scheme is illustrated in Fig. 7. For all node deployment densities, the mGN nodes can be seen to consume more energy than the GN nodes. This is due to additional tasks imposed on the mGN nodes for message reception, analysis, and delivery to the base satation, as compared to the stan derd tasks of a GN node.

For low node mGN nodes are higher, as compared to networks with higher values of N.



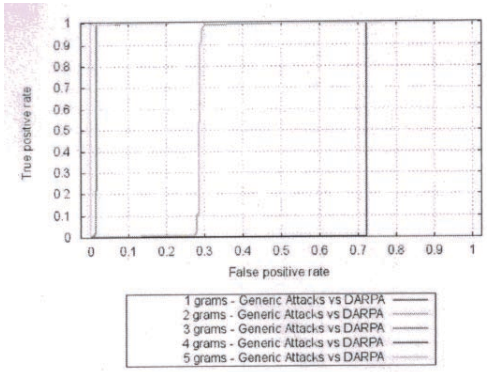
ROC curves for generic attacks vs DARPA-x2 distance

For dataest, the ROC curves for our x2, adhoc *n*-gram, and pattern counting techniques, respectively. Summarize our results for the generic attacks dataest in the form of AUC and AUC_P statistics.



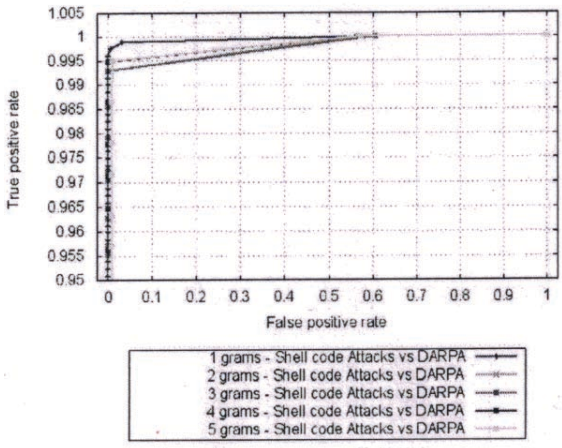
ROC curves for generic attacks vs DARPA – adhoc *n*-gram

These results indicate that we obtain poor results for the pattern counting technique using 3-g or less, but we obtain excellent results in all other cases considered.



ROC curves for generic attacks vs DARPA –pattern counting

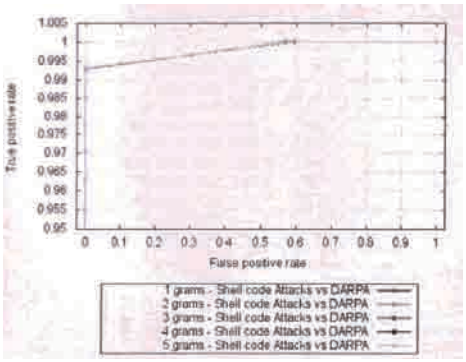
We use DARPA dataest dataest to represent benign traffic fig. 8-10 give the ROC curves obtained for the shellcode attackes using the x2, adhoc *n*-gram, and pattern counting, respectively. The correspondance AIJC and AUC_p statistics appear.



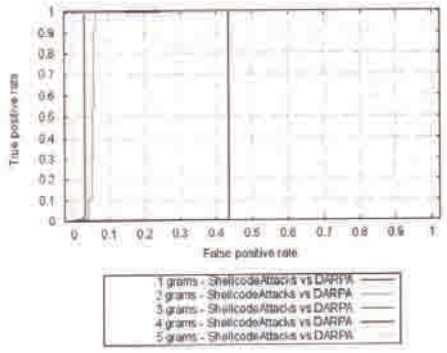
ROC curves for shellcode attacks vs DARPA-x2 distance

The prediction healers require the least amount of time to recover the system when compared to the *RH* and *PH* families. This is due to the prediction capablity of the healers that allow them to deploy

patches efficiently. The recovery time required by the prediction healers in 18% less and 22.5% less than the best random healers RH ($p=1$) and the best profile healers PHB_M, respectively.



ROC curves for shellcode attacks vs DSRPA –adhoc *n*-gram



ROC curves for shellcode attacks vs DSRPA –Pattern Counting

Conclusion

The Clock Skew is a paractical method for node identification in wireless sensor networks. A real clock skew precisely measured by FTSP, more than 80% of an attackers pockets were still able to pass throw the current skew filter. The high accuracy advantage of FTSP not only leads to the success of node identification, but also given attackersthe same power to imitate the identity of other nodes.

The adhoc network is too much sensitive towards varioustype of attack. Black hole attack is one of them. Therefore the quality of serviceof the network becomes an important issue with respect to packet dropping. The trust value is calculated at every 0.07 second of interval and the new trust value is updated. In this way, the set of trusted nodes is maintained whichn is dynamic in nature, Depending upon the trust value and the threshold value the black hole node is identified and it is excluded from the route establishment process.

The availbility of sensor nodes is under constant threat from distributed node exhaustion attacks. The attack detection process is modeledas a pattern recognition problem, with amphasis on the need for having a distributted pattern recognition mechanismin place, to achieve success in atack decttion, withous incurring significant overhead on the limited energy resources of the sensor nodes.

We analyzed three *n*-gram techniques for filtring attackes from begin HTTP traffic, and we compared our results to the HMM-based approach in Rriu et al. (2011). These *n*-gram techniques were extensively tested on publicly available datasets, as well as our own similated traffic, including a highly realistic attack dataset. Theresults indicate that each of our approaches can achieve a detection rate comparable to that in Ariu et al. (2011) and our pattern matching tachnique wasshown to be extermely efficient, in terms of per packet processing time.

Mobile malware have become an emerging problem that threatens smartphones which are growing significantly in recent days. In this paper, we considered realistic mobility patterns to model proxomity dependent malware and compared them against de facto models like random waypoint

mobility mode. We presented several defencemechanisms that allow tuining of parameters to control two dimensions of optimization – either time to recovery or energy utilized. The extensive evalution of all our defense mechanisms shows that prediction healers would be more effective in a time constrained environment whereas profile healers would benefit the most in an energy constrained environment.

References

1. R. Potharaju, E. Hoque, C. Nita-Rotaru, S. Sarkar, S. Venkatesh, Closing the pandora's box: Defenses for thwarting epidemic outbreaks in mobile adhoc networks, in: Proc. of IEEE MASS, 2012, pp. 200–208.
2. McAfee Threats Report: 3rd Quarter 2011, http://goo.gl/jIQPJ.
3. Juniper Mobile Threats Report 2010-11, http://goo.gl/v3yFg.
4. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, Inside the slammer worm, IEEE Security & Privacy 1 (4) (2003) 33–39.
5. C. C. Zou, W. Gong, D. Towsley, Code red worm propagation modeling and analysis, in: Proc. of CCS, ACM, 2002, pp. 138–147.
6. A. Wagner, T. D¨ubendorfer, B. Plattner, R. Hiestand, Experiences with worm propagation simulations, in: Proc. of WORM, ACM, 2003, pp. 34–41.
7. J. O. Kephart, S. R. White, Directed-graph epidemiological models of computer viruses, in: Proc. Of Sym. on Research in Sec. and Priv., IEEE CompSoc, 1991, pp. 343–359.
8. S. H. Sellke, N. B. Shroff, S. Bagchi, Modeling and automated containment of worms, IEEE TDSC 5 (2) (2008) 71–86.
9. Single NFC bonk subjugated Samsung Galaxy SIII and slurped it out, http://www.theregister.co.uk/2012/09/21/android_nfc/ (2012).
10. C. Miller, Exploring the NFC attack surface, in: Blackhat, 2012.
11. McAfee warns of NFC malware risk, http://www.itpro.co.uk/malware/19275/mcafee-warns-nfc-malware-risk (2013).
12. R. Potharaju, E. Hoque, C. Nita-Rotaru, S. Sarkar, S. Venkatesh, Closing the pandora's box: Defenses for thwarting epidemic outbreaks in mobile adhoc networks, in: Proc. of IEEE MASS, 2012, pp. 200–208.
13. McAfee Threats Report: 3rd Quarter 2011, http://goo.gl/jIQPJ.
14. Juniper Mobile Threats Report 2010-11, http://goo.gl/v3yFg.
15. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, Inside the slammer worm, IEEE
16. Security & Privacy 1 (4) (2003) 33–39. C. C. Zou, W. Gong, D. Towsley, Code red worm propagation modeling and analysis, in: Proc. of CCS, ACM, 2002, pp. 138–147.
17. A. Wagner, T. D¨ubendorfer, B. Plattner, R. Hiestand, Experiences with worm propagation simulations, in: Proc. of WORM, ACM, 2003, pp. 34–41.
18. J. O. Kephart, S. R. White, Directed-graph epidemiological models of computer viruses, in: Proc. Of Sym. on Research in Sec. and Priv., IEEE CompSoc, 1991, pp. 343–359.
19. S. H. Sellke, N. B. Shroff, S. Bagchi, Modeling and automated containment of worms, IEEE TDSC 5 (2) (2008) 71–86.
20. C. Miller, Exploring the NFC attack surface, in: Blackhat, 2012.

Efficient Combined Security System and Security Framework for Wireless Sensor Network

Er. Name. Prabhjot Kaur

M. Tech Research Scholar

Amritsar College Of Engineering & Technology, Amritsar

Email-id:-prabhkhehra121@gmail.com

Abstract :-Security is an important in Wireless Sensor Network**.** It requires some mechanism which are more effective .The parameters like speed and energy consumptions affect these mechanism .In Wireless Sensor Network, it enhance speed of network and energy consumption these parameters presents security in this paper. This result of simulation define that Wireless Sensor network, increase its speed ,enhance its security ,it enlarge the life time of the combined system. Wireless Sensor Network used in lots of military and commercial applications and paid lots of attention. In this paper, we proposed a flexible security management framework, which can overcome the drawbacks of early research by using existed methods. In this method, we analyze the attacks and also implemented protection schemes through some control platform for Wireless Sensor Network.

Keyword: - Wireless Sensor Network, Kerberos, Security, Security Management framework.

I. Introduction

Wireless Sensor Network Consists many devices which can monitor real work environment. They are playing important role for military application for providing security for different ranging areas. In this type network, we can deployed very large amount of nodes to monitor vast field in hostel unattended environment. This mechanism defends against different attacks like node capture, physical tempering, eavesdropping, and denial of service and so on. In this mechanism, we need to rethink about speed and energy consumptions parameters which provides secure wireless sensor network without consuming the energy and also increase there speed.Key management and authentication are based on security service like encryption. There are many key establishment protocols which set up a shared key between two entities by trusted third party. In these protocols, the entities share a key with trusted party and entities used this party to prove their identity and generate or transmit a session key for secure communication with each .other.Wireless Sensor Network deployed low cost and high performance sensor nodes which are used in various security applications. If nodes are used in unsecure network then there are many security issues.Security of wireless sensor network much more complicated due to these types of limitations and difficulties. There are many Security issues, we discuss four main points as follows:-

1. Key Management

Key management is very complex, due to dynamic structure and easy node compromise. It increases the difficulty of key management by using self organization property. In this area, we can used large amount of approaches.

2. Attack detection and preventions

Wireless Sensor Network is vulnerable to attacks due to limited communication and computation capabilities. The mechanism which can detect those attacks based on anomalies that are Intrusion detection.

3. Security Routing

Wireless sensor network use wireless communication to communicate and transfer data for each other and also used multi-hop nodes which uses intermediate nodes which need to access the content of message.

4. Secure location

Location information is most important in some applications of wireless sensor network. Location information is required for many routing protocols and security mechanisms.

This paper is organized as follows. Section 2, we introduce some related work .Section 3, proposed the structure of platform and combined security system. Thus, we shows the experiment results in section 4.Finally, closes with conclusion in section5.

II. Related Work

In sensor network key establishment, the nodes are setup a shared secret key either by key transport or key agreement after deployment. In key transport, entity creates a secret key and transfer information securely to another entities. In key agreement, all entities contribute a input to derive shared secure key. In this section we can discuss two protocols:- lightweight kerberos protocols with short messages and ECMQV.

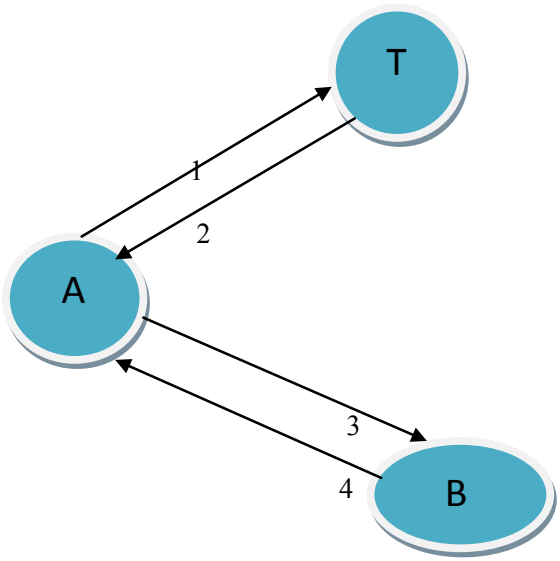


Fig 1: Simplified kerberos protocol exchange

1. AS_Req: A, B, nA

2. AS_Rep :{ kAB, B, tS, tE, nA} kAT, {kAB, A, tS, tE} kBT

3. AP_Req :{ kAB, A, tS, tE} kBT, {A, tA }kAB

4. AP_Rep:{tA}kAB

2.1 Lightweight kerberos protocol with short messages

Kerberos is a distributed authentication service that allows a client to obtain a ticket with user's identification and session key to any server which is registered with authenticated server to prove its identification. This protocol is basically described as "basic kerberos authentication protocol which is without ticket granting service".Fig1 shows that message is transfer between the entities(A,B) and trusted party T. Assume that entity A wish to establish a session key with B and both entities shared a secret key with T. The description of message which is communicated as follows:

- The first message send from A to T that is authentication server request (AR_Req) message. It contains A's identity, B's identity and random nonce nA which is used

for reply message with matching AS_Req and also detect that replays.

- After AS_Req message, now T looks entities A and B in the database and also verifies that these entities are authorized by session key, and fetches their keys kAT , kBT which is long term keys. now they can also establish a new session key kAB that is shared between entities A and B and also embed it a ticket. T also contains A's entity ,expiration time and starting time. its encrypted using kBT. Ticket creates AS_Rep message.
- After receiving a AS_Rep message, A using kAT to decrypt all non ticket part of message and it also verifies that nonce which is supplied is matched with nonce which is received in the AS_Rep message. In the third message, entity A transfer the ticket together with the authenticator to B which is AP_Req(Application request) message. Its main purpose to prove that entity A knows kAB and also ensure that every AP_Req message is unique.
- After receiving AP_Req message, B decrypts the message using kBT and extarct kAB, identity of A, and tE. Mutual authentication requires that entity B proves its identity too by sending application reply (AS_Rep) message which consists of timestamp encrypted in the session key kAB returns to A. After A received and decrypted the AP_Rep message which is verifies the timestamp is the same like that which is sending in the AP_Req messsage. This is ensuring that kAB is successfully transmitted to B.

Now a day, most protocols using third party, such as kerberos, are three ways communication in which two entities wishing to establish a secret key not only for transferring messages but also for trusted authority. The communication energy is much higher in the kerberos protocol.

2.2 Elliptic Curve Menezes-Qu-Vanstone (ECMQV) protocol:

ECMQV protocol is basically modified to work in arbitrary finite group and also in some particular elliptic curve groups. It is basically example of key exchange protocols with implicit authentication.

In this protocol, each entity has a short term key pair and static private/public key pair. A shared secret key is derived by using the short term keys and static keys, which ensures that each protocol runs between two entities (A, B) and produces a different shared secret. Formally a prime field GF (p) which can be defined by the Weierstraß eq1, where a, b GF (p) and 4a3+ 27b2=! 0 mod p [14].

$$y2 = x3 + ax + b$$

Let E be a elliptic curve group of order n, G shall be point on the curve. Suppose that the order n is prime, which means that G is generator of E and E is cyclic. Also assume the parameters p, a, b, n, and G are known to every entities of the networks.

In other side, security is most important in WSN in the recent years, for solving these issues by lot of studies. We want to define current approaches and classified their studies. There are classified into four categories following are:-

Table 1. The research of security for WSN [2]

Field	Classification
Key Management Protocols	Key pre-distribution, hybrid cryptography, one way hash, key infection, key management in hierarchal network.
Attack detection	Internal attacks and external attacks.
Secure Routing Protocols	Multi-path routing, Reputation based schemes, Secure routing for cluster or hierarchical sensor Networks, Broadcast authentication, Secure routing defense against attacks.
Secure Location	Secure location scheme with beacons and without beacons.

However, each category focuses on one aspect that is security, not a complete security model that our approach does. To solve this issue, we can proposed a security management framework. We analysis a attacks on WSN by data mining method and control the protection by control platform.

II. Architecture

3.1 Efficient combined security system

A wireless sensor network can be divided into several clusters and each cluster has number of sensors nodes and one of the node is elected as the coordinator (head). The head is responsible for mission and collecting sensed data of other nodes and routing to the sink so that head energy consumption is higher than another node. The energy analysis of kerberos protocol is based on assumption that an entity A is directly sends and receives messages to and from third party T. This is reasonable small sensor network not for large sensor network where the sensor network is a part of the base station. The communication cost is depending upon the number of intermediate nodes between the entity A and T and transmit level. Multi hop communication between entity A and T increase overall energy consumption. Lightweight kerberos protocol is more efficient than ECMQV.

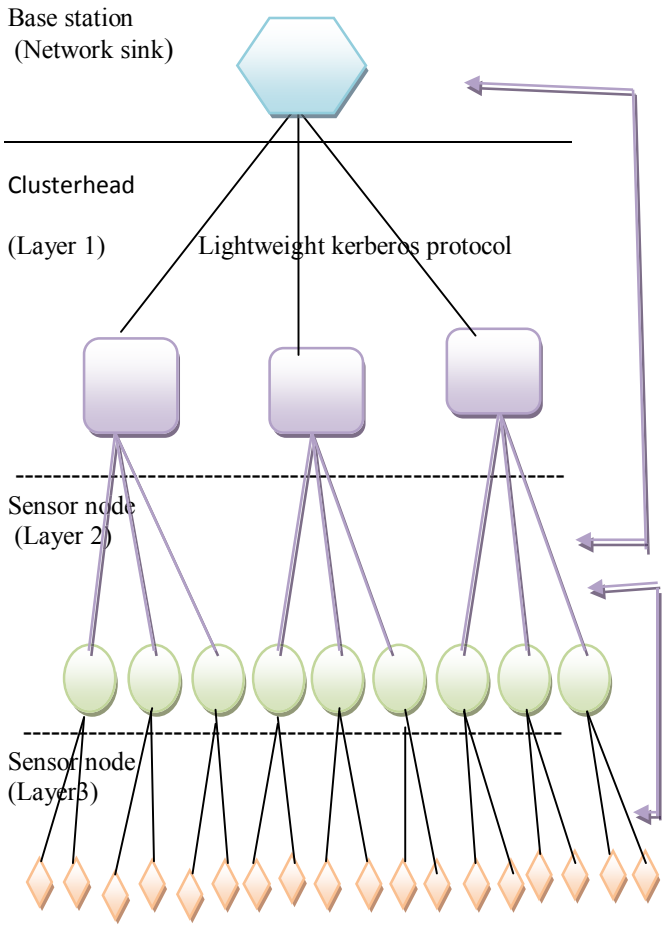


Fig2: Hierarchical architecture for combined system

In this combined system we can use both protocols in such a way network is divided into three layers. The first layer is 1-hop layer which is directly communicated with base station and cluster head. The second layer is 2-hop layer and third layer is 3-hop layer, these layers contains sensors nodes that's belongs to clusters. This system is looking a network which contain two network that is small network and large network. Lightweight kerberos protocol with small messages is applied on small network and ECMQV protocol applied on large network.

The benefit to combining two protocols are as follows:-

- Using two strong protocols ECMQV and Lightweight kerberos increase the speed of network.
- Using these protocols it also improves the network security.

In other side, system architecture and platform module partitions and working process of the wireless sensor networks.

3.2 System Architecture

It is divided into two parts, first one is wireless sensor network and other side is security management platform. Wireless sensor network consists of number of sensor nodes. These nodes working together and collect some sensitive data. The tasks of security management platform are:-

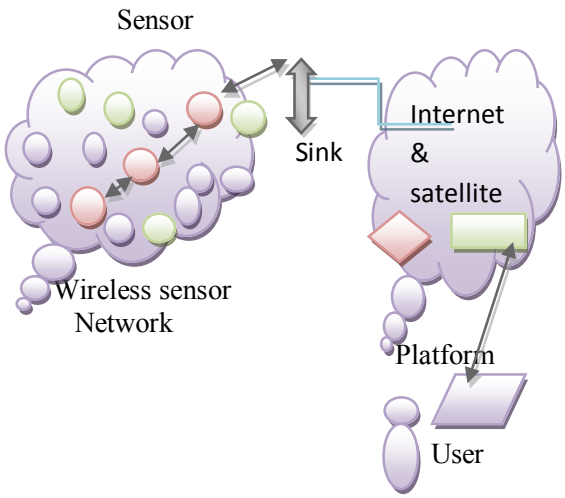


Fig3:-Wireless sensor Network Topology

1. Processing normal data form wireless sensor networks.

2) Managing the secret key's distribution and renew.
3) Detecting malicious nodes and attack .
4) Mining potential attack and malicious nodes.

For these major tasks, the platform interact with wireless sensor network to obtain data and information through the satellite and internet

3.3 Platform module partition

In the logical architecture of our platform, it is divided into eight modules: network processing module, intrusion detection module, control and query module, key management module, behavioral analysis module, database module and user interface module.

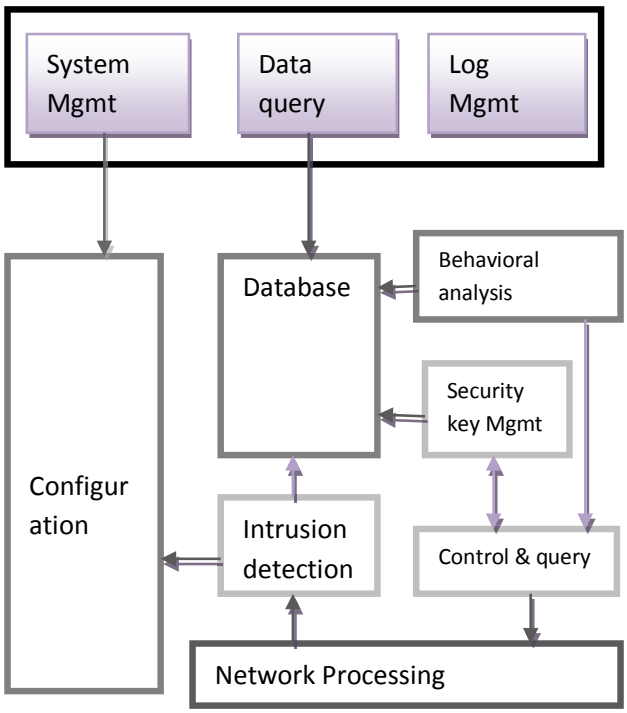


Fig 4:-System Management System framework

1. Network processing module:-its mainly consist receiving and sending data packets. We use socket layer functions to communicate with sink.
2. Intrusion detection and data processing module:-it tries to detect the malicious data. Data processing function interacts with database to read and write data.
3. Control and query module:-It is interface module. It controls wireless sensor network and query which is necessary property of nodes.It is invoked by intrusion detection and data processing module, key management module and behavioral analysis module.
4. Key management module:-it includes node's initialization and renew.
5. Behavioral module:-This module is mining potential attacks and malicious nodes.
6.Database module:-It stores the properties of nodes, the node's log and data. The four modules interact with this module such as: user interface, intrusion detection and data processing, Key management and behavioral analysis module.
7. User interface module:-we design a web user interface to enhance the platform friendly. Users can easily interact with this module, It includes system management, data query and log management.
8. Configuration module:- when we want to extend new detection rules then uses some scripting languages rules and save in configuration files. We can configure new rules with the help of user interface.

3.4 Working Process

The procedure can be summarized as follows:

1. Initialization

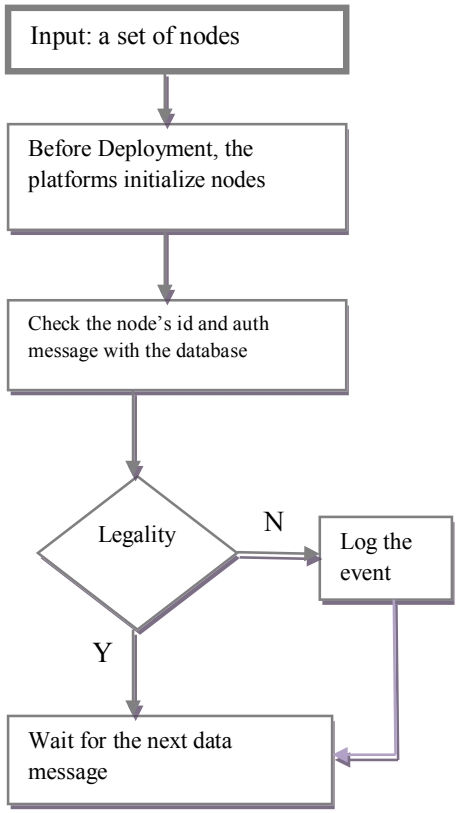


Fig5: working process of Initialization Stage

Step1: Check the node's id and auth message with the database, if the node is legality go to step 2, otherwise log this event and continues.
Step2: Update the database, and wait for the next data messages.

2. Real time monitoring

The system will always receive material form wireless sensor network and its useful for intrusion detection. The procedure for real time monitoring is:

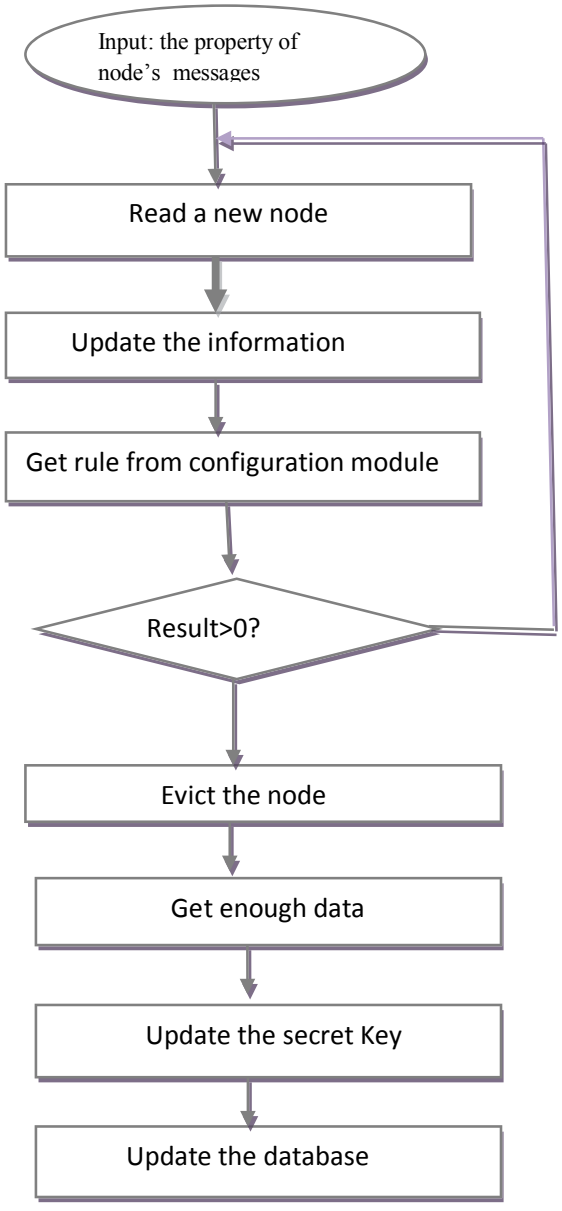


Fig6: The working process of the real time monitoring.

Step1: receiving message from WSN.
Step2: update the information of sensor node.
Step3: read rules from configuration module and check the data using the rule, if the result ret>0 go to step 4 else go to step 1.
Step4: according to the detection to make decision if result is equal to 1, go to step 5 else go to step 6.
Step5: the node is compromised, notes the control module to evict it.
Step6: The system need more information, notes query module to get enough data.
Step7: Note the key management module to update the secret key.

IV Experiment

This section analyzes and compares the energy demands of Lightweight kerberos distribution protocol, ECMQV protocol and combined system.

Table2: Total energy of combined system [1]

Pair layer	Energy consumption of combined system
1	39.6-47.6
2	79.0-84.6
3	79.0-84.6
1 and 2	39.7-47.7
2 and 3	79.0-84.6

Table3: Comparing energy consumption of Lightweight kerberos, ECMQV, and Combined system[1]

Pattern no.	#Com. Pairs	Pairs layer	Energy Consumption Lightweight Kerberos	ECMQV	Combined System
1	1	1	39.6-47.6	79.0-84.6	39.6-47.6
2	1	2	61.5-73.9	79.0-84.6	79.0- 84.6
3	1	3	83.4-100.3	79.0-84.6	79.0- 84.6
4	2	3	166.8-200.6	158-169.2	158- 169.2
5	2	2,3	144.9-174.2	158.169.2	158-169.2
6	3	2	184.5-221.7	237-253.8	237- 253.8
7	3	3	250.2-300.9	237-253.8	237- 253.8
8	3	1,2,3,	184.5-221.8	237-253.8	197.6-216.8
		Sum	1341	1353.6	1025.8

The evaluation of key establishment protocols considers both the energy that during execution of cryptographic algorithm it consumes the strong ARM and energy cost of radio communication. The energy

required for the calculation of cryptographic primitives is simply the product of the average power consumption and the execution time. The execution time is determined by simulation with simIt-ARM. The Communication energy depends upon the distance between sending and receiving node and time which is required for sending the message and message length and transmission rate. Transmission of message consumes energy to sending and receiving messages.

4.1 Energy consumption of the combined system

The result shows for energy consumption for combined system is less as compare to using two protocols individually. Table 2 includes the energy consumption for one pair authentication, it can change according to the layer of two nodes because applied node is different.

Table 3 compares the energy consumption of combined system with two protocols that is Lightweight kerberos and ECMQV. The result shows the efficiency of combined system especially when a communication node increases.In the other site, we deploy our proposed system into smart environment system. The parameters are described in detailed as follows:-

Table4 : Equipment Specification [2]

Parameters	Values
CPU	72MHz
FLASH	128KB
SRAM	64KB
Sampling rate	16KHz

In order to fully evaluate the proposed method we compare our method with some state-of –the art, and comparison result is shown in table 5.

Table5.comparison with some state-of –art [2]

	Key mgmt	Attack detection	Security Routing	Our's
Confidentiality	Yes	No	No	Yes
Availability	No	Yes	Yes	Yes
Integrity	Yes	-	No	Yes
Authentication	Yes	No	No	Yes
Non-Repudiation	No	Yes	No	Yes
Authorization	No	No	No	Yes

In this table, we can see that existed security algorithm consider only few parts of the problem related to security and cannot provide all the security demands but our's system satisfy all these security demands.

V Conclusion

In this paper we can presented combined system which can combine two protocols that is Lightweight kerberos protocol and ECMQV protocol. The main benefit is enhancing the energy consumption. Saving energy means decreasing number of computation and communication and its also improves the speed of network. In this paper we also proposed a flexible security management framework which can combine the existed system together and overcome the drawbacks of individuals. Each part of WSN's security can interact with other part ,which can enhance the security of system.

VI.References

[1] Fayad N.S,Atwan.A," Efficient combined security system for wireless sensor network" Egyptian Informatics Journal (2012) 13, 185–190

[2] Sharma Gaurav,Bala Suman "Security Frameworks for Wireless Sensor Networks-Review" Procedia Technology 6 (2012) 978 – 987

[3] Needham R, Schroeder M. Using encryption for authentication in large networks of computers. Commun ACM 1978;21(12):993–9.

[4] Kohl J, Neuman B. The Kerberos network authentication service (Version 5). Internet Engineering Task Force, Networking Group,
Internet Draft RFC 1510; September 1993.

[5] Raghavendra C, Sivalingam K, Znati T. Wireless sensor networks. Kluwer Academic Publishers; 2004.

[6] Singh K, Muthukkumarasamy V. Analysis of proposed key establishment protocols in multi-tiered sensor networks. J Netw 2008;3(6).

[7] Menezes A, van Oorschot P, Vanstone S. Handbook of applied cryptography. CRC Press; 1996.

[8] Chen X Q, Makki K, Kang Yen, et al. Sensor network security: a survey, Communications Surveys & Tutorials, IEEE, Second quarter 2009, 11(2): 52–73

[9] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor Networks. IEEE Transactions on Wireless Communications, 2002, 1(4): 660–670

[10] Lindsey S, Raghavendra CS. PEGASIS: Power-efficient gathering in sensor information systems. IEEE Aerospace Conference Proceedings, 2002, (3): 1125–1130

[11] Younis O, Fahmy S. HEED:A hybrid energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing, 2004, 3(4): 660–669

[12] Tan H O, Korpeoglu I. Power efficient data gathering and aggregation in wireless sensor networks. ACM SIGMOD Reeord, 2003, 32(4): 66–71

[13] Lee B, Park K, Elmasri R. Energy Balanced in Network Aggregation Using Multiple Trees in Wireless Sensor Networks. Consumer
Communications and Networking Conference, 2007: 530–534
[14] Li Q, Ma H, Huang Q. A hierarchical framework for audio scene analysis in sensor networks. Proc IRADSN2009, May 2009, Hangzhou, Zhejiang, 2009: 170–177
[15] Gajbhiye P, Mahajan, A. A survey of architecture and node deployment in Wireless Sensor Network. ICADIWT 2008. Aug 4–6. 2008, Ostrava, Czech Republic, 2008: 426–430.
[16] AkyildizI, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Commun Mag 2002;40(8):102–14.
[17] Sen J. A survey on wireless sensor network security. Int J Commun Netw Inform Secur (IJCNIS) 2009;1(2).

Valuable Use Of TEAM: Trust Extended Authentication Mechanism in Vehicular Adhoc Networks

Er. Govind Sood
Student, Dept. of CSE
Amritsar College of Engineering and Technology,
PTU, Jalandhar, Punjab
aryanprincesood@gmail.com

Dr. Tanu Preet Singh
Professor and HOD, Dept. of ECE
Amritsar College of Engineering and Technology,
PTU, Jalandhar, Punjab
tanupreet.singh@gmail.com

ABSTRACT

Security in Vehicular ad hoc networks (VANETs) getting an important form of interest in the field of wireless mobile networking because VANETs are expose to spiteful attacks. A number of secure verification schemes based on asymmetric cryptography have been proposed to stop such attacks but these schemes are not appropriate for highly active environments such as VANETs, because they cannot capably deal with the verification procedure. In this paper, we propose a decentralized lightweight verification scheme called trust extended authentication mechanism (TEAM) for vehicle to vehicle communication networks. TEAM satisfies the following requirements: ambiguity, location privacy, mutual verification, fake attack resistance, modification attack resistance, replay attack resistance, no clock synchronization problem, no verification table, fast error detection, perfect forward secrecy, man in the middle attack resistance, and session key agreement.

General Terms- Verification, decentralized, lightweight, trust extended, VANETs.

1. INRODUCTION

Vehicular Ad Hoc networks are rising new technologies to combine the ability of new generation wireless networks to vehicles [1]. The key workings of a VANET are wireless on board unit (OBU), the roadside unit (RSU), and the authentication server (AS) illustrate in figure 1. OBUs are installed in vehicles to give wireless communication capability, while RSUs are deployed on intersections or hotspots as an infrastructure to provide information or access to the internet for vehicles within their radio coverage. The AS is liable for installing the secure parameters in the OBU to validate the user. Based on IEEE 802.11p, the keen short range communication system [2] supports two kinds of communication environments: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications.

The security issue in VANETs has become a blistering topic, and then many researchers provide the V2I and V2V authentication mechanism to protect valid users. However the design for an efficient V2V authentication mechanism is more challenge than that for V2I authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in V2V communications. Therefore, we focus on V2V network environments and propose an efficient authenticated scheme in this paper.

To deal with the above need, we propose a decentralized authenticated scheme, called TEAM, for V2V communication networks. TEAM is a lightweight authentication scheme because it only uses an XOR operation and a hash function. Although TEAM needs low computation cost and it also requires few storage spaces than other schemes.

In this paper, we propose the analysis of computational and storage costs of TEAM, and then we use the NS-2 network simulator to evaluate the performance of TEAM. The remainder of this paper is organized as follows. Section 2 introduces preliminaries, and in Section 3, we describe the proposed scheme in detail. Analyses of the security and performance are presented in Section 4. Then in Section 5, we summarize our conclusions and consider future research avenues.

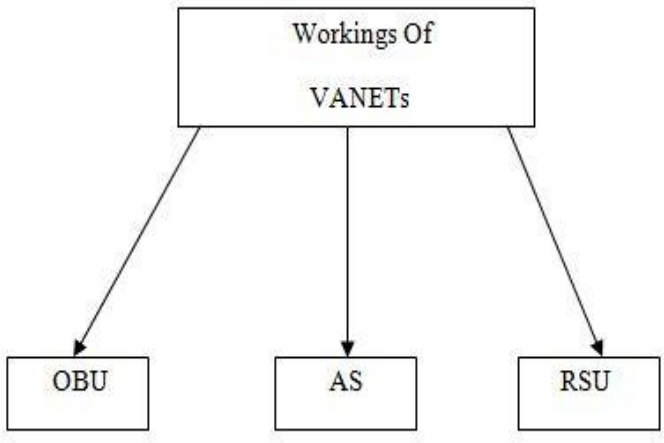


Fig.1 Components of VANETs

2. PRELIMINARIES

This section includes the concept of transitive trust relationship, some threat models, and the security requirements of VANETs.

I. Transitive Trust Relationships

In VANETs the vehicles are described into the following roles: a law executor (LE), a mistrustful vehicle (MV), and a trustful vehicle (TV) as illustrated in figure 2. An LE, such as public transport vehicle (e.g. buses), acts as Authenticated Server and LE is trustful permanently. A normal vehicle is regarded as trustful if it is authenticated successfully; otherwise it is deemed to be mistrustful. In addition, the TV becomes the MV when the key lifetime gets over. To provide a secure communication environment, the OBU should be authenticated successfully before it can access the service. In V2V communication networks, the number of LEs is finite and LE is not always in vicinity of the OBU. In this paper, we propose a TEAM to improve the performance of the authentication procedure in V2V communication networks.

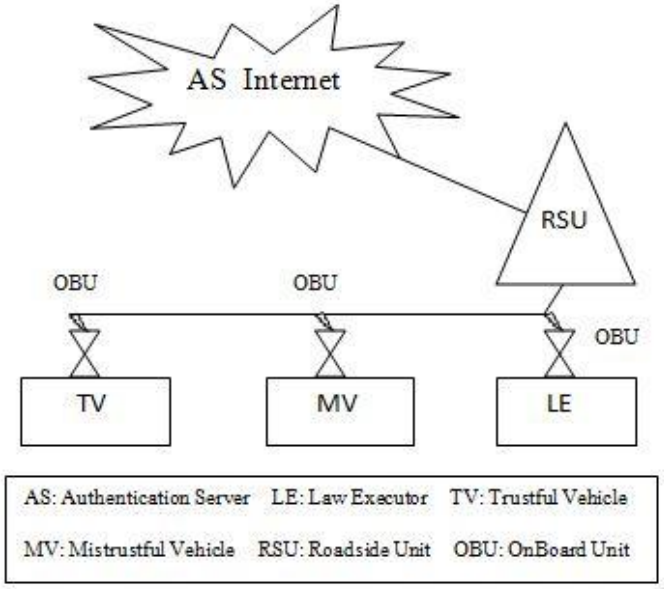


Fig 2: Architecture and the transitive trust relationships of VANETs.

The TEAM is based on the concept of transitive trust relationships. Initially there are three vehicles in VANET: a trustful LE and two other MVs carrying OBUs. The mistrustful OBUs can be authenticated by any trustful OBU without necessarily finding an LE, and all vehicles in a VANET can complete the authentication procedure quickly but the key design issues in this relationships are the authentication ability, the computational cost, the trustful state of TV, and the storage cost.

II. Adversary Model

The following possible attack models can be used during the V2V authentication procedure.

1. Message replay attack: The adversary resends valid messages sent previously in order to disturb the traffic flow.
2. Impersonation attack: The adversary pretends to be a valid LE/TV to cheat the unauthenticated OBUs.

III. Security Requirements in VANETs

The main objective is to design a scheme that is robust to such attacks. Based on related studies [3]-[11], we define the following key security requirements for VANETs.

1. Efficiency: In VANETs the computational cost of vehicles must be as low as possible in order to have a real time response.
2. Anonymity: The anonymous authentication procedure verifies that an OBU does not use its real identity to execute the authentication procedure.
3. Location privacy: An adversary collects the serial authentication messages of the OBU but it still failed to track the location of the vehicle.
4. Mutual authentication: A mutual authentication procedure is implemented whereby the LE must verify that the OBU is a legal user and the OBU must ensure that the LE is genuine.
5. Integrity: The message integrity means that data cannot be modified undetectably.

3. TEAM

In this part, we explain the proposed scheme in detail. A TEAM is a decentralized authentication scheme, and the LEs need not to keep the authentication information of the whole vehicles. The proposed scheme includes eight procedures: initial registration, login, general authentication, password change, trust-extended authentication, key update, key revocation, and secure communication. Before joining a vehicle to VANET, its OBU must register with the AS. As soon as a vehicle desires to access the service, it has to complete the login procedure. Next, the OBU verify the authentication condition itself (i.e., the lifetime of the key). If the lifetime of the key is reached to zero, the vehicle is mistrustful, and vice versa. The MV makes the general or trust-extended authentication procedure to be authenticated. The trustful vehicles help other MVs in performing the authentication procedure or converse with other trustful vehicles (i.e., secure communication procedure) to access the Internet. The trustful vehicle performs the key update process with the LE when the key lifetime is below the desired threshold. Furthermore, we also define the password alter process for user friendly. Fig. 3 shows the login process in TEAM.

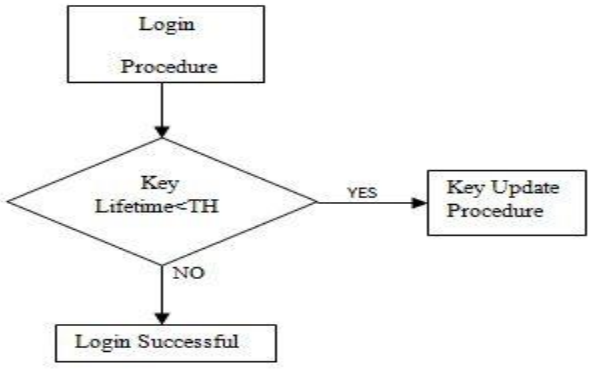


Fig 3: Login Process

A. Assumptions

Several interrelated mechanism point out that the system of vehicle is better protected than the common mobile device (e.g., PDA, smart phone, etc.). Hence, we assume that each vehicle's OBU is equipped with security hardware (e.g., trusted platform module), including an event data recorder (EDR), and a tamper-proof device (TPD) [12]-[14] so that an intruder cannot retrieve information about the vehicle from the OBU. The EDR is answerable for recording significant data about the vehicle, such as the location, time, preload secret key, and access log. The TPD gives the cryptographic processing capabilities. Lastly, we assume that the time of each vehicle is synchronous via GPS device.

B. Notations

The notations used during this paper are given in Table I.

TABLE I
NOTATIONS

Symbol	Description
x	A secret key protected by AS
IDi	The public identification of entity i
AIDi	The alias of entity i
PWi	The password of user i
MSG	A key update message
X→Y	User X sends a message to user Y through a secure channel
H()	A collision free one way hash function
Ni	A random number i
PSK	A secure key set that is pre shared among LEs and the AS

C. Periodic Hello Message

In VANETs, the vehicles transmit the hello message sometimes with the authentication state (i.e., trust or mistrust). In order to guarantee the network security, only the trustful vehicle can perform the secure communication procedure. On the other hand, the MV must finish the authentication process in advance to converse with other vehicles.

D. Initial Registration Procedure

1) *LE Registration:* The LE performs registration process with the AS via secure channel. The AS compute the safe key set based on the hash-chain method (e.g., $h^2(x) = h\ (h(x))$) and transmit this key set to the LE. Note that the LE only needs to hold a secure key set that is stored in the security hardware and it does not require storing any authentication information of the user. Each trustful vehicle performs the key update process with the LE when the key lifetime is going to finish.

2) Normal Vehicle Registration: The vehicles other than the Authenticated Server require to perform the normal vehicle registeration process with the following steps to be followed.

1. User→ AS: The user sends the ID and the password to the authenticated server via secure channel.
2. Once getting the user's ID and password, the AS computes the different parameters to perform the vehicle registeration process. The user should have the personal information (i.e.ID, password) in the login procedure. Otherwise, the OBU rejects this login request.
3. AS→ User: The AS stores the parameters in the OBU's security hardware via secure channel.

E. Login Procedure

The login process is the first task require to get the information of the user. The OBU will detect an error event immediately if the user has spiteful intentions.

1. User→ OBU: The first step require is when the user wants to login he/she should have to provide ID and password to OBU.
2. The OBU checks the ID and password given by the user is correct and matches. If the information is correct, the OBU performs the general authentication process and if the information is incorrect login process will fail.

F. General Authentication Procedure

The OBU performs the general authentication process after the login process completes by the user. The OBU never uses the real uniqueness of the user to perform the authentication process so no one can get the identity of the user. The authentication process is done by the OBU with LE. The LE authenticate the OBU and becomes trustful by LE. Thus, the other mistrustful OBU can be authenticated by it without necessarily finding an LE.

G. Trust-Extended Authentication Procedure

Trust extended mechanism based on the idea of transitive trust relationships is better than the other authentication process. The situation of a mistrustful OBU becomes trustful and then gather an authorized parameter (i.e. PSK) when the OBU is authenticated successfully. Then, the trustful OBU plays the role of LE temporarily to help with the authentication procedure of a mistrustful OBU. In this process, the trustful vehicle performs the authentication process and works as an LE. It still does not require to store the authentication information of the user. So, this scheme only require few storage spaces. Then, the steps of the general authentication and the trust extended mechanism are the same. As a result, all vehicles in a VANET can complete the authentication process swiftly.

H. Password Change Procedure

This process is invoked when a user wants to alter his password. It can be completed without any help from the AS.

1. The user provide the ID and password.
2. The OBU checks the ID and password if it is correct than the user can give the new password and the new password replaces the old password.

I. Secure Communication Procedure

Two trustful vehicles do the secure communication process when they want to converse with each other. The steps are described as follows and in figure 4.

1. After the login procedure, the OBU sends a secure communication request to another OBU.
2. The OBU verifies that the sender OBU and if the OBU is trustful then it reply message.

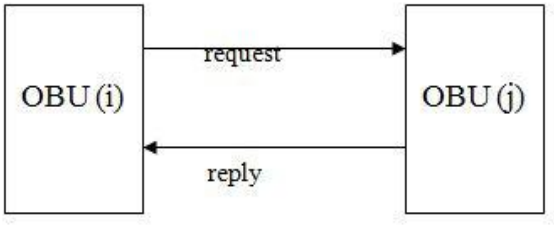


Fig 4: Secure vehicular communication.

J. Key Revocation Procedure

In this method it depicts lifetime of the key. If the lifetime of the key gets over than the vehicle becomes mistrustful otherwise it remains trustful vehicle.

4. ANALYSIS

This section discusses the security analysis, computational cost, and storage cost of TEAM. A TEAM satisfy the following security requirements.

A. Security Analysis

1. *Anonymity:* Under the proposed scheme, the original uniqueness of each user is always converted into an assumed name. Therefore an intruder cannot determine the user's original identity.
2. *No verification table*: The AS, LEs, and TVs do not require to store the user's verification table.
3. *Location privacy*: Even if an intruder intercepts a number of messages during a certain period, he cannot trace the user's physical position because the system's anonymity mechanism uses a dynamic identification process.
4. *Mutual authentication*: A mutual authentication process is necessary. The LE needs to verify that the OBU is a legal user, and the OBU needs to ensure that the LE is genuine.
5. *Resistance to replay attacks*: In order to protect the new scheme from replay attacks, we add a random number to the authentication message. If an intruder intercept the message and tried to copy a valid OBU by replaying the message immediately, the LE would reject the request because the nonce in the replayed messages would be invalid. Moreover, the OBU also checks the random number sent by the LE to prevent replay attacks.
6. *Resistance to modification attacks*: An intruder can effort to alter the authentication and reply messages. However, in this one-way hash function used to guarantee that information cannot be tailored.
7. *Fast error detection*: In the login or password change process, the OBU will detect an error at once if an intruder gives the wrong user ID or password.
8. *Choose and change password easily*: Users can choose or change their passwords without the AS's help and constrain, so that it is simple for them to remember their passwords.
9. *Resistance to man-in-the-middle attack*: The password and the secret key of the system are used to prevent the man-in-middle attack. The intruder cannot pretend to be trustful vehicle or LE to authenticate other MVs since he does not own the password.

B. Analysis of Storage Cost

In the asymmetric cryptography schemes, each vehicle needs to store the entire public key of users. However, this behavior in VANETs is costly and impractical. The complexity of storage cost of asymmetric cryptography is O(n), where n is the total number of vehicles in VANETs. Thus, these asymmetric cryptography schemes are not useful as the storage cost raise when the number of vehicles increases. On the other hand, the number of vehicles does not affect the storage cost of TEAM, and the complexity of storage cost of TEAM is O(1). As a result, TEAM saves lots of storage cost and with high scalability compared with the asymmetric cryptography schemes.

CONCLUSION AND FUTURE WORK

In this paper, we proposed a decentralized lightweight authentication scheme called TEAM to defend valid users in VANETs from spitful attacks. The amount of cryptographic calculation under TEAM was considerably less than in existing schemes because it only used an xor operation and a hash function. Moreover, TEAM is based on the concept of transitive trust relationships to improve the performance of the authentication process. In addition, TEAM has a few storage spaces to store the authentication parameters.

In the future, we will study three issues.

1. We intend to develop an intrusion detection mechanism to enhance the network security.
2. We will design a secure routing protocol for vehicular ad networks.
3. We will propose a cryptanalysis scheme to prove that our authentication mechanism is secure.
4. We will consider solving the inside attack.

References:

[1] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart
vehicles," *IEEE Security Privacy Mag.*, vol. 2, no. 3, pp. 49–55, May–
Jun. 2004.
[2] Dedicated Short Range Communications (DSRC) [Online]. Available:
http://grouper.ieee.org/groups/scc32/dsrc/index.html
[3] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *J.*
Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.
[4] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location
privacy in vehicular networks," in *Proc. First Int. Workshop Wireless*
Netw. Intell. Transp. Syst., Aug. 2007, pp. 1–7.
[5] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA:
Robust location privacy scheme for VANET," *IEEE J. Selected Areas*
Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
[6] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided
message authentication scheme in vehicular communication networks,"
in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 1451–1457.
[7] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication
mechanism for vehicular ad hoc networks," in *Proc. IEEE Int. Conf.*
Consumer Electron., Commun. Netw., Apr. 2011, pp. 1758–1761.
[8] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K.
Sezaki, "CARAVAN: Providing location privacy for vANET," in *Proc.*
ACM VANET, Sep. 2006, pp. 1–15.
[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identitybased
batch verification scheme for vehicular sensor networks," in *Proc.*
IEEE INFOCOM, Apr. 2008, pp. 246–250.
[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient
conditional privacy preservation protocol for secure vehicular communications,"
in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1229–1237.
[11] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented
vehicular networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 16–22,
Aug. 2009.
[12] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M.
Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular
communication systems: Design and architecture," *IEEE Commun.*
Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.
[13] G. Guette and C. Bryce, "Using TPMs to secure vehicular ad-hoc
networks (VANETs)," in *Proc. Int. Federation Informat. Process.*, May
2008, pp. 106–116.
[14] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "VANET security
framework for trusted grouping using TPM hardware," in *Proc. IEEE*
Int. Conf. Commun. Software Netw., Feb. 2010, pp. 309–3012.

A Survey of Vehicular Ad Hoc network on Attacks & Security Threats in VANETs

1**Mandeep Kaur Saggi,** 2**Ranjeet Kaur Sandhu**
1,2Dept. of CSE, D.A.V University, Jalandhar, Punjab, India
mandeepsaggi90@gmail.com , er.ranjeetsandhu@gmail.com

ABSTRACT-Vehicular Ad hoc NET work (VANET) is an emerging paradigm in networking. Vehicular ad-hoc networks (VANETs) are classified as an application of mobile ad-hoc network(MANET) that has the potential in improving road safety and in providing travelers comfort. VANET enables vehicle to vehicle (V2V) communication with the goal of providing road safety and reduce traffic congestion. The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by adversaries. In this paper, we review the secure infrastructure of VANET, some Security Challenges and applications. We also discuss about different attacks and security issues in VANET.

KEYWORDS: Vehicular Ad hoc Networks (VANETs), Routing protocols, Attacks, Security, Safety applications

I. INTRODUCTION

At the present time cars and other private vehicles are used daily by many peoples. The biggest problem regarding the increased use of Private transport is the increasing number of fatalities that occur due to accidents on the roads. Recently, with the advancement in technology more and more vehicles are being embedded with GPS and Wi-Fi devices that are connected in a self organized way, this enables vehicle to vehicle (V2V) communication, forming a Vehicular Ad-hoc NET work (VANET) [1]. VANETs are a subset of Mobile Ad-hoc NET works (MANETs) in which communication nodes are mainly vehicles. In the Case of this network should deal with a great number of highly mobile nodes, eventually disseminate in different roads. In VANETs as shown in Figure 1, vehicles can communicate each other is called as inter - vehicle communication or Vehicle-to-Vehicle communications (V2V), vehicles can connect to infrastructure that is road side units- (RSU) is called as vehicle-to-roadside or Vehicle to Infrastructure communication (V2I) to get some service.

This infrastructure is assumed to be located along the roads and infrastructure can communicate to each other is called as inter roadside or infrastructure-to-infrastructure (I2I) communication. These types of communications infrastructure allow vehicles to share different kinds of information for example protection information for the purpose of post-accident, accident prevention investigation or traffic jams.

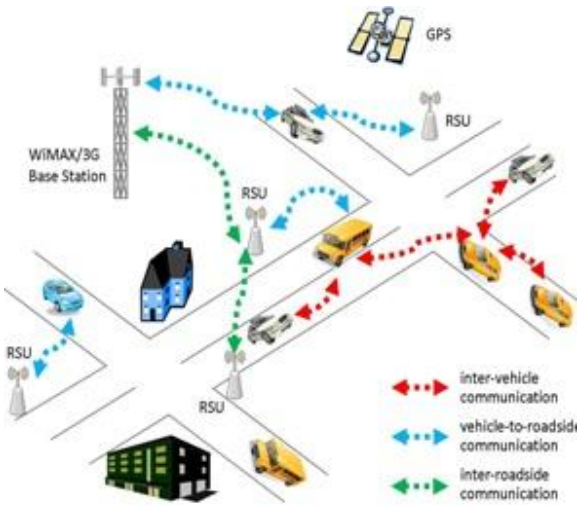


Figure 1: VANETs communication between V2V, V2I and I2I

VANET technology presents certain advantages, such as a reduction in the number of road accidents, a more enjoyable driving and traveling experience with the simplification of certain payment processes for tolls, parking, fuel, etc. Road users employ various

applications for safety and efficiency, traffic management, infotainment, warning, comfort, maintenance, music sharing and network gaming. These applications involve the exchange of messages such as emergency message distribution, traffic incidents and road condition warnings that enhance traffic safety and driving efficiency. These applications require data communication between nodes. The content of the message can have an impact on drivers' behavior. This may change the network topology and security may be threatened if a malicious user alters the message. Some possible attacks could cause traffic jams, spread bogus information, cheat the positioning information, disclose IDs, replay, masquerade or forge data, violate privacy or cause wormholes, Denial-of-Service (DoS) attacks, in-transit traffic tampering, impersonation as well as hardware tampering [2].

II. OVERVIEW OF VANET ARCHITECTURE

VANET architecture can be divided into three categories: the cellular/WLAN, ad hoc and hybrid architectures. If the infrastructure consists of a cellular gateway or a WLAN or a WIMAX access point, the network will be considered a pure cellular/ WLAN. When no infrastructure is available, the nodes must communicate with one another without relying on an infrastructure. This denotes a pure ad hoc architecture. Sometimes, various access points, such as cellular gateways, will be available for communication. In this case, nodes can communicate with these infrastructures or they may also communicate directly with one another. This is called a hybrid architecture.

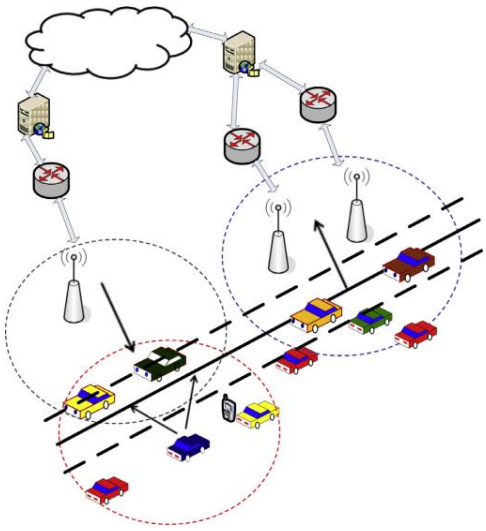


Figure 2: System architecture in VANETs.

The communication between vehicles or between a vehicle and an RSU is achieved through a wireless medium called WAVE. This kind of communication provides a wide range of information to drivers , travelers and enables safety applications to enhance road safety and provide a comfortable driving. The main system components are the application unit (AU), (OBU) and (RSU)

A. On board unit (OBU):

The main functions of the OBU are reliable message transfer, wireless radio access, ad-hoc and geographical routing, Network congestion control, data security and IP mobility. An OBU is a wave device usually mounted on-board a vehicle used for exchanging information with RSUs or with other OBUs.

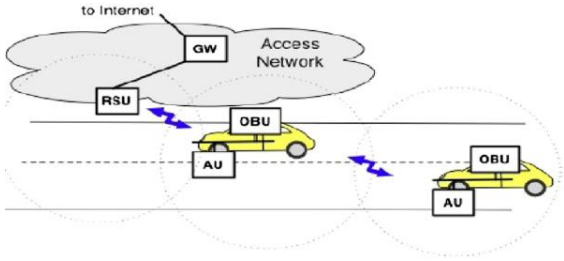


Figure 3: Vanet System Architecture (OBU, AU, RSU)

B. Application unit (AU)

The AU is the device equipped within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, The AU can be connected to the OBU through a wired or wireless connection and may reside with the OBU in a single physical unit the distinction between the AU and the OBU is logical.

C. Roadside unit (RSU)

The RSU is a wave device usually fixed along the road side or in dedicated locations such as at junctions or near parking spaces. The RSU is equipped with one network device for a dedicated short range communication based on IEEE802.11p radio technology, and can also be equipped with other network devices so as to be used for the purpose of communication within the infrastructural network.

1. Extending the communication range of the ad hoc network by re-distributing the information to other OBUs and by sending the information to other RSUs in order to forward it to other OBUs.

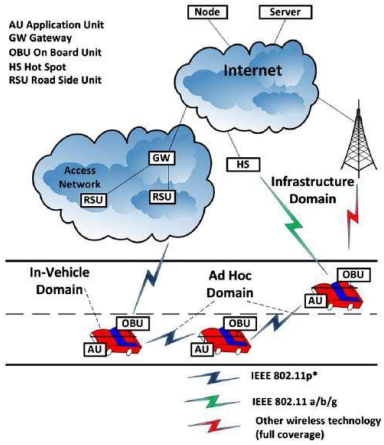


Figure 4: Vanet Architecture

2. Running safety applications such as a low bridge warning accident warning or work zone using infrastructure to vehicle communication (I2V) and acting as an information source.
3. Providing Internet connectivity to OBUs.

VANET architecture can be divided into different forms based on different perspective. According to as shown in figure 4, the architecture of VANET falls into three main categories:

A. Inter-vehicle communication
This is also known as vehicle-to-vehicle (V2V) communication or pure ad hoc networking. In this method the vehicles communicate among each other without infrastructure support. Any use full information collected from sensors on a vehicle or communicated to a vehicle can be directed to neighboring vehicles.

B. Vehicle-to-roadside communication
This is also known as vehicle-to-infrastructure (V2I) communication. In this category, the vehicles can use cellular gateways and wireless local area network access points to connect to the Internet and enable vehicular applications.

C. Inter-roadside communication
This is also known as hybrid vehicles-to-roadside communication (VRC). Vehicles can use infrastructure to communicate with each other and exchange information received from infrastructure or from other vehicles through ad hoc communication. Besides that vehicles can communicate with infrastructure either in single-hop or multi-hop fashion depending on their location during moving or stationary. This architecture includes V2V communication and provides greater flexibility in content sharing and increases network reliability.

According to the communication between vehicles and the RSU and the infrastructure form three types of domains as shown in figure. 5.

A. In-vehicle domain
This domain consists of an OBU and one or multiple AUs. An OBU and an AU can reside in a single device. The OBU provides a communication link to the AU in order to execute a set of applications provided by the application provider.

B. Ad hoc domain
The ad hoc domain on VANET is composed of vehicles equipped with OBUs and a station along the road side, the RSU. Two types of communications are available in the ad hoc domain: vehicle to vehicle (V2V) communication and Vehicle to RSU communication.

C. Infrastructural domain
The RSU can connect to the infrastructural networks or to the Internet, allowing the OBU to access the infrastructure network.

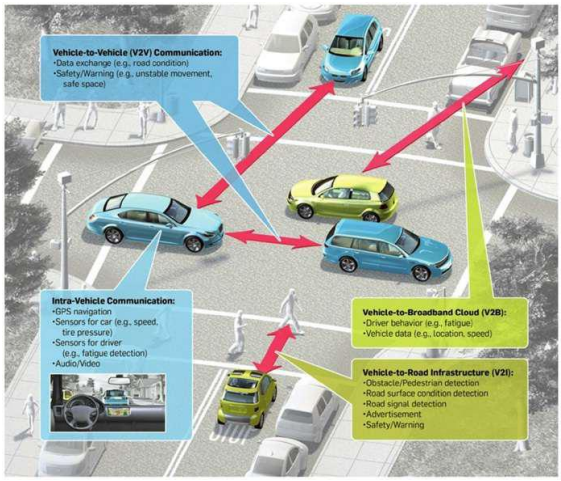


Figure 5: Communication types in VANET

III. APPLICATIONS OF VANET

VANET applications are classified according to their primary purpose into: Applications that increase vehicle safety on the roads are called safety applications. Applications that provide value added services, for example, entertainment, are called user applications.

A. User applications:
The main aim of comfort applications is to improve passenger comfort and traffic efficiency. Passengers in vehicles who spend a very long period in transit might be interested in certain application domain for vehicular networks consisting in the provision of many different types of information. These can provide vehicle users with various information, announcements, and entertainment during their journey. They can provide drivers or passengers with weather and traffic

information as well as detail the location of the nearest restaurant, hotel, café, petrol station and their prices. Passengers can play online games, access the internet and send or receive emails, chat with friends and can perform office works while the vehicle is connected to the infrastructure network.

B. Safety applications:

The main goal of the safety applications is to increase public safety and protect the loss of life. The main characteristic of these applications is that the safety data should be delivered to the intended receivers (vehicles approaching the dangerous area) within a bounded time. These applications use the wireless communication between vehicles or between vehicles and infrastructure, in order to improve road safety and avoid accidents; the intention being to save people's lives and provide a clean environment.

IV. CHARACTERISTICS AND CHALLENGES OF VANET

A. CHARACTERSITICS

Unique characteristics of VANETs that distinguish them from MANET are as follows [4]:

1. High mobility
2. Predictable and restricted mobility patterns
3. Rapid topology change
4. No power constraints
5. Localization
6. Abundant network nodes
7. Hard delay
8. Large scale network.
9. Energy storage and computing

B. CHALLENGES OF VANET

The main challenges of the vehicular networks can be summarized as follows:

1. Frequent neighborhood change due to high mobility

2. Increasing channel load (high density environment)

3. Irregular connectivity due to the variation of the received signal power

4. Packet loss due to exposed and hidden terminal problems

5. Keeping a reasonable balance between the security and privacy is one of the main challenges in VANET the receipt of trustworthy information from its source is important for the receiver. Keeping a reasonable balance between the security and privacy is one of the main challenges in VANET; the receipt of trustworthy information from its source is important for the receiver.

6. In Routing protocol beecause of the high mobility of nodes and rapid changes of topology, designing an efficient routing protocol that can deliver a packet in a minimum period of timewith few dropped packet s is considered to be a critical challenge in VANET. Frequent neighborhood change due to high mobility.

7. Involved entities in VANETs security:

7.1. The driver: The driver is the most important element in the VANET safety chain because it is ubiquitous and he has to make vital decisions. In addition, all used cases currently scheduled for VANET applications make the driver as an interactive component with the driving assistance systems.

7. 2. The vehicle (OBU): Although it does not reflect the reality, The OBU refers to the driver and the vehicle at the time in the literature. In a VANET network, we can distinguish two kind of vehicles: the normal vehicles that exist among network nodes and operate in a nor- mal way, and the malicious vehicles.

7.3. Road Side Unit (RSU): As in the case of the OBU, we can distinguish normal RSU terminals, which operate in a normal way, and malicious RSU terminals.

7.4. Third Parties: We denote by third parties (may be trusted or semi-trusted), all digital equivalents of stakeholders in a direct way in intelligent transportation system. Among these third parties, the regulator of transport, vehicle manufacturers, traffic police, and judges. They all have their respective secrets/public key pairs. These public keys can be integrated for example into the OBU which is supposed an inviolable device.

7.5. The Attacker: In the context of VANET security, the attacker is one (or more) compromise entity that wants to violate successfully the security of honest vehicles by using several techniques to achieve his goal. An attacker can also be a group of vehicles that cooperate together. An attacker may be internal (an authentic vehicle of the VANET network) or an external vehicle.

V. ATTACKS AND SECURITY THREATS IN VANETS

Attacker's role is important in vehicular network due to launching different type of attacks. The objective of attackers is to create problems for other users of the network by changing the contents type of messages.

Attackers can be classified according to scope, nature, and behavior of attacks as follow:

A. *Passive Attackers*

These attackers eavesdrop only on the wireless channel to collect traffic information which may be passed onto other attackers. As these attackers do not participate in the communication process of the network, they are called passive attackers

B. *Active Attackers*

These attackers either generate packets containing wrong information or do not forward the received packets.

C. *Insider Attackers*

These attackers who are an authentic user of the network and have detail knowledge of network. When they have all information about the configuration then it's easy for them to launch attacks and create more problem as compare to other attackers.

D. *Outsider Attackers*

The outsider attacker is considered as an authentic user of the network. It is a kind of intruder which aims to misuse the protocols of the network and the range of such attacks are limited. These attackers create fewer problems as compared to insider attackers.

E. *Malicious Attackers:*

These attackers are not personally benefited from the attack. Their aim is to harm other members of the network or disrupt the functionality of a VANET. These attackers are considered the most dangerous category since they can cause severe damage to the network.

F. *Rational attacker:* These attackers seek personal benefit and are more predictable in terms of type and target of the attack.

G. *Local attacker:* These attackers' launches an attack with a limited scope, that is, an attack is restricted to a particular area

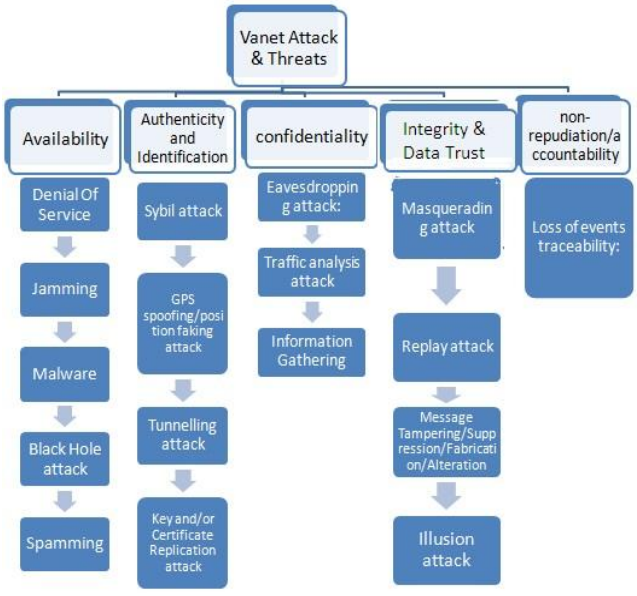


Figure 6: Vanet Attacks & Threats

Some are attacks Threats following below:

1. Attacks on availability

Availability is a very important factor for VANETs. It guarantees that the network is functional, and useful information is avail- able at any functioning time. This critical security requirement for VANETs, which main purpose is to ensure the users' lives, is an important target for most of the attackers. Several attacks are in this category, the most famous are the Denial of Service attacks (DoS).

1.1 DDoS attack

(Distributed Denial of Service) is a variant of DOS attacks, it is a distributed attack ordered by a main attacker who plays the role of "attack manager" with other agents who may be also victims unknowingly. The action methods of DDoS attacks are in most cases flooding the network and the results are always disastrous. Jamming, greedy behavior, black hole attack, is examples of DOS attacks

1.2 Jamming attack:

The jamming attack is a physical level of Denial of Service attack. Jamming in its basic definition is the transmission of a signal to disrupt the communications channel, it is usually intentional.

1.3 Greedy behavior Attack

Greedy behavior causes overload and collision problems on the transmission medium, which produces delays in authorized user's services. Greedy behavior is independent and hidden to upper layers, and then it cannot be detected by mechanism designed for those layers.

1.4 Black hole attack

In Black hole attack, the malicious node receives packets from the network, but it refuses to participate in the operations of routing data. A Black hole node can e.g. redirect the traffic that receives to a specific node which does not exist in fact and this causes data loss [6].

1.5 Malware attack:

Given the existence of software components to operate the OB and RSU, the possibility of infiltration of malware (malicious software) is possible in the network during the software update of VANET units

2. Attacks on authenticity and identification

Authenticity is a major challenge of VANETs security. All existing stations in the network must authenticate before accessing available services. Any violation or attack involving the process of identification or authentication exposes the entire network to a serious consequence. Ensure authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infiltrating the network using a

falsified identity [3]. The importance of identification–authentication process comes from the fact that it is frequently used whenever a vehicle needs to join the network or a service. There are several types of attacks in this category.

2.1 Sybil attack

The idea of the Sybil attack as presented for the first time in is that a malicious entity can present multiple identities at once. One of the direct means by which two entities can convince a third that they are distinct is to run, at the same time, some tasks that one entity cannot do it alone. To ensure the identity of a node, several techniques have been proposed such as testing resources based o computational, storage and communication challenges.

2.2 GPS spoofing/position faking attack

This attack consists on providing neighbors node a false location information. The exact location information can easily be obtained from a system such as GPS, when the name of the attack: GPS spoofing. Each vehicle of a VANET is equipped with a positioning system (receiver), then the attack can be achieved using a transmitter generating localization signals stronger than those generated by the real satellites

2.3 Tunneling attack

The tunneling attack is almost similar to the wormhole attack [8]. In this attack, attackers use the same net work to establish a private connection (tunnel), while in the Wormhole the attackers (assumed to be external) use a different radio channel for the exchange of packets. The Tunneling attack connects two distant parts of the vehicular network by using an additional communication channel such as a tunnel

2.4 Key and/or Certificate Replication attack

The attack consists in the use of duplicate keys and or certificates which used as proof of identification and to create ambiguity which make more difficult to authorities to identify a vehicle, especially in the case of dispute.

3. Attacks on confidentiality

Confidentiality is an important security requirement for VANETs communications; it ensures that data are only read by authorized parties. In the absence of a mechanism to ensure the confidentiality of the exchanged data between nodes in a vehicular network, exchanged messages are particularly vulnerable to attacks such as the improper collection of clear information.

3.1 *Eavesdropping attack*

In wireless networks such as VANETs, listening to the media is an attack easy to carry out. In addition, it is passive and the victim is not aware of the collection. Eavesdropping attack is against confidentiality, it is without imminent impact on the network [6]. Through this attack, several types of useful information can be collected such as location data that can be used for tracking vehicles.

3.2 Traffic analysis attack

In a VANET, the traffic analysis attack is a passive serious threat against confidentiality and privacy of the users. The attacker analyzes collected information after a phase of listening to the network, it tries to extract the maxi-mum of useful information for its own purposes.

4. Attacks on integrity and data trust

The integrity of exchanged data in a system is to ensure that these data have not been altered in transit. Integrity mechanisms help therefore to protect information against modification, deletion or addition attacks. In the case of VANETs, this category targets mainly V2V communications compared to V2I communications be-cause of their fragility. One of the possible techniques which facilitate this kind of attacks is the manipulation of in-vehicle sensors.

4.1 Masquerading attack

In this attack, the attacker is hidden using a valid identity (called a mask), and tries to form a Black hole or produce false messages that have the appearance of coming from an authentic node. For example, to slow down the speed of a vehicle or require it a lane changes. A malicious node at-tempts to act as an emergency vehicle e.g. and thus cheat the other vehicles.

4.2 *Replay attack*

This is a classic attack it consists in replaying (broadcast) a message already sent to take the benefit of the message at the moment of its submission. Therefore, the attacker injects it again in the network packets previously received. This attack can be used e.g. to replay beacons frames, so the attacker can manipulate the location and the nodes routing tables. Unlike other attacks, replay attack can be performed by non-legitimate users.

4.3MessageTampering/Suppression/Fabrication/Alteration

As its name implies, this attack is against integrity it consists in modifying, deleting, constructing or altering existing data. It can occur by modifying a specific part of the message to be sent [7]. For example, the attacker falsifies received data indicating that the route is congested, and changes them to deceive users, so it indicates that there is no congestion and traffic on the road is normal. In this attack, the attacker can also delete a part of the message, alter or make new

messages which help him achieving its intended purpose of the attack.

4.4 *Illusion attack*

A direct application of the fabrication of mes-sages attack is the Illusion attack, which is an attack against integrity and data trust. It consists in placing voluntarily sensors which generate false data. These data can move normally in the network and require drivers interaction to make decisions. Authentication mechanisms are not able to detect this attack, because the attacker connects to the network in an authentic way.

5. Attacks on non-repudiation/ accountability

Non-repudiation in computer security means the ability to verify that the sender and the receiver are the entities who claim to have respectively sent or received the message. Otherwise, the non-repudiation of data origin proves that data has been sent, non-repudiation of arrival proves that they were received. In a VANET context and since the manipulated data related to the safety and privacy of the users, it should be always possible to verify all hard- ware and software changes of security settings and applications (update, modification, addition, etc.

5.1 Loss of events traceability

Despite its importance, we have not seen any document that addresses this attack that we find quite feasible in a VANET environment. In fact, this non repudiation attacks consists of taking action, allowing subsequently an attacker to deny having made one or more actions.

VI. SECURITY SOLUTIONS

Modern cryptography offers several security techniques such as confidentiality, authentication, integrity, non-repudiation, secret sharing, etc. To satisfy these security services, cryptography uses methods such as encryption/decryption algorithms, Keys generation and exchange protocols, hash functions, digital signature and a lot of other techniques.

A. digital signatures

These are presented as a building block. In this section, the fact that safe messages must be authenticated in VANETs is emphasized and the preferred way of securing messages involves a digital signature.

B. Certification Authorities (CA)

A way to secure messages is presented. Before a vehicle sends a safety message, it signs it with its private key and includes the Certification Authorities (CA). After presenting this way of securing messages, a tamper-proof device is proposed to physically secure confidential information such as private keys. This device could also sign outgoing messages.

C. Cryptographic key distribution, certification and revocation are addressed.

For this purpose, they identified two components related to cryptography: the electronic identity and the anonymous key pairs used for privacy issues. This key will be boots trapped and rekeyed by the governmental transportation authority or the car manufacturer. The key must be authenticated by the certification authorities. It would be possible to revoke the key if compromising activities are observed. In order to ensure users' privacy, the use of anonymous public keys is proposed by the authors. In order to establish an authenticated session, the use of symmetric cryptographic primitives is suggested and switching between different channels or even communication technologies is suggested to prevent DoS attacks. To prevent bogus information attacks, the authors propose that the data received from a given source be verified by correlating it with those received from other sources. Anonymity is ensured by a key changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker.

D.PKI, digital certificates and time stamping:

A PKI can provide several security services, the most important is to be a trust third party between digital counterparts. PKI ensures that role through the certification authority (CA), so it signed, delivers and keep up to date digital certificates which rep- resent a digital ID for an entity. a certificate is an electronic file (can be stored in many forms), which binds together a public key with an identity with the guarantee of the certification authority. A certificate allows authenticating and signing (signing certificates) and also encrypting messages (encryption certificates). Time stamping is also among the services that PKI can provide. It certifies that an event (send/receive/signing a message,) happens at a given time. The time stamping faces basically to authentication and non-repudiation attacks.

E. Anonymous public keys:

Vehicle owners generally concern about identity and location privacy, since safety messages will not contain any secret data about their senders. [5]

1. Identity and location privacy

Although anonymous keys do not contain any public relationship to the true identity of the key owners, privacy can still be revealed by logging the messages containing a given key and thus tracking the sender until discovering his identity (for example, to associate the person with his place of living). Thereby, anonymous keys should be changed frequently such that a malicious observer cannot track the owner of the keys. The drawback of this approach is that a vehicle needs to store a lot of key and certificate set.

2. Conditional anonymity

Anonymity should be conditional and overridden on issues of law enforcement or national security. Police as well as other law enforcement entities may abuse their right, if they are given full control over the ID disclosure process. Thus, the capability of identity disclosure should be distributed among multiple authorities. For instance, police can be able to retrieve the identity corresponding to an anonymous key only after obtaining the permission of a judge.

F. Authenticated session establishment

Raya and Hubaux have considered several options to reduce this overhead. They prominently rely on the establishment of symmetric keys. If two nodes need to securely communicate for a long time, it is a common practice that two nodes will establish a shared session key. In terms of time and space overhead, symmetric cryptographic primitives are more efficient than the asymmetric ones. In the context of vehicular networks, the trust level is equal for all legitimate vehicle which possess an authorized certificate. Two different symmetric key types will be considered, pair wise and group keys.

G. Key agreement vs. key transport

In view of the equality of members, the distributed nature of VANET groups will naturally make key agreement be the general approach for key establishment. Several methods are available to fulfill this.However, key transport allows a group leader (either chosen by the specific application or randomly) to create a group key and broadcast it to all members. This method can efficiently terminate in one round but it will burden most of the computational overheads on the group leader. The group leader may also be a single point of failure.

D. CONCLUSION & FUTURE RESEARCH

1. CONCLUSION

Vehicle communication technology has become crucial in Designing vehicles for the future. VANET offers communication services among vehicles or with road side infrastructure. Given their importance related to the safety of humans' lives, VANETs attract attackers and represent a favorite target for several types of attacks which consequences vary from negligible to severe. Therefore, securing VANETs poses a great challenge. In this work, we reviewed some of the main areas that researchers have focused on in the last few years and these include attacks, security in VANETs. Hence enhance road safety and reduce the number of car accidents and traffic congestions.

2. FUTURE RESEARCH AREAS

VANETs introduce a new challenging environment for developers and communication engineers. There are many different hot topics to be studied by researchers are Mobilitilty Modeling, Routing Protocols, Scalability Issues, Security Frameworks, Quality Of Service (QoS) , Broadcasting.

E. REFERENCES

[1] Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, and Jie Zhang,"A Reputation-Based Announcement Scheme for VANETs ", IEEE Transactions on Vehicular Technology, Vol. 61, No. 9, pp. 4095-4108, November-2012.

[2] Engoulou, R. G.,Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications*, *44*, 1-13.

[3] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks(VANETs): status, results, and challenges, Telecommun. Syst. 50 (4) (2012)217–241.

[4] Tangade, S. S., & Manvi, S. S. (2013, July). Dept. of Electronics and Communication Engg., REVA Institute of Technology and Management, Bengaluru, India. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-6). IEEE.

[5] Wang, N. W., Huang, Y. M., & Chen, W. M. (2008). A novel secure communication scheme in vehicular ad hoc networks. Computer communications, 31(12), 2827-2837.

[6] A. Dhamgaye, N. Chavhan, Survey on security challenges in VANET, Int. J. Comput.Sci. 2 (2013) 88–96, ISSN 2277-5420.

[7] A. Rawat, S. Sharma, R. Sushil, VANET: security attacks and its possible solutions,J. Inform. Oper. Manag. 3 (1) (2012) 301–304.

Types and Techniques of Data Dissemination used in Vehicular Adhoc Networks- A Review

Er.Navneet Kaur
M.Tech Research Scholar
Department of Computer Science and Engineering
Amritsar College of Engineering & Technology, Amritsar
navneetsethi2102@gmail.com

Dr.Tanupreet Singh
Professor and HOD
Department of Electronics and Communication Engineering
Amritsar College of Engineering and Technology,Amritsar
tanupreet.singh@gmail.com

Abstract—**Vehicular Adhoc Network (VANET) is a form of Mobile Adhoc Network (MANET) in which vehicle nodes act as router as well as host. In VANETs data transmission is done through multihop communication in which the high speed vehicles are acting as data carrier. VANETs enable dissemination of traffic conditions and road situations as detected by moving vehicles independently. Data dissemination enables delivery of message from source vehicle to destination vehicles and it is used to improve the quality of driving in terms of safety, time and speed. This paper shows that there are different types of data dissemination and several techniques are there by which data can be disseminated. For each type there may be unique technique of data dissemination. Challenging task in data dissemination is to utilize limited bandwidth and disseminate maximum data over the vehicular network. Data aggregation is used for utilizing bandwidth efficiently.**

Index Terms—**Vehicular adhoc network; data dissemination; data aggregation**

I. INTRODUCTION

Vehicular Adhoc Network (VANET) is a form of Mobile Adhoc Network (MANET), where mobile nodes are vehicles [5]. VANETs provide wireless communication between vehicles and road side equipments [1]. Vehicles that are in radio range of each other can communicate with one another. In VANETs, delivery is not single hop rather multihop delivery is done and even the vehicle which is miles away from destination can also send their request like- traffic conditions, obstacle information can be obtained by the vehicles when they are currently not in the city [3]. VANETs are distributed, self-organized and potentially highly mobile networks of vehicles interacting via wireless media [2]. The main problem that needs to be solved in VANETs is how to exchange information in scalable fashion [4].

In Vehicular adhoc networks, there is very high mobility in which each vehicle node act as a router as well as host and sending packets to other mobile nodes and changing their topology very fast [3]. In Vehicular adhoc networks topology keeps on changing and also vehicles are not always connected to the network. There are frequent disconnections in VANETs. Therefore, protocols used in MANETs are not necessarily be suitable for VANETs as in MANET's protocols there is an implicit assumption of network connectivity [2, 3]. Intermittent connectivity, frequent changes in network topology and low reception rate are those properties that distinguish VANETs fromother types of adhoc networks [2].

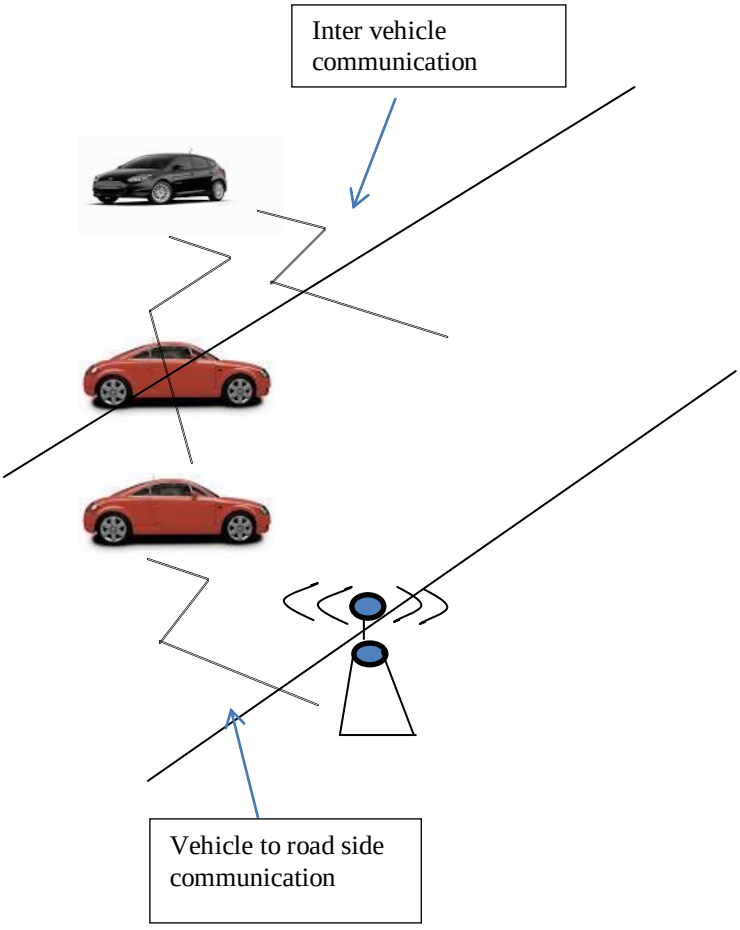


Fig1. Vehicular Adhoc network

A) Challenges in VANETS:

i) Multihop data delivery is challenging task as frequent disconnections and high mobility is there in VANETs [3].

ii) Gathering of information like accident, speed limit, obstacle information, and traffic conditions

etc. for safety and entertainment convenience purpose [3].

iii) Vehicles should be chosen for data delivery in such a way in such a way that packets will be transmitted with minimum delay to destination [3].

II. DATA DISSEMINATION IN VANETS

Data dissemination in VANETs is used to inform drivers or vehicles for traffic jams and to spread emergency warning messages among the vehicles (incidents or accidents) to avoid collision [1, 6]. So, data dissemination in VANETs improves the efficiency of traffic system. It also improves the quality of driving. In India alone,the total number of deaths every year due to road accidents has passed 130,000 mark, according to the latest report of National Crime Records Bureau (NCRB) **[8].** Indian roads usually have problems like traffic flow and instability. Lots of lives, money and time can be saved by sending or forwarding appropriate information to the driver or vehicle regarding congestion and traffic management. Numbers of techniques in comfort, safety and convenience have made and today's vehicle is totally different machine than it was in the past days. Now, a new technology that is characterized by proliferation of low cost wireless connectivity and distributed peer-to-peer cooperative systems is changing the way in which next generation vehicles will evolve. So data dissemination in VANETs plays a vital role for safety (such as collision warning, work zone warning etc.) and non- safety applications (like traffic condition applications and comfort applications) [6]. In short, data dissemination is a process of propagate data or information over distributed wireless networks, which is superset of VANETs [1].

A) Challenges in Data Dissemination:

i) High Mobility and Frequent Disconnections:

The big challenge in VANETs is the high mobility and frequently disconnected topology at different regions of the city. The traffic density is low during the night and in suburban areas, but network node density is very high in urban areas and especially during the peak hours in day time, which causes frequently network disconnection. There is no simple 'one-for-all' solution for disseminate data to all recipients spreading across the city [1].

ii) Data Transmission in presence of Disconnection:

The second main challenge in VANETs how to disseminate data over the network with less delay and before occurring the disconnections among vehicles. When target vehicle moves closer to the roadside unit and placed in densely area, disconnection is less concern. But the major problem is when different vehicles those are in radio range of one another requesting the same data at the same time and sharing the wireless media then utilization of bandwidth is the key issue. When a vehicle reaches within the one-hop range of the road side units, data can be transmitted to the vehicle at the highest throughput. Thus a vehicle passes by the roadside unit, it is most desirable to extend the connection time between the vehicle and road side unit so as to spread more data [1].

iii) Data Distribute over the Mesh Nodes:

For efficient data dissemination, many roadside units are connected together to form an infrastructure like mesh network and cooperatively disseminate data to the vehicles. So, it becomes very difficult how to distribute data in the mesh network [1].

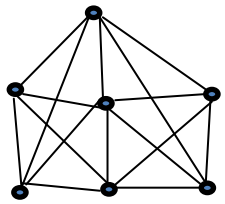


Fig2. Mesh Network

B) Types of Data Dissemination

Data Dissemination is a process of spreading data or information over distributed wireless networks. Aim of data dissemination is the optimum use of network resources to serve the data needs of all users [1]. Different types of data dissemination used in VANETs are:

i) V2I/I2V Dissemination (Vehicle to infrastructure or RSU)

ii) V2V Dissemination (Vehicle to vehicle)

iii) Opportunistic Dissemination

iv) Peer-to-peer Dissemination

v) Cluster Based Dissemination

i) V2I/I2V Dissemination:

It consists of two types of mechanisms: Push based and pull based. In Push based data dissemination, data pouring and buffering concepts are used. With data pouring concept, road is selected having high mobile vehicles and data center broadcast the data to the vehicles on the same road as well as on crossing roads. Data center is a computer having wireless interface that collects the data from outside world and deliver it to the vehicles. And buffers are placed at intersection points to store the data and from these buffers data will be transmitted to moving vehicles [3]. So, in push based data dissemination, data is efficiently delivered from the moving vehicles or RSUs (Road Side Units) to another vehicle [1]. While pull based data dissemination scheme is used by vehicles if they want to get some information from data center or from some other vehicles. This scheme is mainly used by vehicles for making queries and receiving response [3].

ii) V2V Dissemination:

In vehicle to vehicle data dissemination flooding and relaying mechanisms are used [1]. In flooding, data is broadcasted to all nodes that participate in data dissemination. One to all communication is done here. In the relay type of data dissemination, relay node is selected and this node forward the data to next relay hop and so on. Relay approach is generally preferred for congested networks [1].

iii) Opportunistic dissemination:

In opportunistic data dissemination, messages are stored at each intermediate node and forwarded to every encountered node till the destination is reached [1].

iv) Peer-to peer Dissemination:

In P2P dissemination, the source node stores the data in its storage device and sends the data in the network only when it is demanded by another node [1].

v) Cluster Based Dissemination:

In order to reduce broadcast storms and for providing better delivery ratio, a data packet has to be relayed by a minimum of intermediate nodes to the destination. To do so, nodes are arranged on a set of clusters in which one node or more collects data in its cluster and send them after to the next cluster [1].

III. COMPARISON OF DATA DISSEMINATION TYPES

Dissemination Type	Dissemination Approach	Pros	Cons	Reference
V2I/I2V	Push based	Suitable for popular data	Unsuitable for non-popular data	[6]
	Pull based	Suitable for non-popular data, user specific data	cross traffic incurs heavy interferences and collisions	[1,6]
V2V	Flooding	Data distribution is done quickly and reliability	Not suitable for dense networks	[6]
	Relaying	Works well in dense networks and in congested networks	Selecting next best hop and reliability is difficult	[1,6]
Opportunistic	Store and forward	Routes are built dynamically	It is data centric architecture in which applications are not concerned with transporting data to the right place.	[1, 9, 10]
P2P	Store and forward on asking	Works well in delay tolerant applications	Messages are not sent in the network	[1, 11]
Cluster based dissemination	Clusters are generated	It provides high delivery ratio and delay is less	It does not allow all nodes to broadcast messages	[1, 11]

Table1. Comparison of types

IV. TECHNIQUES USED IN DATA DISSEMINATION

Data Dissemination is a process of spreading data or information over distributed wireless networks. Aim of data dissemination is the best use of network resources to serve the data needs of all users [1, 6]. But data dissemination is a challenging task because by utilizing limited bandwidth, maximum data has to transmit over the vehicular network [3]. The solution of above problem lies in data aggregation. Data aggregation is a process in which bandwidth is utilized efficiently as whole data is integrated before sending them on vehicular networks. And it also helps in reducing the data redundancy.

In order to access data more efficiently many researchers have provided several techniques to disseminate the data. Some of the techniques are described in this paper:

i) Opportunistic Dissemination:

In this technique, data center is used which is responsible for broadcasting the data to the vehicles and vehicles which are in range of data center will receive and store the data. Whenever two vehicles will reach into the transmission range of each other, they will be able to exchange data. Advantage of this technique is that there is no need of any infrastructure and are suitable for highly dynamic VANETs [3]. And Drawback is that data cannot be efficiently updated in urban areas [3] as there is no infrastructure so there is no way to store the data and in urban areas vehicle density is too high and frequent network disconnections are there because of this media access control (MAC) layer collision usually occurs.

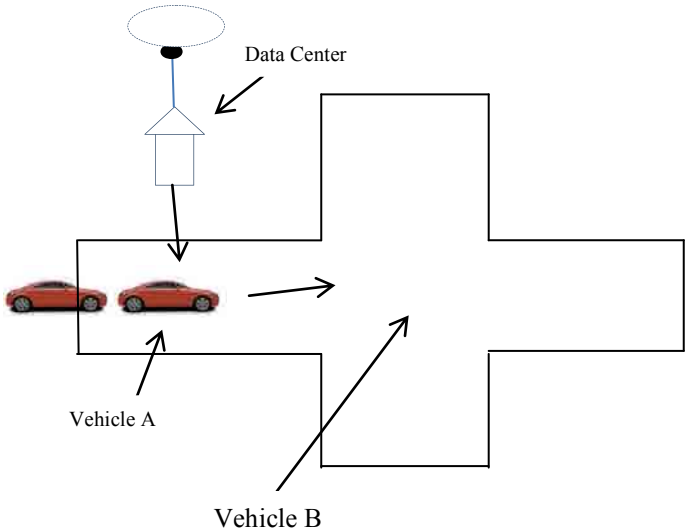


Fig3. Opportunistic Dissemination

ii) Push Based Dissemination Technique:

In Push based data dissemination technique, data is managed by data center that collects the data from outside world and deliver the data to the vehicles. Data center can be a computer/ workstation having wireless interface. Data center makes a list of data items that needs to be disseminated over the network. Data center sends this information on the road with header which contains all necessary information [3] like source id,

source location, forwarding direction, and packet generation time etc.

Data Pouring and Buffering are two schemes that come under push based data dissemination.

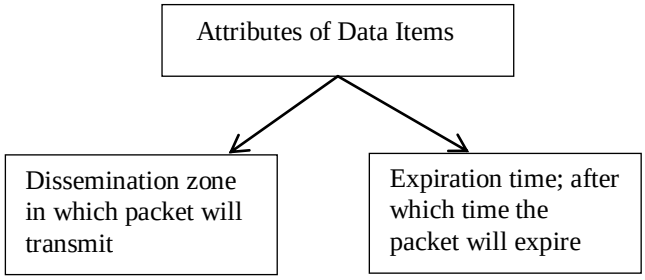


Fig4. Data items' attributes

a) **Data Pouring (DP):**

The Data Pouring scheme selects that road having high density and mobility of vehicles i.e. axis road (A-road) and data center broadcasts data not only to that road (A-road) but as well as on the crossing roads (C-roads) as shown in figure 6.

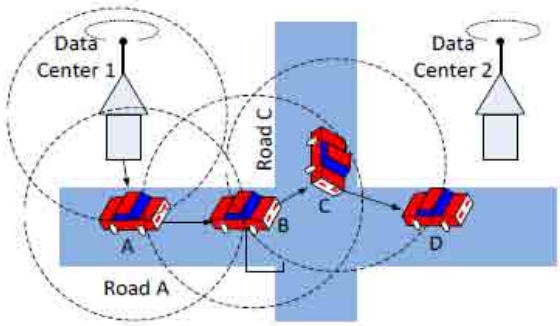


Fig5. Directional Broadcast [3]

b) Data Buffering:

Data Buffers or Intersection Buffers (IBers) are located at intersection points which are used to store the data at the intersections and in this scheme data is transferred from data center to the buffers located at the intersections and from these buffers data is transmitted to the vehicles. Advantage of using Data Pouring Intersection buffering scheme is that availability of data is increased at intersections and the load on server is reduced and data delivery ratio is increased [3].

iii) Pull Based Dissemination Technique:

Pull based data dissemination technique is mainly used by vehicles if they want to get some information from data center or from some other vehicles. This scheme is used by some specific users. In this technique, data is managed by data center and the vehicles which are moving on the road [3]. In this scheme, carry and forward mechanism is used to deliver the data. And dynamic path selection is done throughout the packet forwarding process because vehicular adhoc networks are unpredictable in nature, so best path for successful routing cannot be computed before delivering the packet [3].

Since, pull based dissemination technique is pivoted around making queries and receiving responses. So, the whole process is divided into two sub processes:

a) Requesting data from moving vehicle to fixed location:

This approach is explained by Vehicular Assisted Data Dissemination (VADD) Protocol and forwards packet either in intersection mode or in straightway mode until the packet reaches to the destination [3].

When packets are forwarded in intersection mode then there are two choices that lead to two different forwarding protocols: Location First Probe (L-VADD) and Direction First Probe (D-VADD). In L-VADD protocol, vehicle reaching to the intersection will forward its packet to the vehicle that will be in its range and whose direction will be opposite to the destination vehicle but that is near to the destination vehicle. In case of D-VADD protocol, packets are forwarded to the vehicles which are moving in the direction of destination vehicle.

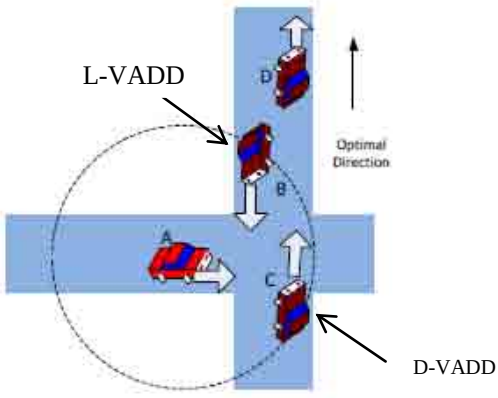


Fig6. Selection of next vehicle to forward the packet using L-VADD or D-VADD protocols [3]

While in case of straightway mode simply the greedy approach is used to forward the packet to the destination in which packets wait for vehicles moving in the direction of destination and when it finds such a vehicle it forwards the packet to that vehicle [3]. Protocols are also used in this mode some of them are: Vehicle Density Dependent Data Delivery (VD4) protocol, Vehicle Collision Warning Communication (VCWC) protocol etc.

b) Receiving response from fixed location to moving vehicle:

VADD protocol deals with the pull based technique of data dissemination in VANETs. When the data packet has to be forwarded from one place to another then this protocol suggests that which path should be selected and path selection is done on the basis of high density of vehicle even by following that path data has to traverse more distance but data forwarding delay will be less on this path [3].

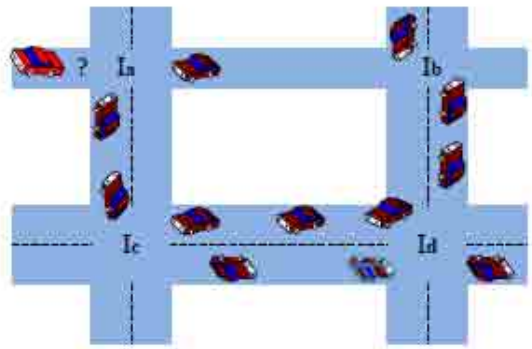


Fig7. Find a path to the destination [3]

Suppose any vehicle is coming towards the intersection $I_a$and it wants to send the request to its friend located at the corner of Intersection Ib (as shown in above figure). To forward the request through Ia→Ic→Id→Ib would be faster than through Ia→Ib although it provides the shortest possible routing path. The reason is that in case of disconnection, the data packet has to be carried by the vehicle whose moving speed is significantly slower than the wireless communication [3].

V. CONCLUSION

This paper shows that there are various types of data dissemination. Each type has its own pros and cons. Number of techniques are there through which data can be disseminated. It would be very difficult to say which technique is best for disseminating data or information as it depends upon particular road situation and vehicle condition. Disseminating data is a challenging task because by utilizing limited bandwidth, maximum data has to disseminate over vehicular networks. For this, one mechanism known as Data aggregation comes in which bandwidth is utilized efficiently because in this mechanism, whole data is integrated first and redundant data is eliminated in order to make best use of available bandwidth and then integrated data is transferred over the network.

VI. REFERENCES

[1]MorAnnu, "Study of Different Type of Data Dissemination Strategy in VANET," International Journal of Engineering Science and Innovative Technology (IJEST), Vol.1, issue2, nov-2012, pp. 6-8

[2] DaraghmiYousef-Awwad, Yi Chih-Wei, Stojmenovic Ivan, Abdulaziz King, "Forwarding Methods in Data Dissemination and Routing Protocols for Vehicular Ad Hoc Network," IEEE 2013, pp. 74-79

[3] DubeyBrijBihari, Chauhan Naveen, Kumar Prashant, "A Survey on Data Dissemination Techniques used in VANETs," International Journal of Computer Applications, vol.10, issue7, nov-2010, pp. 5-10

[4] NadeemTameer, Shankar Pravin, IftodeLiviu, "A Comparative Study of Data Dissemination Models for VANETs", IEEE july-2006

[5] Kakkasageri M.S., Manvi S.S., "Regression based critical information aggregation and dissemination in VANETs: A cognitive agent approach," july 2014

[6] TomarPratibha, ChaurasiaBrijesh Kumar, Tomar G.S., "State of the Art of Data Dissemination in VANETs," International Journal of Computer Theory and Engineering, Vol.2, No.6, Dec-2010, pp. 957-962,

[7] Salvo Pierpaolo, Cuomo Francesca, Baiocchi Andrea, Bragagnini Andrea, "**Road Side Unit coverage** extension for data dissemination in VANETs"

[8] http://www.dw.de/india-has-the-highest-number-of-road-accidents-in-the-world/a-5519345-1

[9] L.Pelusi, A. Passarella, M. Conti, "Opportunistic Networking: data forwarding in disconnected mobile adhoc networks" Communication Magazines, IEEE Vol.44, Issue 11, Nov-2006, pp.134-141

[10]http://orbit.dtu.dk/fedora/objects/orbit:82647/datastreams/file_5048167/content

[11] Kumar Sushil, Rani Sudesh, "A Study and Comparative Analysis of cluster based data dissemination protocols in VANETs," International Journal for Science and Emerging Technologies with Latest Trends Vol.14, Issue 1, 2014, pp. 12-16

An Efficient Algorithm for Load Balancing and Cluster Identification in MANETs

Jayant Vats
Department of Computer Applications
Amritsar College of Engineering & Technology
Amritsar, INDIA
jayantvasu@gmail.com

Dr. Tanu Preet Singh
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology
Amritsar, INDIA
tanupreet.singh@gmail.com

Abstract: MANETs are set of nodes that act autonomous to form temporary connections in between them. The network formed using such nodes is also temporary and allows low cost infrastructure deployment for its operability. The major research issue with such network during last few years is load balancing. This means adequate sharing of data amongst network nodes to sustain the network for longer duration. In this paper, an algorithm is proposed based on the load balancing and cluster identification that can be integrated with a routing protocol to enhance the performance of such network. The proposed algorithm is integrated with maodv and its effectiveness is checked using simulations.

Keywords: MANETs, load balancing, cluster formation, maodv.

I. INTRODUCTION

A mobile Ad hoc network (MANET) is an autonomous system of mobile hosts which are free to move around randomly and organize themselves arbitrarily. All wireless enabled devices within the range of each other can discover and communicate in a peer-to-peer fashion without involving central access points. In Ad hoc networks nodes can change position quite frequently. The nodes in an ad hoc network can be Laptops, PDA (personal digital Assistant) or palm tops etc. These are often limited in resources such as CPU capacity, storage capacity, Battery Power, Bandwidth. Each node participating in the network acts both as a router and as a host and must therefore is willing to transfer packets to other nodes. For this purpose a routing protocol should try to minimize control traffic. There is limitation of Battery life and in an Ad hoc environment battery is most commonly used. The mobility of nodes and the error prone nature of the wireless medium pose many challenges, including frequent route changes and packet losses, in the way of meeting the requirements of QoS. Such Challenges increases packet delay, decreases throughput and reduce network failure. The network performance degradation gets worse as traffic load increases. Despite there are large amount of effort invested in routing protocols, improving TCP performance and medium access control (MAC) for MANET [1]. MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. MANET technology allows a set of mobile uses equipped with radio interfaces (Mobile nodes) to discover each other and dynamically form a communication network [2]. MANET provisioning of real time multimedia services such as voice and video over ad- hoc networks is problematic since wireless links are unreliable and are of limited bandwidth [3].MANET incorporates routing functionality into mobile nodes so that they become capable of forwarding packets on behalf of other nodes and thus effectively become the infrastructure. Providing multiple routing paths between any source-destination pair of nodes has proved to be very useful in the context of wired networks.

In this paper, an algorithm is proposed that integrates load balancing and cluster identification schema with maodv routing protocol to enhance its performance in terms of packet delivery ratio and throughput. The remaining paper is structured as follows: Section 2 gives brief related work; proposed schema is presented in section 3. Results and discussions are presented in section 4. Section 5 concludes the paper.

II. RELATED WORK

The multipath routing appears an efficient solution for the ad hoc networks. It can provide load balancing and route failure protection by distribution traffic among a set of diverse paths. Load balancing mechanism allowing the traffic through the less congestion route [4]. Multipath routing allows the establishment of multiple paths between a single source and single destination node [5]. Multipath routing protocols are useful for finding more than one possible route between source and the destination [3]. A formula used by routers to determine the appropriate path onto which data should be forwarded. The routing protocol also specifies how routers report changes and share information with the other routers in the network so that they can reach. A routing protocol allows the network to dynamically adjust to changing conditions, otherwise all routing decisions to be

predetermined and remain static [6]. The details of some of the routing protocol that support load balancing is given below:

1. AODV
2. DSR
3. DSDV
4. MAODV
5. AOMDV
6. PUMA
7. TORA

In this paper, the algorithm is integrated with maodv routing protocol and its performance is evaluated over the standard metrics.

III. PROPOSED LOAD BALANCING ALGORITHM

The algorithm operates in two parts. The first part controls the cluster formation that helps in deciding the coordinating units of the network. In the second part, load is balanced using the location based identification of each node marked by distance and position with respect to each other. This allows nodes to trace the path and also allows formation of efficient connections between any two peers at same moment, thus, preventing total dependency on the single node. The algorithm for load balancing is shown below:

1. Check_network(Initialize)
2. Set centralized_node== node (0)
3. Identify cluster(node)
4. While(cluster_formation=false)
5. {
6. While (Ring_Search (n) ==True)
7. {
8. Set node_location=GPS Reading
9. Generate Postion_Signal
10. If (Node_location==Common)
11. {
12. Change_direction (node (n))
13. }
14. Else
15. {
16. Reset_GPS
17. }
18. Maintain GPS_Table
19. cluster_formation( )
20. {
21. Relay_node(S)
22. S (Node, Current_location, Location_changed)
23. Maintain location_change_table
24. Check for common entries
25. If(entry_common)
26. {
27. Transmit Hello
28. Ack (Random)
29. Send refine_msg
30. Trace_route
31. }
32. Exit
33. Check for common entries
34. Exit
35. }
36. }

The proposed algorithm can easily be integrated with any of the above given routing protocol with modification in its headers. The algorithm proposed uses GPS device to track the moment of each node. The system is maintained as a tree structure maintained as binary heap. All the normal process of node addition and subtraction is performed just similar to tree procedures.

IV. SIMULATION RESULTS

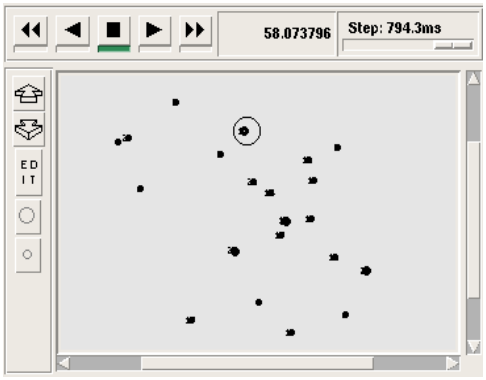


Fig 1. Intial Structure

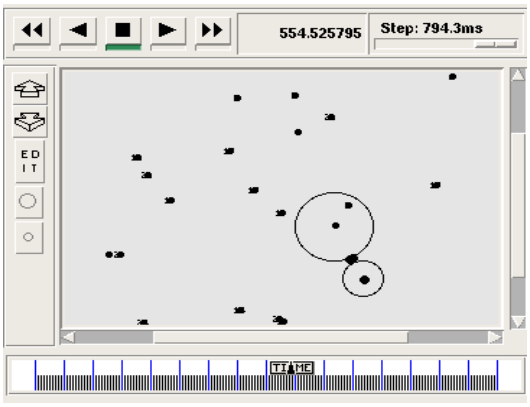


Fig 2. Formation of Clusters

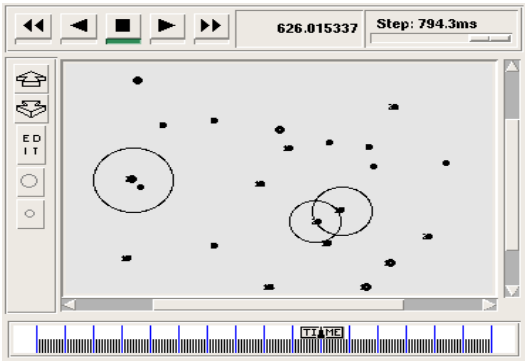


Fig 3. Identification of Clusters

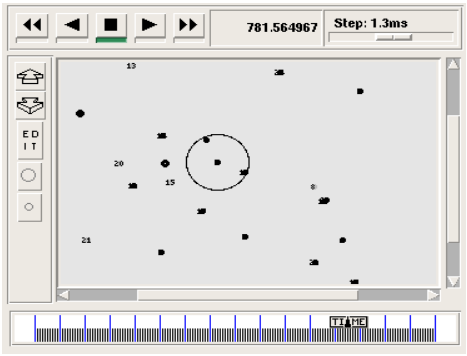


Fig 4. Range Identification

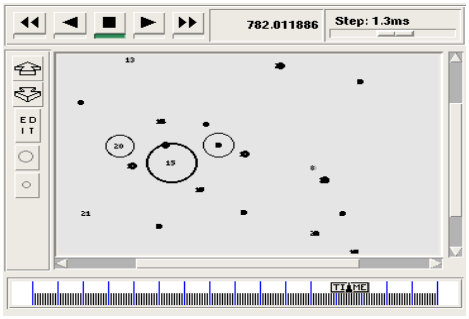


Fig 5.Node Cluster Ranging and Communication

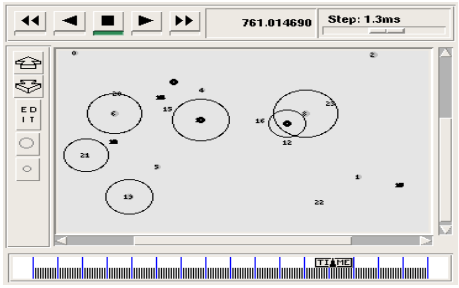


Fig 6. Data Transmission and Colaboration

Explanation of Simulation Results:

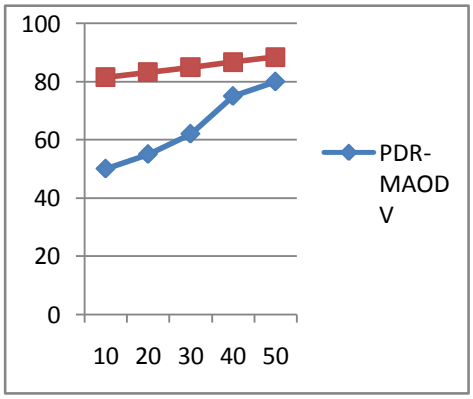
The above figures show the initial structure of mobile Adhoc networks and the formation of Clusters. After that the node finds that weather it belongs to that particular cluster or not and the Communication nodes weather its lies in the range of another node or not for data communication. Node will identify the next possible relay node that detects its range. After Detecting, it will finally collaborate with that particular note for communication. At last data transmission between the nodes of different clusters and balancing the load between the clusters.

V. RESULTS

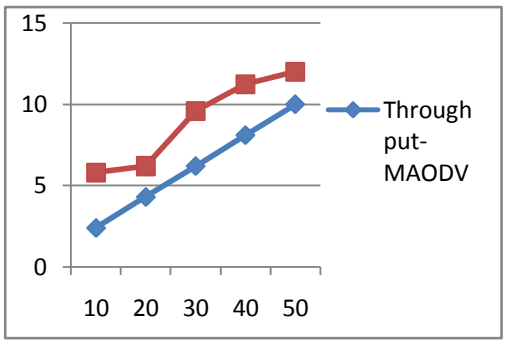
The network simulations for the proposed algorithm were carried using NS-2 simulator. The base protocol for evaluation considered was maodv as its header is simple and effectively supports load balancing. The various parameters configured for evaluations are shown in table below:

Paramete	Value
Dimensions	1000X1000 sq. m.
Number of Nodes	10-50
Simulation Time	300 s
Source Type	CBR
Number of Connections	10
Packet Size	512 bytes
Mac	IEEE 802.11 b
Buffer	50 packets
Propagation Radio Model	Two Ray Ground
Physique layer	Band width as 2
Maximal Speed	10 m/s
Pause Time	10 s
Interval Time To send	2 packets /s

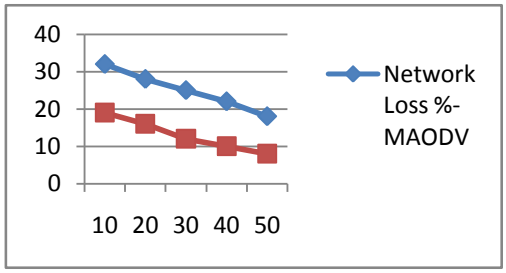
The results for analysis were traced for:
1. Packet Delivery ratio
2. Throughput
3. Network Losses
4. Percentage Load Balanced



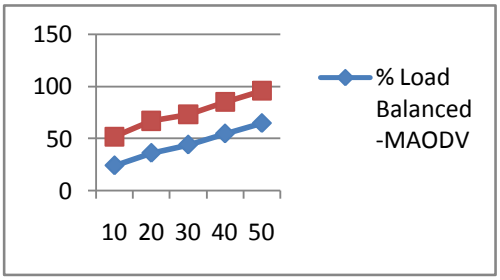
Graph 1. Packet Delivery Ratio



Graph 2. Throughput



Graph 3. Network Loss



Graph 4. Percentage Load Balanced

VI. CONCLUSION

In this paper, an efficient load balancing algorithm is proposed that can effectively solve the routing issues in MANETs. The proposed algorithm is integrated with maodv routing protocol to give network analysis and to demonstrate its effectiveness. The algorithm is capable to handle load more efficiently when integrated with proposed algorithm, thus, showing improvement in terms of lesser network loss, more throughout and packet delivery ratio with higher percentage of load balanced.

References

[1] Maysam Hedayati, Hamid reza hoseiny, Seyed Hossein Kamali, Reza Shakerian, " Traffic Load Estimation and Load Balancing in Multiple Routing Mobile Ad Hoc Networks", 2010 International Conference on Mechanical and Electrical Technology(ICMET 2010), 2010 IEEE, pp 117-121

[2] M.Saravana karthikeyan, M.Murali, Dr.S.Sujatha:"Identifying performance metrics to maximize Manet's throughput"; 2010 International Conference on Advances in Computer Engineering.

[3] Manika Vinay Rali, Min Song, Sachin Shetty:"Virtual wired transmission scheme using directional antennas to improve energy efficiency in Wireless Mobile Ad Hoc Network"; 978-1-4244-2677-5, IEEE 2008.

[4] http://www. csi.uoregon.edu.

[5] Sehoon Kim, Jinkyu Lee and Ikjun Yeom," Modeling and Performance Analysis of Address Allocation Schemes for Wireless sensor networks", IEEE transactions on vehicular technology, vol. 57, NO. 1, JANUARY 2008.

[6] Rekha Patil, Dr. A. Damodaram:"cost basedd power aware cross layer routing protocol for Manet"; 2008 IJCSNS.

[7] Changchun Bae and Wayne E. Stark:"A Tradeoff between Energy and Bandwidth Efficiency in Wireless Networks"; 2007 IEEE.

[8] V. Rodoplu and T. H. Meng: "Bits-per-Joule capacity of energy-limited wireless networks," IEEE Transaction Wireless Communications, vol.6(3), pp.857-865, March 2007.

[9] B. Rankov and A. Wittneben: "Spectral efficient protocols for half-duplex fading relay channels," IEEE Journal on Selected Areas in Communications, vol. 25, pp.379-389: Feb. 2007.

Network simulator-2 www.isi.edu/nanam/ns/.

Comparative Study Of Various Routing Protocols In Adhoc Networks

Er. Bhawna Dhawan
M.Tech Research Scholar
Deptt. of CSE
PTU Regional Centre
ACET, Amritsar
Bhawnadhawan52@gmail.com

Abstract

A Mobile Ad hoc NETwork (MANET) is a self-organizing, temporary, infrastructure-free, multi-hop, dynamic topology wireless network that contains collection of cooperative autonomous freely roaming mobile nodes. The nodes communicate with each other by wireless radio links with no human intervention. Each mobile node functions as a specialized router to forward information to other mobile nodes. In order to provide efficient end-to-end communication with the network of nodes, a routing protocol is used to discover the optimal routes between the nodes. The routing protocols meant for wired networks can not be used for MANETs because of the mobility of nodes. Routing in ad hoc networks is nontrivial due to highly dynamic nature of the nodes. Various routing protocols have been proposed and widely evaluated for efficient routing of packets. This paper presents an overview on classification of wide range of routing protocols for mobile ad hoc wireless networks.

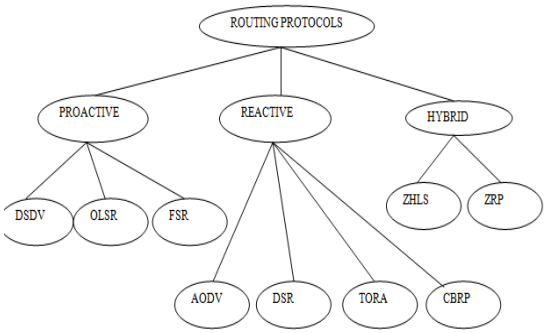
Keywords: routing, routing protocols, classification, comparison etc

I. INRODUCTION

The advent of ubiquitous computing and the proliferation of portable computing devices have raised the importance of mobile and wireless networking. Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. Ad hoc is a Latin word, which means "for this purpose only". The term "ad hoc" tends to imply "can take different forms" and "can be mobile, stand alone, or networked" [1]. Ad hoc networks have the ability to form "on the fly" and dynamically handle the joining or leaving of nodes in the network. Mobile nodes are autonomous units that are capable of roaming independently. Typical mobile ad hoc wireless nodes are Laptops, Personal Digital Assistants, Pocket PCs, Cellular Phones, Internet Mobile Phones, Palmtops or any other mobile wireless devices. All of these have the capability and need to exchange information over a wireless medium in a network. Mobile ad hoc wireless devices are typically lightweight and battery operated[2]. The nodes in the network are free to move independently in any direction. Node mobility causes route changes. The nodes themselves are responsible for dynamically discovering other nodes to communicate. When a node wants to communicate with a node outside its transmission range, a multi-hop routing strategy is used which involves some intermediate nodes. The network's wireless topology changes frequently and randomly at unpredictable times. Every node in ad hoc wireless network acts as a router that discovers and maintains routes in the network. Hence, the primary challenge is to establish a correct and efficient route between a pair of nodes and to ensure the correct and timely delivery of packets. Route construction should be done with a minimum of overhead and bandwidth consumption. Various protocols-proactive, reactive and hybrid-have been proposed and widely evaluated for efficient routing of packets in the literature [2-3].Routing protocols [2-5] often are very vulnerable to node misbehavior. A node dropping all the packets is considered as malicious node or selfish nodes. A malicious node misbehaves because it intends to damage network functioning. A selfish node does so because it wants to save battery life for its own communication by simply not participating in the routing protocol or by not executing the packet forwarding. A malicious node could falsely advertise very attractive routes and thereby convince other nodes to route their messages via that malicious node.These protocols can be classified into three different groups:global or proactive,on demand or reactive and hybrid. In proactive routing protocols,the routes to all the destinations(or parts of the network) are determined at the start-up .required by the source using a routing discovery process. Hybrid routing protocols combine the basic properties of two classes of protocols into one. That is, they

are both reactive and proactive in nature. Each group has a number of different routing strategies, which employ a flat or a hierarchical routing structure. The domain of applications for ad hoc wireless networks is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks [2-4].

II. CLASSIFICATION OF ROUTING PROTOCOLS



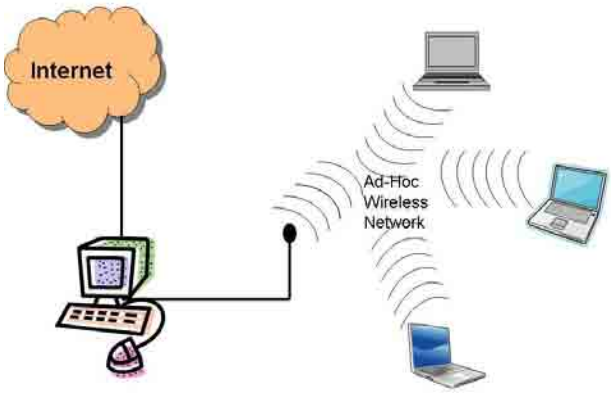


Fig1. Adhoc network**[7]**

i. PROACTIVE

A proactive routing protocol is also called a "table-driven" routing protocol. Using a proactive routing protocol, nodes in a mobile ad hoc network continuosly evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one. In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. Whwn a network topology change occurs, respective updates must be propagated throughout the network to notify the change. Most proactive routing protocols proposed for mobile ad hoc networks have inherited properties from algorithms used in wired networks. To adapt to the dynamic features of mobile ad hoc networks, necessary modifications have been made on traditional wired network routing protocols. Using proactive routing algorithms, mobile nodes proactively update the network state and maintain a route regardless of whether data traffic exists or not and the overhead to maintain up-to-date network topology information is high. Following are proactive network routing protocols.

a. DESTINATION-SEQUENCED DISTANCE VECTOR(DSDV)

DSDV is also based on the traditional Bellman-Ford algorithm. However, its mechanisms to improve routing performance in mobile ad hoc networks are quite different. In routing tables of DSDV, an entry stores the next hop toward a destination, the cost metric for the routing path to the destination and a destination sequence number that is created by the destination. Sequence numbers are used in DSDV to distinguish stale routes from fresh one and avoid the formation of route loops. The route updates od DSDV can be either time driven or event driven. Every node periodically transmit updates, including its routing information, to its immediate neighbors. While a significant change occurs from the last update, a node can transmit its changed routing table in an event-triggered style. Moreover, the DSDV has two ways when sending routing table updates. One is the "full-dump" updae type in which the full routing table is included inside the update. An incremental update, in contrast contains only those entries with metrics that have been changed since the last update was sent. Additionally, the incremental update fits in one packet.

b. OPTIMIZED LINK STATE ROUTING(OLSR) PROTOCOL

OLSR is developed for mobile ad hoc networks. It operates as a table-driven, proactive protocol, it exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). In OLSR only nodes selected as such MPRs are responsible for forwarding control traffic intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmission required. Nodes selected as MPRs also have a special responsibility when declaring link state information in the network. Indeed the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link state information for their MPR

selectors. Additional available link state information may be utilized for example for redundancy.

c. FISHEYE STATE ROUTING (FSR)

The Fisheye State Routing (FSR) [8] is a proactive unicast routing protocol based on link state routing algorithm with effectively reduced overhead to maintain network topology information.FSR is an implicit hierarchical routing protocol. It uses the "fisheye" technique proposed by kleinrock and Stevens where the technique was used to reduce the size of information required to represent graphical data. The eye of a fish captures with high detailthe pixels near the focal point. The detail decreases as the distance from the focal point increases. In routing, the fisheye approach translates to maintaining accurate distance and path quality information about the immediate neighborhood of a node with progressilvely less detail as the distance increases.

ii. REACTIVE ROUTING PROTOCOLS

In a reactive routing protocols, routing paths are searched only when needed. A route discovery operation invokes a route determination procedure. The discovery procedure terminates when either a route has been found or no rout is available after examination for all routes permutations. In a mobile ad hoc network, active routes may be disconnected due to node mobility. Therefore, route maintenance is an important operation of reactive routing protocols. Compared to the proactive routing protocols for mobile ad hoc network, less control overhead is a distinct advantage of the reactive routing protocols. Thus, reactive routing protocols have better scalability than proactive routing protocols in mobile ad hoc networks. However, when using reactive routing protocols,source nodes may suffer from long delays for route searching before they can forward data packets. Following are reactive network routing protocols:

a. AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. AODV is a novel algorithm for the operation of such ad hoc networks. Each mobile host operate as a specialized router and routes are obtained as needed. The AODV routing algorithm is quite suitable for a dynamic self-starting network as required by users wishing to utilize ad hoc networks. AODV provides loop-free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile mobile nodes is less than in those protocols that do necessitate such advertisements.

b. DYNAMIC SOURCE ROUTING (DSR) PROTOCOL

The DSR protocol is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring requiring no existing network infrastructure or administration. Network nodes cooperate to forward packets for each other to allow communication over multihops-between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network and as wireless transmission conditions such as sources of inference change, all routing is automatically determined and maintained ny the DSR routing protocol.

c. TEMPORALLY ORDERED ROUTING ALGORITHM (TORA)

TORA is a distributed routing protocol for mobile, multihop wireless networks. Its intended use is for the routing of IP datagrams within an autonomous system. The basic underlying algorithm is neither a distance vector nor a state link, it is one of algorithm called ad "link-reversal" algorithms. The protocol's reaction is structured as a temporally ordered sequence of diffusing computations each computation consisting of a sequenced of directed link reversals. The protocol is highly adaptive, efficient, scalable and is well suited for use in large,dense,mobile networks.

d. CLUSTER-BASED ROUTING PROTOCOL (CBRP)

CBRP is a routing protocol designed for use in mobile ad hoc networks. The protocol divides the nodes of the ad hoc network into a number of overlapping or dis-joint two hop diameter clusters in distributed manner. A cluster head is elected for each cluster to maintain cluster membership information. CBRP has the following features:

- Fully distributed operation.
- Less flooding traffic during the dynamic route discovery process.
- Explicit exploitation of unidirectional links that would otherwise be unused.
- Broken routes could be repaired locally without re discovery.
- Suboptimal routes could be shortened as they are used.

iii. HYBRID ROUTING PROTOCOLS

Hybrid routing protocols are a new generation of protocols which are both proactive and reactive in nature. These protocols are designed to increase scalability by allowindg nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.

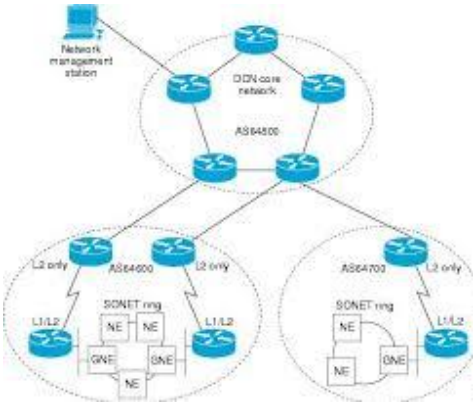


Fig2. Hybrid routing protocol[6]

This is achieved by proactively maintaining routes to nearby nodes and determining routes to faraway nodes using a route discovery strategy. Most hybrid protocols proposed to date are zone based which means that the network is partitioned or seen as a number of zones by each node. Others group nodes are formed into trees and clusters. Following are some hybrid routing ptocols:

a. ZONE ROUTING PROTOCOL(ZRP)

The ZRP protocol combines the advantages of the proactive and reactive approaches by maintaining an up-to-date topological map of a zone centered on each node. Within the zone, routes are immediately available. For destinations outside the zone, ZRP employs a route discovery procedure which can benefit from the local routing information of the zones.

b. ZONE-BASED HIERARCHICAL LINK STATE(ZHLS)

A point to point hierarchical routing protocol, zone based hierarchical LSR protocol (ZHLS) incorporates location information into a novel point to point hierarchical routing approach. The network is divided into no overlapping zones. Aggregating nodes into zones conceals the detail of the network topology. Initially, each node knows its own position and therefore zone ID through GPS. After the network established, each node knows the low level (node-level) topology about node connectivilty within its zone and the high-level (zone-level) topology about node connectivity of the whole network. A packet is forwarded by specifying the hierarchical address zone ID and node ID of a destination node in the packet header.

III. COMPARISON BETWEEN PROACTIVE,REACTIVE AND HYBRID PROTOCOLS

Table1. Comparison between proactive,reactive and hybrid protocols

SR.NO.	PROACTIVE	REACTIVE	HYBRID
TYPE	Peridically maintains routes between every mobile node pair	Routes not maintained.	Network divided in small zones.
ROUTES	Predefined routes are available	No pre-defined route. Routes maintained only if data to transmit	• Reactive inter-region routing • Intra-region proactive routing
LATENCY	Low latency	High latency.	Latency higher than proactive.
SCALABILITY	Low scalability	High scalabilty	Medum scalability
EXAMPLE	DSDV	AODV	ZRP
ROUTING STRUCTURE	Both flat and hierarchical	Mostly flat,except CBR	Mostly hierarchical
STORAGE REQU	High	Usually lower than proactive	Usually depend upon the size of each cluster

IREMENT		protocols	
TRAFFIC CONTOL VOLUME	Usually high	Low	Mostly lower than proactive and rective
MOBILITY HANDOVER EFFECT	Usually updates occur based on mobility at fixed interval	AODV uses local route discovery	Usually more than one path may be available
SCALABILITY LEVEL TO PERFORM EFFICIENT ROUTING	Usually upto 100 nodes	Source routing protocols upto few 100 nodes point-to-point may scale higher	Designed for uoto 1000 or more nodes

IV. ADVANTAGES AND DISADVANTAGES OF PROACTIVE,REACTIVE AND HYBRID ROUTING PROTOCOLS

Table2. Advantages and disadvantages of proactive, reactive and hybrid routing protocols

	ADVANTAGES	DISADVANTAGE
PROACTIVE	• Up-to-date routing information • Quick establishment of routes • Small delay • A route to every other node in the network is always available	• Slow convergence • Tendency of creating loops • Large amount of resources are needed • Routing information is not fully used
REACTIVE	• Reduction of routing load • Saving of resources • Loop-free	• Not always up-to-date routes • Large delay • Control traffic and overhead cost
HYBRID	• Scalability • Limited search cost • Up-to-date routing information within zones	• Arbitrary proactive scheme within zones • Inter-zone routing latencies • More resources for large size zones

V. CONCLUSION

In this paper, the classifications of routing protocols for ad hoc wireless networks were discussed. In proactive protocols, each node maintains network connectivity and up-to-date routing information to all the nodes in the network. In reactive protocols, a node finds the route to a destination when it desires to send packets to the destination. In hybrid routing protocols, some of the characteristics of proactive and some of the characteristics of reactive are combined, by maintaining intra-zone information proactively and inter-zone information reactively, into one to get better solution for mobile ad hoc networks.

Generally speaking, reactive protocols require fewer amounts of memory, processing power, and energy than that of the proactive protocols. The mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid

protocols often possess the advantages of both types of protocols.

VI. REFRENCES

[1] C. K. Tok, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Pearson Education, Boston, 2002, pp. 28-30.

[2] Kuncha Sahadevaiah1, Oruganti Bala Venkata Ramanaiah,Department of Computer Science & Engineering, University College of Engineering, Jawaharlal Nehru Technological University, Kakinada, India ,Department of Computer Science & Engineering, University College of Engineering, Jawaharlal Nehru Technological University, Hyderabad, India, Int. J. Communications, Network and System Sciences, 2010, 3, 511-522 doi:10.4236/ijcns.2010.36069 Published Online June 2010 (http://www.SciRP.org/journal/ijcns/).

[3] C. S. R. Murthy and B. S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," Pearson Education, Boston, 2006.

[4] P. Mohaptra and S. V. Krishnamurthy, "Ad Hoc Networks: Technologies and Protocols," Springer International Edition, New Delhi, 2005.

[5] F. Anjum and P. Mouchtaris, "Security for Wireless Ad hoc Networks," John Wiley & Sons, Chichester, 2007.

[6]{https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=&url=http%3A%2F%2Fwww.elitha-eri.net%2F2009%2F11%2F25%2Fhybrid-routing-protocol%2F&ei=hZZVO74I9iQuASC7oGAAg&bvm=bv.78677474,d.c2E&psig=AFQjCNGbK9xFDPpDgvhwETaDNyddmDfvPQ&ust=1415211130727911}

[7]https://www.google.co.in/search?q=reactive+routing+protocol&es_sm=93&source=lnms&tbm=isch&sa=X&ei=lxZZVN_rBcOMuAT2x4CYAg&ved=0CAgQ_AUoAQ#tbm=isch&q=adhoc+network&facrc=&imgdii=_&imgrc=JRPbtiYj2BYBkM%253A%3BRt_a6fw1_DGdMM%3Bhttp%253A%252F%252Fimg.photobucket.com%252Falbums%252Fv92%252Fsemanticoverload%252Fadhoc%252520wireless%252FAdhocWirelesssetup.jpg%3Bhttp%253A%252F%252Fwww.semanticoverload.com%252F2007%252F10%252F25%252Fhome-wireless-network-without-a-router%252F%3B960%3B720

[8] M. Gerla, X. Hong and G. Pei, "Fisheye State Routing (FSR) Protocol for Ad Hoc Networks," 2002. http://tools. ietf.org/html/draft-ietf-manet-fsr-03

Resource Allocation Models for QoS in Mobile Adhoc Networks: A Review

Sachin Khurana
Department of Computer Applications
Amritsar College of Engineering & Technology
Amritsar, INDIA
sachin331@gmail.com

Dr. Vijay Kumar Banga
Principal
Amritsar College of Engineering & Technology
Amritsar, INDIA
vijaykumarbanga@gmail.com

Abstract: In this paper we focused on supporting resource allocation for improving quality of service (QoS) in the network (routing) layer. Resource allocation is one of the important methodologies that can improve Quality of Service (QoS) for ad hoc networks. In this paper we have analyzed the different resource allocation approaches based on differential services. In **this paper we discuss various Resource allocation models for quality of service like Deficit Round Robin Method, Stochastic Fairness Queue model; Relative Bandwidth based flow control, Group of Picture (GOP) level based transmission and Weighted Fair Queue Model. These models work on the basis of bandwidth and transmission time.**

Keywords: MANETs, clustering, QOS, Resource allocation Models.

I. INTRODUCTION

Mobile Ad hoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected [15]. MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. MANET technology allows a set of mobile uses equipped with radio interfaces (Mobile nodes) to discover each other and dynamically form a communication network. MANET incorporates routing functionality into mobile nodes so that they become capable of forwarding packets on behalf of other nodes and thus effectively become the infrastructure. Providing multiple routing paths between any source-destination pair of nodes has proved to be very useful in the context of wired networks [20]. They are opening up to various applications of Quality of service, Such as delay, throughput, packet loss and network lifetime. The mobility of nodes and the error prone nature of the wireless medium pose many challenges, including frequent route changes and packet losses, in the way of meeting the requirements of QoS. Such Challenges increases packet delay, decreases throughput and reduce network failure. The network performance degradation gets worse as traffic load increases. Despite there are large amount of effort invested in routing protocols, improving TCP performance and medium access control (MAC) for MANET.

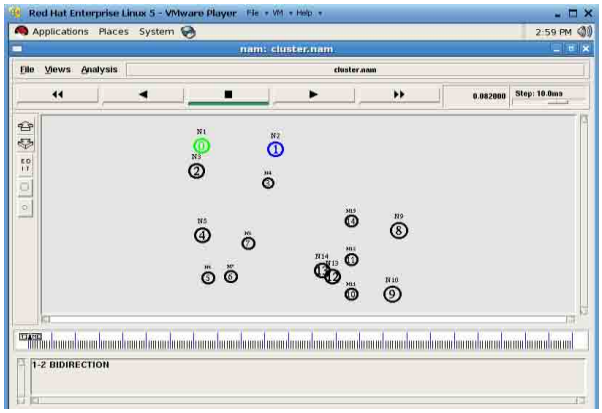


Figure 1: Typical Mobile ad-hoc network Diagram

Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment [13]. Intelligent vehicular ad hoc networks (In VANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc. Internet Based Mobile Ad hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such

type of networks normal ad hoc routing algorithms don't apply directly [14] [15].

Mobile Adhoc networks provide multiple routing paths between source to destination for the transmission of packets. It also provides shortest path and adaptive routing. Mobile Adhoc Networks used in various practical applications such as military applications, emergency operations and wireless sensor networks

II. CLUSTERING

Clustering is the process of building hierarchies among nodes in the network. In this approach an ad hoc network is partitioned into group of nodes called as clusters. The MANET can be divided into several clusters. Each cluster is composed of one clusterhead and many normal nodes, and all the clusterhead form an entire dominating set. The clusterhead is in charge of collecting information (signaling, message, etc.) and allocating resources within its cluster and communicating with other clusterheads. And the normal nodes communicate with each other through their clusterhead, no matter they are in the same cluster or not. The cluster architecture in MANET with a large number of mobile terminals ensures efficient performance. The cluster structure provides a certain amount of benefits, some of which are mentioned below:

Aggregation of Topology Information

With clustering in place each node is only required to store a small portion of the entire network routing information. As the number of nodes of a cluster is less than the number of nodes of the whole network, the clustering process assists in aggregating topology information. [12].

Efficiency and Stability

The important quality of a cluster structure is that it causes a MANET to seem smaller and more stable in the aspect of mobile terminals. When a mobile node switches its attaching cluster, only mobile nodes residing in the corresponding clusters are required to modify their data structures [13][14].

Communication Coordination

The process of clustering limits the inter-cluster interactions to clusterheads and also avoids unnecessary exchange of messages amongst the mobile nodes and thus also conserves communication bandwidth.

Routing Efficiency

Flat architecture of MANET supports every node to bear equal responsibility to act as a router for routing the packets to every other node. A great amount of message flooding takes place in order to obtain better routing efficiency. In return, such message flooding reduces the MAC layer efficiency to a certain extent. Cluster structure can be one possible solution to improve MAC layer efficiency and makes the routing process easier [15].

1) Spatial Reuse of Resources

A cluster increases the system capacity; by the way that the information is stored once on the clusterhead, which facilitates the spatial reuse of resources. Two clusters can distribute a similar frequency or code set if they are not adjoining clusters, this can be facilitated with the non-overlapping multi-cluster structure. Likewise, there can be a better coordination by a clusterhead of its transmission with the assistance of a specialized mobile node residing in it. This change in the existing system can save much of the resources, which are used for retransmission resulting from decreased transmission collision [16].

III. LITERATURE SURVEY

In this survey, we focused on supporting resource allocation for improving quality of service (QoS) in the network (routing) layer. To support QoS in Ad Hoc Networks, the link state information such as delay, bandwidth, cost, loss rate, and error rate in the network should be available and manageable. However, collecting, updating, and managing the link state information in Ad Hoc Networks are hard tasks because a wireless link is opting to change with the surrounding circumstances. Furthermore, the resource limitations and the mobility of nodes make things much more complicated. The challenge of resource allocation for supporting QoS in Ad Hoc Networks is to implement complex QoS functionality with limited available resources in a dynamic environment [10]. The network attempts to deliver all traffic as soon as possible within the limits of its abilities, but without guarantees related to throughput, delay or packet loss. It is left up to the end systems to cope with network transport impairments. Although best effort will remain adequate for most applications, QoS support is required to satisfy the growing need for multimedia over IP, like video streaming or IP telephony. QoS is usually defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination. The network needs are governed by the service requirements of end user applications. The network is expected to guarantee a set of measurable pre specified service attributes to the users in terms of end-to-end performance, such as delay, bandwidth, probability of packet loss, delay variance (jitter), packet delivery rate etc. Power

consumption is another QoS attribute which is more specific to Ad Hoc Networks. For the transmission of non-real time data, timing is not a critical issue, the data is elastic. As a result, the non-real time network could work well without guarantee of timely delivery of data. But it always has high requirement for packet loss. Retransmissions are used if there are some lost packets. The applications of non real time data transmissions are Telnet, FTP, E-mail and web browsing. For real time transmission like telephone, video conference, streaming video and audio, the basic requirement is to transmit packets to the destination on time. People cannot tolerate large delay for example on the phone. As a result, some QoS mechanisms are badly needed to ensure the required quality of the connection. QoS parameters differ from application to application. For example, in case of multimedia applications, bandwidth, delay jitter, and delay are the key QoS parameters, whereas military applications have stringent security requirements. For applications such as emergency search and rescue operations, availability of network is the key QoS parameter. Applications such as group communication in a conference hall require that the transmissions among nodes consume as minimum energy as possible. Hence battery life is the key QoS parameter here unlike traditional wired networks, where the QoS parameters are mainly characterized by the requirements of multimedia traffic, in ad hoc wireless, the QoS requirements are more influenced by the resource constraints of the nodes. Thus, resource allocation is to be carried out efficiently and with less complex operations. This can be done by using differential process of transmission in networks. Differential process actually divided the traffic into set of various classes and then allocates resource depending upon particular set of pre-defined parameters and also upon the availability of the resources. In general, it can be stated that resource allocation is actually combination of admission control and congestion control algorithms. This can be further, optimized by reducing complexity of application of these models and algorithms. Resource allocation is one of the important methodologies that can improve Quality of Service (QoS) for ad hoc networks. Resource allocation means providing ad hoc network node with all the required resources in terms of battery, memory consumption and information required for maintain routing table. The resource allocation in networks can be based upon approaches shown in Fig.2.

A. *Differential Services*

Differentiated Service is a design pattern for services and software, in which the service varies automatically according to the identity of the consumer and/or the context in which the service is used. Sometimes known as ***Smart Service or Context-Aware Service (Chen et al.).*** Differential Service divides the network traffic into set of classes depending upon the type of application for which it is being transmitted also upon the nature of the traffic.

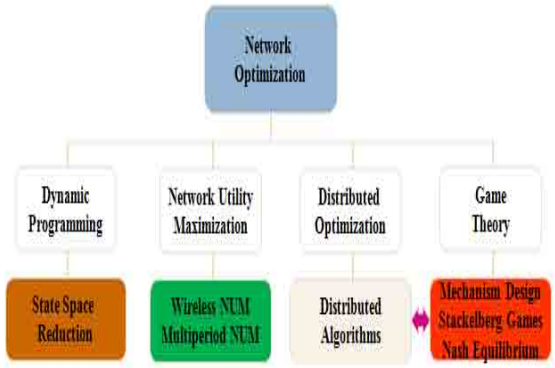


Fig. 2 Resource Allocation Approaches

B. *Classification of Differential Services*

Differential Services can be classified into two broad set depending upon the type of the network for which services are to be used.

- ***Absolute***
- ***Relative***

Absolute is used for static networks where mobility rate approaches to zero. It requires pre-reservation of resources. Relative is used for dynamic networks and it does not require and resource reservation for transmission process. It dynamically associates particular service to node. Also a relative differentiation mechanism that supports a small number of the service classes is simple in terms of implementation, deployment, and manageability.

C. *Resource Allocation Models for QoS*

For Improving QoS in MANETs, various resource allocation models have been proposed. These models work on principle of one to one n ode management policy and thus, ensure that QoS should not be limited to intermediate or the relaying node, rather it should be effectively provided to end user also. Some of resource

allocation models that have been surveyed are as follows:

- Deficit Round Robin Method [1]
- Stochastic Fairness Queue Model [2]
- Relative Bandwidth based flow control [3]
- Group of Picture (GOP) level based transmission [4]
- Weighted Fair Queue Model [5]

Deficit Round Robin Model

Deficit Round Robin *(Mclaughlin et al.)* is extension to round robin model for resource allocation. It is better than the round robin in terms of bandwidth reservation, though it pre reserves it. It uses deficit counter for managing resources among various routing units in network. As it is counter based approach, it uses more memory thus, can be used for network with small size and lesser number of nodes. It preserves the resources and takes more bandwidth. This produces longer delays and thus, cannot be deployed for large and highly dynamic networks. It assigned weight to judge the priority of the queue but transferred depending upon availability of bandwidth regardless to weight if queue. Thus, real time applications could not be handled using this model.

Stochastic Fairness Queue Model

Stochastic Fairness Queue *(Shreedhar et al.)* is resource allocation model that provides QoS by classifying the packets on basis of destination address in the packet header. It uses queue as data structure for maintain proper flow of data. It uses hash function to map incoming packets to available queue. This model stored different flow packets in the same queue regardless of their importance or priority. Hash function uses a timely counter to manage different hash generation for different set of packets. The model was relatively slow in terms of bandwidth allocation that results in jitters during transmission peak time. A separate drop queue has to be maintained for packets to be sequenced whenever a packet is dropped during forwarding process. Transmission of packets was based on principle of queue fill policy. The priority was assigned by the hash function to select between two similar queues.

Relative bandwidth based Flow Control Model

Relative Bandwidth based flow model *(Chen et al.)* is service profile model that maintains traffic profile for usage of bandwidth for maintain routing link between the nodes in ad hoc networks. This model requires dynamic adjustment of bandwidth as link capacity is not certain and may vary depending upon the mobility of the node and change in distance between relaying node. It maintains path on basis of common bandwidth requirement. This model maintains short term relationship between the arrived load and allocated service to particular class.

The major problem with this model was that it proves ambiguous and unrealistic, as service profiles are arbitrarily assigned into the queue. Also, it does not show how a target rate for a particular flow is arrived and passed to other nodes.

Group of Picture (GoP)-level based Transmission

GoP (*Pejman Goudarzi et al.)* model is based upon store and forward based method. Most of the search engines use this methodology for effective transmission and keeping information intact with demand of the network. The model was used for sending multimedia applications in limited size ad hoc networks. It divided the complete set of traffic into GoPs and then managed bit by bit transmission for each GoP (shown in Fig.).

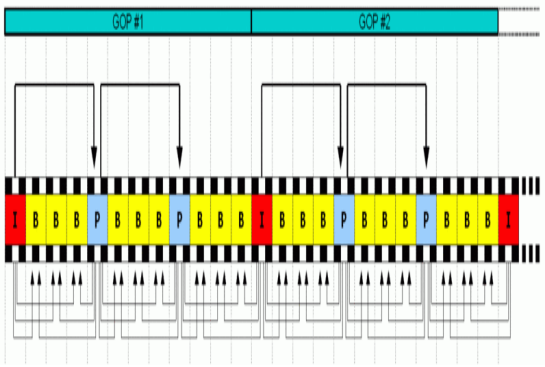


Fig 3. GoP for multimedia applications

Loss induced distortion for traffic associated with it is minimum. However, GoP is range based model and is applicable to only limited sized network. Its performance degrades as network size increases.

Weighted Fair Queue Model

Weighted Fair Queue *(Varaprasad et al.)* is used for avoiding congestions in network to provide better QoS to end users. The model classified the data into queue based upon following parameters:

- Source destination pair
- Ports
- Socket no
- Type of service value

It works as conservative model for providing QoS to end user. It uses priority based queuing method for providing QoS to end user. It assigned weight to queues in order of largest assigned to that queue which contained packet with larger priority and thus, transmitted in non-ascending order. The model needs to be combined with some admission

control algorithm that will decide the congestion policy. Also, it pre –reserves bandwidth for larger process, this decrease dynamicity of the network and bandwidth may be wasted if the process fails.

Comparative Analysis

Graph 1 (Bandwidth Vs Transmission Time)

IV. CONCLUSION AND DISCUSSION

In this paper we discuss various Resource allocation models for quality of service like Deficit Round Robin Method, Stochastic Fairness Queue model; Relative Bandwidth based flow control, Group of Picture (GOP) level based transmission and Weighted Fair Queue Model. These models work on the basis of bandwidth and transmission time. The deficit Round Robin Model used networks for same size and lesser number of nodes and the real time applications cannot be handled using this model. Stochastic Fairness queue model works on the basis of destination address, a separate drop queue has to be maintains for the transmission of packets. This model finds difficulty when queue size is almost same of different queues. Relative Bandwidth based flow control model works on the bandwidth for maintaining routing link between source and destination. The problem of this model was that it proved indistinct as out of reach profiles are assigned into the queue. GOP level based transmission model works on the transmission of picture from source to destination. It divides set of traffic into GOP and then transmits, but its performance decreases when the size of picture is increased. The Weighted Fair queue model works on the basis of source destination pair, Port number, socket number and the type of service values. It transfers data on the basis of weight. It pre-reserves the bandwidth for larger process, this decreases the dynamicity of network and the bandwidth may be wasted and process fails.

References

[1] L. Chen and W. B. Heinzelman, "QOS aware routing based on bandwidth estimation for mobile ad hoc networks," IEEE J. Select. Areas Commun., vol. 23, no. 3, pp. 561–572, 2005.

[2] K. McLaughlin, S. Sezer, H. Blume, X. Yang, F. Kupzog, and T. Noll, "A scalable packet sorting circuit for high-speed WFQ packet scheduling," IEEE Trans. VLSI Syst., vol. 16, no. 7, pp. 781–791, 2008.

[3] Sarakis, N. Moshopoulos, D. Loukatos, K. Marinis, P. Stathopoulos, and N. Mitrou, "A versatile timing unit for traffic shaping, policing and charging in packet-switched networks," Syst. Architecture: EUROMICRO J., vol. 54, no. 5, pp. 491–506, 2008.

[4] P. Goudarzi, "Minimum distortion video transmission over wireless adhoc networks," in 14th European Wireless Conference, 2008.

[5] P. Goudarzi, M. Hosseinpourr , "Quality of Service Model for Multimedia Applications in a Mobile Ad Hoc Network," Consumer Electronics, IEEE Transactions on , vol. 56, no. 4, pp. 2217-2225, 2010.

[6] G. Varaprasad, R.S.D. Wahidabanu , "Quality of Service Model for Multimedia Applications in a Mobile Ad Hoc Network," IEEE Potentials, vol. 30, no. 2, pp. 44-47, 2011.

[7] F. L. Jeng, M. C. Chen, and Y. Sun, "WF2Q-M: Worst-case fair weighted fair queueing with maximum rate control, computer networks," Proc. Int. J. Comput. Telecommun. Networking, vol. 51, no. 6, pp. 1403–1420, 2007

[8] Patil, Esfahanian, Yunhao Liu, Li Xiao, "Resource Allocation Using Multiple Edge-Sharing Multicast Trees," IEEE Transactions on Vehicular Technology , vol. 57, no. 5, pp. 3178 - 3186 , 2008.

[9] www.digitaltut.com /ccie-written/resource-models

[10] V.S. Anitha, Sebastian, "(k, r)-Dominating set-based, weighted and adaptive clustering algorithms for mobile ad hoc networks," Communications IET , vol. 5, no. 13, pp. 1836-1853, 2011.

[11] Chinara, S., & Rath, K. (2009). TACA: A Topology Adaptive Clustering Algorithm For Mobile Ad Hoc Network. The 2009 World Congress in Computer Science Computer Engineering and Applied Computing. Las Vegas, USA.

[12] El-Bazzal, Z., Kadoch, M., Agba, B., Gagnon, F., & Bennani, M. (2006). A Flexible Weight Based Clustering Algorithm in Mobile Ad hoc Networks. International Conference on Systems and Networks Communication (ICSNC'06), (pp. 50-56) .

[13] Mai, K., Shin, D., & Choo, H. (2009). Toward Stable Clustering In Mobile Ad Hoc Networks. Information Networking, 2009. ICOIN 2009. International Conference on, (pp. 308-310).

[14] Sucec, J., & Marsic, I. (2004). Hierarchical Routing Overhead in Mobile Ad Hoc Networks.IEEE Transactions on Mobile Computing , Volume: 3 Issue: 1, (pp. 46 – 56).

[15] Tolba, F., Magoni, D., & Lorenz, P. (2007). Connectivity, energy & mobility driven Weighted clustering algorithm. in proceedings of IEEE GLOBECOM 2007, (pp. 2786 – 2790).

[16 Fridman, S. Weber, C. Graff, D.E. Breen, K.R.Dandekar, M. Kam , "OMAN: A Mobile Ad Hoc Network Design System ," IEEE Transactions on Mobile Computing, vol. 11, no. 7, pp. 1179 - 1191, 2012.

Comparative Study of Various Routing Protocols in VANET

Ranjeet Kaur [1*], Dr. Tanupreet Singh Preet[2]
Assistant Professor in CSE Department, DAV University, Jalandhar, E-mail: er.ranjeetsandhu@gmail.com
Professor in CSE Department, ACET Amritsar, E-mail: tanupreet.singh@gmail.com

ABSTRACT
Vehicular Ad Hoc Network (VANET) is a sub class of mobile ad hoc networks. VANET provides wireless communication among vehicles and vehicle to road side equipment's. The communication between vehicles is used for safety, comfort and for entertainment as well. In this study we investigated about different ad hoc routing protocols for VANET. In this paper we review the existing routing protocols for VANETs and categorize them into a taxonomy based on key attributes such as network architecture, applications supported, routing strategies, forwarding strategies, mobility models and quality of service metrics. Protocols belonging to unicast, multicast, geocast and broadcast categories are discussed.
Keywords: VANET, Ad Hoc networks, GPSR, GSR, AODV, FSR.

1. INTRODUCTION

The increasing demand of wireless communication and the needs of new wireless devices have tend to research on self organizing, self healing networks without the interference of centralized or pre-established infrastructure/authority. The networks with the absence of any centralized or pre-established infrastructure are called Ad hoc networks. Ad hoc Networks are collection of self-governing mobile nodes [2]. Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks (MANETs). VANET is one of the influencing areas for the improvement of Intelligent Transportation System (ITS) in order to provide safety and comfort to the road users. VANET assists vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation through Vehicle to Vehicle communication e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. The basic target of VANET is to increase safety of road users and comfort of passengers. VANET is the wireless network in which communication takes place through wireless links mounted on each node. VANET is a special type of MANET, in which

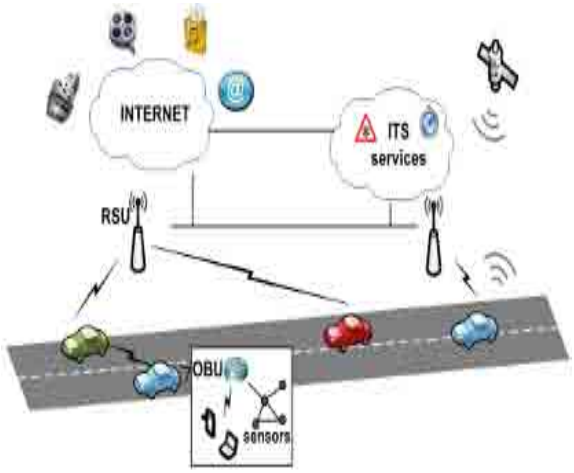


Fig. 1: Architecture of VANET

vehicles act as nodes. Unlike MANET, vehicles move on predefined roads, vehicles velocity depends on the speed signs and in addition these vehicles also have to follow traffic signs and traffic signals [6]. There are many challenges in VANET that are needed to be solved in order to provide reliable services. Stable & reliable routing in VANET is one of the major issues. Hence more research is needed to be conducted in order to make VANET more applicable. As vehicles have dynamic behavior, high speed and mobility that make routing even more challenging.

1.1 Architecture Categories of VANET: The various types of routing protocols have recently been proposed in MANET networks. They are classified as either proactive, reactive, or hybrid and same classification in VANET networks. The three categories of VANET protocols we discuss in below cellular, Ad-hoc, Hybrid.

1.1.1 Pure Ad-hoc Networks: The pure Ad-hoc network are use for emergencies environments where, in spite of nonexistent infrastructure. Nodes help each other in conveying information to and for creating the connections. Each node in Ad-hoc networks act like a router. In VANET environment, the communication between Vehicle-to-Vehicle (V2V) is a

pure Ad-hoc because of no infrastructure needed for communication between vehicles. Adhoc networks are self-organized networks and there is no need for infrastructure but range is limited.

1.1.2 Pure Cellular/WLAN Networks: In Cellular/WLAN category the network is a pure cellular and the access points are connect with internet and collect the information for analyzing. The system is use for Vehicle-to-Infrastructure (V2I) communication for provision of information [3].Cellular or Wireless Local Area Network based vehicular network are use for infotainment, web browsing, parking information. Cellular system still suffers from a main problem of fixed infrastructure deployment. LAN and DSRC are the most considered technologies in V2V and V2I communications.

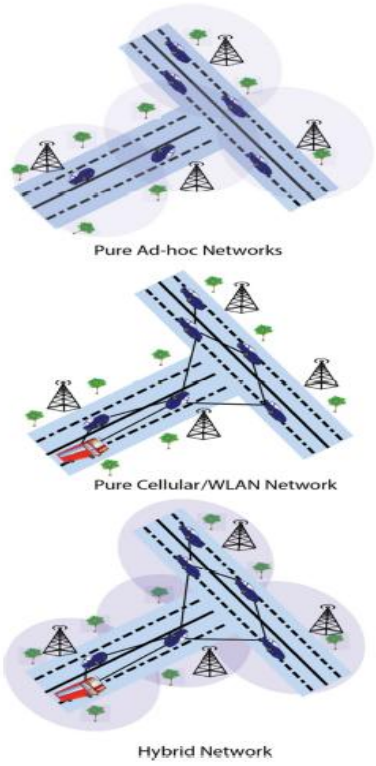


Fig 2: Three Architectures of VANET Pure Ad-hoc Networks, Pure Cellular /WLAN Networks, Hybrid Architecture

1.1.3 Hybrid Networks: The Combination of Cellular and Ad-hoc networks is hybrid networks and the architecture of hybrid network combine the Cellular and Ad-hoc network characteristics [6] . The hybrid network, which uses some vehicles with both WLAN and cellular capabilities as the gateway, and mobile network. Through multi-hop network the vehicles which are not WLAN capable communicate with others. VANETs contain of radio-enabled vehicles, which act as mobile nodes as well as routers for other nodes. Further, the similarities to ad hoc networks, such as short radio transmission range, self-organization and self-management, and low bandwidth, VANETs can be distinguished from other kinds of ad hoc networks.

2. VEHICULAR AD HOC NETWORK ROUTING:

History of VANET routing protocols starts from MANET protocols like Ad-hoc on Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR)[9]. Vehicular Ad-hoc networks nodes are a dynamic nature and challenging for finding and maintaining routes. In Vehicular Ad-hoc networks, different protocols were proposed for routing and they provides routing the different messages for different purposes. In Vehicular Ad-hoc networks there are different routing strategies have been defined based on architecture and need of applications or scenarios. In VANET, the routing protocols are categorized into five types: Topology, Position, broadcasting, Clustering, and Geo cast routing protocol. These protocols are characterized based on area / application where they are most suitable. The routing protocol of VANET can be classified into two categories such as Topology based routing protocols & Position based routing protocols. Topology based routing is further classified into Proactive and Reactive Protocols [1].

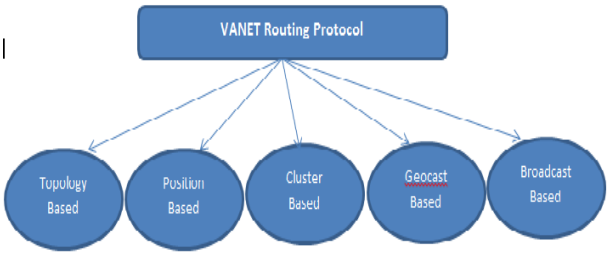


Fig 3: VANET Routing Protocols

2.1 Topology based routing protocols: The topology based routing protocols are divided into two categories:

2.1.1 Proactive Routing Protocols: Proactive protocols allow a network node to use the routing table to store routes information for all other nodes, each entry in the table contains the next hop node used in the path to the destination, regardless of whether the route is actually needed or not. The table must be updated frequently to reflect the network topology changes, and should be broadcast periodically to the neighbors. This scheme may cause more overhead especially in the high mobility network. However, routes to destinations

will always be available when needed. Proactive protocols usually depend on shortest path algorithms to determine which route will be chosen; they generally use two routing strategies: Link state strategy and distance vector strategy.

a) Destination Sequenced Distance Vector (DSDV): Destination Sequenced Distance Vector is a Proactive routing protocol that solves the major problem associated with the Distance Vector routing of wired networks i.e., Count to-infinity, by using Destination sequence numbers [6]. Destination sequence number is the sequence number as originally stamped by the destination. The DSDV protocol requires each mobile station to advertise, to each of its current neighbors, its own routing table (for instance, by broadcasting its entries).The entries in this list may change fairly dynamically over time, so the advertisement must be made often enough to ensure that every mobile node can almost always locate every other mobile node. In addition, each mobile node agrees to relay data packets to other nodes upon request. At all instants, the DSDV protocol guarantees loop free paths to each destination. Routes with more recent sequence numbers are always preferred as the basis for making forwarding decisions, but not necessarily advertised. Of the paths with the same sequence number, those with the smallest metric will be used. The routing updates are sent in two ways: a "full dump" or incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas, in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. The update can be time periodic or event periodic.

b) Optimized Link State Routing Protocol (OLSR): OLSR protocol implements the link state strategy; it keeps a routing table contains information about all possible routes to network nodes. Once the network topology is changed each node must send its updated information to some selective nodes, which retransmit this information to its other selective nodes. The nodes which are not in the selected list can just read and process the packet. Some researchers thought that OLSR has easy procedure which allows it to built-in different operating systems, besides it works well in the dynamic topology, also it is generally suitable for applications that required low latency in the data transmission (like warning applications). However, OLSR may cause network congestion; because of frequent control packets which sent to handle topology changes, moreover OLSR ignore the high resources capabilities of nodes (like transmission range, bandwidth, directional antenna and so on). Therefore, some researchers propose Hierarchical Optimized Link State Routing (HOLSR) protocol as enhancement of the OLSR protocol, which decreases routing control overhead in the large size networks, also maximizes the routing performance; by the defining network hierarchy architecture with multiple networks [7]. Also some researchers propose QOLSR as a solution of providing a path such that the available bandwidth at each node on the path is not less than the required bandwidth. QOLSR considers delay as a second for path selection .These protocols usually provide average enhancement for the QOS of packets. However, they cause more complexity, increasing packet overhead, and only suitable for some limited applications.

c) Fisheye State Routing (FSR): It is a proactive or table driven routing protocol where the information of every node collects from the neighboring nodes. Then calculate the routing table. It is based on the link state routing & an improvement of Global State Routing [4].FSR is similar to LSR, in FSR node maintains a topology table (TT) based upon the latest information received from neighboring and periodically exchange it with local neighbors. For large networks to reduce the size of message the FSR uses the different exchange period for different entries in routing tables. Routing table entries for a given destination are updated preferably with the neighbors having low frequency, as the distance to destination increases. The problem with the FSR routing is that with the increase in network size the routing table also increases. As the mobility increases route to remote destination become less accurate. If the target node lies out of scope of source node then route discovery fails [5].

2.1.2 Reactive (On Demand) Routing Protocols: Reactive routing protocols such as Dynamic Source Routing (DSR), and Ad hoc On-demand Distance Vector (AODV) routing implement route determination on a demand or need basis and maintain only the routes that are currently in use, thereby reducing the burden on the network when only a subset of available routes is in use at any time. Communication among vehicles will only use a very limited number of routes, and therefore reactive routing is particularly suitable for this application scenario.

a) Ad Hoc on Demand Distance Vector (AODV): In AODV routing, upon receipt of a broadcast query (RREQ), nodes record the address of the node sending the query in their routing table. This procedure of recording its previous hop is called backward learning. Upon arriving at the destination, a reply packet (RREP) is then sent through the complete path obtained from backward learning to the source. At each stop of the path, the node would record its previous hop, thus establishing the forward path from the source. The flooding of query and sending of reply establish a full duplex path. After the path has been established, it is maintained as long as the source uses it [1]. A link failure will be reported recursively to

the source and will in turn trigger another query-response procedure to find a new route.

b) Temporally Ordered Routing Algorithm (TORA): TORA belongs to the family of link reversal routing in which directed a cyclic graph is built which directs the flow of packets and ensures its reachability to all nodes. A node would construct the directed graph by broadcasting query packets. On receiving a query packet, if node has a downward link to destination it will broadcast a reply packet; otherwise it simply drops the packet. A node on receiving a reply packet will update its height only if the height of replied packet is minimum of other reply packets. The advantages of TORA is that the execution of the algorithm gives a route to all the nodes in the network and that it has reduced far reaching control messages to a set of neighboring nodes. However, because it provides a route to all the nodes in the network, maintenance of these routes can be overwhelmingly heavy, especially in highly dynamic VANETs [5].

c) Dynamic Source Routing (DSR): It uses source routing, that is, the source indicates in a data packet's the sequence of intermediate nodes on the routing path. In DSR, the query packet copies in its header the IDs of the intermediate nodes that it has traversed. The destination then retrieves the entire path from the query packet (source routing), and uses it to respond to the source. As a result, the source can establish a path to the destination. If we allow the destination to send multiple route replies, the source node may receive and store multiple routes from the destination. An alternative route can be used when some link in the current route breaks. In a network with low mobility, this is advantageous over AODV since the alternative route can be tried before DSR initiates another flood for route discovery. There are two major differences between AODV and DSR. The first is that in AODV data packets carry the destination address, whereas in DSR, data packets carry the full routing information. This means that DSR has potentially more routing overheads than AODV. Furthermore, as the network diameter increases, the amount of overhead in the data packet will continue to increase. The second difference is that in AODV, route reply packets carry the destination address and the sequence number, whereas, in DSR, route reply packets carry the address of each node along the route.

2.2 Position Based Routing: The dynamic and highly mobile nature of VANET, where nodes behave very rapid and changes its location frequently demands such routing method that can deal with the environment of such network. These demands tend the researchers to use positions of nodes in order to provide successful communication from source to destination. Such method in which geographical positions of nodes are used to perform data routing from source to destination is called position based routing.

a) Motion Vector Routing Algorithm (MOVE): MOVE algorithm is designed for light networks, especially for road side vehicle communication. This protocol assumes that each node has global locations information, that's beside the knowledge of a mobile router speed and its neighboring nodes velocity. From this information the node can estimate the nodes which are the closest distance to the destination. In this protocol each node regularly broadcasts a HELLO message; and its neighbor replays by a RESPONSE message; by this replayed message the node will know its neighbors and their locations. Given this information, the node can estimate the shortest distance to destination, in that case the node decides how to forward the message according to the information about nodes which are currently located nearby the destination. MOVE protocol uses less memory size compared with Non DTN position based routing; it also has a higher data transmission rate in light environments [2]. However, Non DTN position-based routing could have better performance only if the routes are stable and consistent.

b) Greedy Perimeter Stateless Routing (GPSR): Greedy Perimeter Stateless Routing (GPSR) [7] is one of the best examples of position based routing. GPSR uses closest neighbor's information of destination in order to forward packet. This method is also known as greedy forwarding. In GPSR each node has knowledge of its current physical position and also the neighboring nodes. The knowledge about node positions provides better routing and also provides knowledge about the destination. On the other hand neighboring nodes also assists to make forwarding decisions more correctly without the interference of topology information. All information about nodes position gathered through GPS devices. GPSR protocol normally devised in to two groups: Greedy forwarding: This is used to send data to the closest nodes to destination. Perimeter forwarding: This is used to such regions where there is no closer node to destination [7]. In other words we can say it is used where greedy forwarding fails.

c) Anchor-based Street and Traffic Aware Routing (A-STAR): Anchor-based Street and Traffic Aware Routing (A-STAR) is position based routing protocol. The development of A-STAR was inconsideration with city environment. In city area, almost all roads and streets are covered by big buildings and there are close ends in the streets and so frequent stop signal, turns and speed breakers make routing more challenging. Problems faced by the position based routing protocols in city environment defined before in GSR. The capability of A-STAR protocol to overcome these problems will be defined here. A-STAR is anchor based routing protocol. In anchor based routing before transmitting the

packet, source node address add in the header of packet and information of all intermediate node junction that packet must travel to reach the destination [3]. To use city maps and road information of town to make routing decisions called "Spatial Aware Routing". Spatial awareness is used to get topology information and different nodes position in the network. Mostly anchor based routing and spatial aware routing used together.

d) Geographic Source Routing (GSR): Due to deficiencies of GPSR in presence of radio obstacles, network demanded new routing strategies that can compete with challenges occurred due to radio obstacles. Therefore, Geographic Source Routing (GSR) is proposed [8]. It deals with high mobility of nodes on one hand, on the other hand it uses roads layout to discover routes. GSR finds the destination node using "Reactive Location Service (RLS)". GSR combines both geographic routing and road topology knowledge to ensure promising routing in the presence of radio obstacles [8]. In city area there are buildings and tress etc that may create problems in direct communication among nodes. Hence, previously proposed protocol GPSR for highways may not perform well in city environment.

3. Cluster Based Routing: Cluster based routing is preferred in clusters. A group of nodes identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Good scalability can be provided for large networks but network delays and overhead are incurred when forming clusters in highly mobile VANET. In cluster based routing virtual network infrastructure must be created through the clustering of nodes in order to provide scalability. The various Clusters based routing protocols are COIN and LORA_CBF.

4. Broadcast Routing: Broadcast routing is frequently used in VANET for sharing, traffic, weather and emergency, road conditions among vehicles and delivering advertisements and announcements. The various Broadcast routing protocols are BROADCOMM, UMB, V-TRADE, and DV-CAST.

5. Geo Cast Routing: Geo cast routing is basically a location based multicast routing. Its objective is to deliver the packet from source node to all other nodes within a specified geographical region (Zone of Relevance ZOR). In Geo cast routing vehicles outside the ZOR are not alerted to avoid unnecessary hasty reaction. Geo cast is considered as a multicast service within a specific geographic region. It normally defines a forwarding zone where it directs the flooding of packets in order to reduce message overhead and network congestion caused by simply flooding packets everywhere. In the destination zone, unicast routing can be used to forward the packet. One pitfall of Geo cast is network partitioning and also unfavorable neighbors, which may hinder the proper forwarding of messages. The various Geo cast routing protocols are IVG, DG-CASTOR and DRG

Table1: Difference between Topology-based and Position-based Routing Protocols

VANET Routing Protocols	Topology Based Routing Protocols	Position Based Routing Protocols
Methodology	• Use shortest path algorithm • Packet forwarding is done based on link information stored in routing table.	• Position determining service is used • Vehicle position is required to forward data packets.
Benefits/Strength	• Route discovery is required to search best possible shortest route between source node and destination node. • Beaconless. • Suitable for unicast, multicast and broadcast routing.	• Route discovery and maintaining protocol routes is not required. • Beaconing • Support high mobile environment.
Limitations	• Use more overhead. • Route discovery and delay constraint maintenance. • Failure in discovering complete path due to frequent network changes.	• Give least overhead. • Position finding services. • Deadlock may occur in location server.
Usage	• Basically proposed for MANETs. • Give less overhead and suitable for small networks.	• Suitable for large networks such as VANETs. • Research is in progress for control congestion and small networks.

CONCLUSION:

In this paper we discussed various routing approaches used in VANET. Routing is one of the most important parameter in inter-vehicle communication (IVC) and vehicles to infrastructure communications (V2I). VANET suffers from several internal and external factors of its dynamic nature. Internal factors include dynamic and highly movement of mobile nodes, frequent changes in network topology etc. External factors include impact of outside environment on network such as roads layout in city and interference of obstacles such as building, railway crossing etc. To overcome these internal and external issues several routing approaches have been proposed. Position based routing uses the physical position/location of nodes to make routing decisions in VANET. Position based routing assumes that each node in network is aware of its physical location with help of GPS. Thus position based routing contain many different protocols in order to provide successful communication in a highly dynamic network. We discussed three types of networks in VANET, Ad-hoc Networks, Pure Cellular /WLAN Networks and Hybrid Architecture. Through this study we have represented about the open issues and challenges involved in various VANET protocols. We hope that this paper will be an instrument for the students and researchers to address the challenges involved in VANET protocols.

REFERENCES:

[1] Garg, N., K. Aswal, and D.C. Dobhal, "A *review of Routing Protocols Inmobile Ad hoc Networks."* International Journal of Information Technology, 2012. **5**(1): p. 177-180.

[2] Marwane, A., et al. *HHLS: "A Hybrid Routing Technique for VANETs."* in *IEEE Global Communications Conference, IEEE GLOBECOM'12*. 2012.

[3] Park, S. and S.-M. Yoo, "*An efficient reliable one-hop broadcast in mobile ad hoc networks"*. Ad Hoc Networks, 2013. **11**(1): p. 19-28.

[4] Bilal, S.M., C.J. Bernardos, and C. Guerrero, *"Position Based Routing in Vehicular Networks: A Survey"*. Journal of Network and Computer Applications, 2012.

[5] W. Sun, et al., *"GVGrid: A QoS routing protocol for vehicular ad hoc networks,"* in Proc. 14th IEEE Int. Workshop on Quality of Service, 2006, pp. 130-139.

[6] S.-H. Cha, K.-W. Lee and H.-S. Cho, *"Predictive Grid-Based Predictive Geographical Routing for Inter-Vehicle Communication in Urban Areas,"* Hindawi International Journal of Distributed Sensor Networks, Vol. 2012, Mar. 2012.

[7] Ram Shringar Raw, Sanjoy Das, *"Performance Comparison of Position-based Routing Protocols in Vehicle-to-Vehicle (V2V) Communication,"* in IJEST, Jan 2011.

[8] Yun-Wei Lin et al, *"Routing Protocols in Vehicular ad hoc networks: A survey and future perspectives"*, Journal of information Science and engineering, 2010, pp.913-932.

VARIOUS ROUTING PROTOCOLS IN MANET

Er.Sania Gupta
MTech CSE (Research Scholar)
Deptt. Of CSE
PTU Regional Centre
ACET, Amritsar
Saniagupta02@gmail.com

Dr. Tanupreet Singh
Professor and Head
Dept of ECE
A.C.E.T. Amritsar

ABSTRACT- Due to limited resources in MANETs, to design an efficient and reliable routing strategy is still a challenge. An intelligent routing strategy is required to efficiently use the limited resources. Routing in MANETs is a challenging task and has received a tremendous amount of attention from researchers around the world. To overcome this problem a number of routing protocols have been developed and the number is still increasing day by day. It is quite difficult to determine which protocols may perform well .In this paper we provide an overview of a wide range of the existing routing protocols with a particular Focus on their characteristics and functionality. Also, the Comparison has described which is based on the routing decisions. The performance of all the routing protocols is also discussed. Further this study will help the researchers to get an overview of the existing protocols and suggest which protocols may Perform better with respect to varying network scenarios.
Keywords—Mobile ad hoc networks, Routing Protocols Comparison.

I. Introduction

A Mobile ad hoc network is a group of wireless mobile Computers in which nodes collaborate by Forwarding packets for each other to allow them to create Communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or Fixed network infrastructure such as base stations or access Points. A MANET is an autonomous group of mobile users that communicates over reasonably slow wireless links. The Network topology may vary rapidly and unpredictably over time, because the nodes are mobile. Such a network may operate in a standalone fashion, or may be connected to the larger internet. MANETs possess certain characteristics like
Bandwidth-constrained, variable capacity links. Figure shows mobile ad-hoc network with 6 nodes

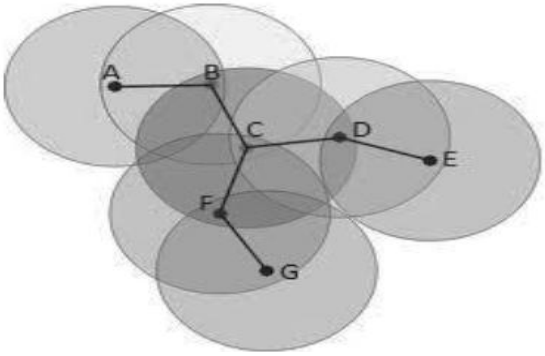


FIG1 MOBILE AD-HOC NETWORK

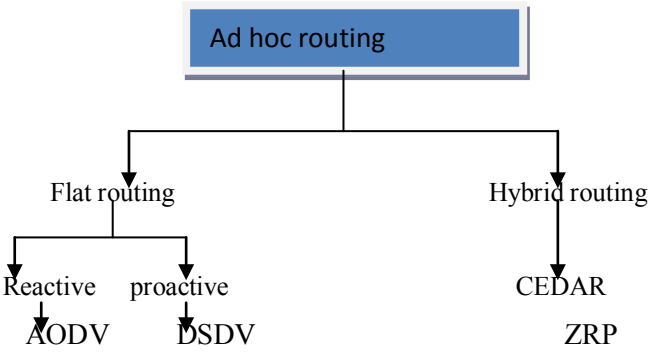
II. ROUTING IN MANETS

A Mobile Ad Hoc Network or spontaneous network is an Infrastructure less, self-organized network with rapidly changing topology causing the wireless links to be broken. A key issue is the necessity that the Routing Protocol must be able to respond rapidly to the topological changes in the network. In these networks, each node must be capable of acting as a router. As a result of limited bandwidth of nodes, the source and destination may have to communicate via intermediate nodes. Major problems in routing are Asymmetric links, Routing Overhead, Interference, and Dynamic Topology. Routing in MANETs has been an active area of research and in recent years numerous protocols have been introduced for addressing the problems of routing, reviewed in later sections. These protocols are divided into two broad classes which are reactive and proactive. In reactive the routes are created only when needed. The application of this protocol has shown in DSR(dynamic source routing protocol) and ad-hoc on demand distance routing protocol(AODV).
When Proactive the nodes keep Updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and Destination Sequenced Distance Vector Protocol (DSDV). All these protocols are quite insecure because attackers can easily take the information about the network

III.CLASSIFICATION OF ROUTING PROTOCOLS

We will now described the classification of existing wireless ad hoc routing protocols .The Routing Protocols for ad hoc wireless networks can be divided into three subtypes based on the routing information. They could be Reactive

(On-demand), Proactive (Table-driven) or Hybrid. Figure 2 shows the three subtypes of Ad hoc routing protocol.



CLASSIFICATION OF AD-HOC ROUTING PROTOCOL

This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol needs a route to a new destination, it will have to wait until such a route can be discovered. On the other hand, because routing information is continuously maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed .In this paper we have presented a critical analysis of the above mentioned secure routing protocols. the two broad classes of routing protocols based on their routing methodology and other network

IV. PROACTIVE PROTOCOLS

These protocols always maintain up-to-date information Of routes from each node to every other node in the network. These protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a Destination, such route information is available immediately. Different protocols have record of different routing state Information. These protocols needs each node to maintain one or more tables to store up to date routing information and to spread updates throughout the network. As such, these protocols are often also referred to as table-driven. These protocols try and maintain valid Routes to all communication mobile nodes all the time, which means before a route is actually needed. Periodic route updates are exchanged in order to synchronize the tables. Some examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) Optimized Link State Routing Protocol (OLSR) and Wireless Routing Protocol (WRP) .These protocols differ in the number of routing related tables and how changes are broadcasted in the network structure.

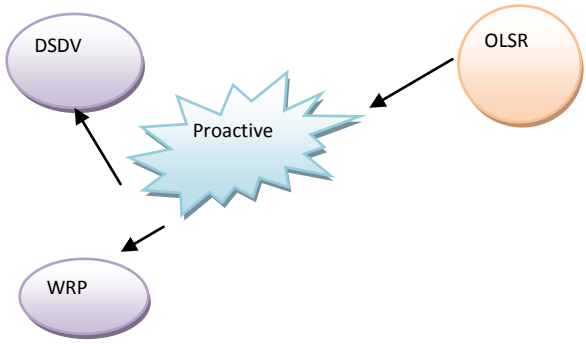


Fig. 3 Examples of table driven ad hoc routing protocols.

A. DSDV

DSDV is proposed by Perkins and Bhagwat. The Destination-Sequenced Distance-Vector (DSDV) Routing protocol is based on the idea of the classical Bellman-Ford Routing Algorithm with certain such improvements like making it loop-free. The distance vector routing is less robust than link state routing due to problems such as count to infinity and bouncing effect. In this, each device maintains a routing table containing entries for all the devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbour devices. When a neighbour device receives the broadcasted routing message and knows the current link cost to the device, it compares this value and the corresponding value stored in its routing table. If changes were found, it updates the value and re-computes the distance of the route which includes this link in the routing table

B. OLSR

Clausen and Jacquet proposed the Optimized Link State Protocol, a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying [16, 17]. It optimizes the pure link state routing protocol. Optimizations are done in two ways: by reducing the size of the control packets and by reducing the number of links used for forwarding the link state packets. Here each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. OLSR is based on the following threemechanisms: neighbor sensing, efficient flooding and computation of an optimal route using the shortest-pathalgorithm. Neighbour sensing is the detection of changes in the neighbourhood of node. Each node determines an optimal route to every known destination using this topology information and stores this information in a routing table. The shortest path algorithm is then applied for computing the optimal path. Routes to every destination are immediately available when data transmission begins and remain valid for a specific period of time till the information is expired updates, security patches etc. Though they are quite effective and eases

an organization effort since everything is already there, it does face some criticism, especially on security related issue.

C. WRP

The Wireless Routing Protocol, as proposed by Murthy and Garcia-Luna-Aceves [18], is a table-based protocol similar toDSDV that inherit the properties of Bellman-ford algorithm. The main goal is maintaining routing information among all nodes in the network regarding the shortest distance to every destination. Wireless routing protocols (WRP) is a loop free routing protocol. WRP is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbours. Each node in the network uses a set of four tables to maintain more accurate information: Distance table. (DT), Routing table (RT), Link-cost table (LCT), Message retransmission list (MRL) table. In case of link failure between two nodes, the nodes send update messages to their neighbours. WRP belongs to the class of path-finding algorithms with an important exception. It counters the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbours. This eliminates looping situations and enables faster route convergence when a link failure occurs.

D. STAR

The STAR protocol [19] is also based on the link state algorithm. Each router maintains asource tree, which is a set of links containing the preferred paths to destinations. This protocol has significantly reduced the amount of routing overhead disseminated into the network by using a least overhead routing approach (LORA), to exchange routing information. The optimum routing (ORA) approach obtains the shortest path to the destination while LORA minimizes the packet overhead. Garcia–Luna–Aceves and Spohn propose STAR where each node maintains a source tree which contains preferred links to all possible destinations. Nearby source trees exchange information to maintain up-to-date tables. The routes are maintained in a routing table containing entries for the destination node and the next hop neighbour. The link state update messages are used to update changes of the routes in the source trees. Since these packets do not time out, no periodic messages are required

.

E. FSR

Pei et al. propose the FSR protocol which takes inspiration from the ‘‘fisheye’’technique of graphic information compression proposedby Kleinrock and Stevens. When adapted to a routing table, this technique means that a node maintains accuracy distanceand path quality information about its immediate vicinity, but the amount of detail retained decreases with the distance from the node. Each node considers a number of surrounding fish-eye scopes, areas which can be reachedwith 1, 2 ... hops. FSR reduces the size of the update messages by updating the network information for nearby nodes at a higher frequency than for theremote nodes, which lie outside the fisheye scope. This makes FSR more scalable to large networks than the protocols.

Table 1 Comparison of Proactive Routing Protocol

Parameters	DSDV	WRP	OLSR
Route updates	Periodic	Periodic	Periodic
Loop free	Yes	Yes	Yes
Routing overhead	High	High	Low
Caching Overhead	Medium	High	High
Throughput	Low	Low	Medium

V. REACTIVE PROTOCOLS

The reactive or on-demand routing protocols are based on Query-Reply topology in which they do not attempt to continuously maintain the up-to-date topology of the network. When a route is desired, a procedure is invoked tofind a route to the destination node. The major goal of on demand or reactive routing protocols is to minimize the network traffic overhead. These routing protocols are basedon some type of "query-reply" dialog. They do not attemptto continuously maintain the up-to-date topology of the network. Rather, when the need arises, a reactive protocolinvokes a procedure to find a route to the destination; such aprocedure involves some sort of flooding the network withthe route query. As such, such protocols are often also referred to as on demand. The common element in reactive protocols is the mechanism used for discovering routes. Thesource node emits a request message, requesting a route tothe destination node. This message is flooded, i.e. relayedby all nodes in the network, until it reaches the destination.The path followed by the request message is recorded in themessage, and returned to the sender by the destination, or byintermediate nodes with sufficient topological information,in a reply message. Thus multiple reply messages mayresult, yielding multiple paths - of which the shortest is tobe used. Some examples of source initiated ad hoc routingprotocols include the Dynamic Source Routing Protocol(DSR) [22], Ad Hoc On-Demand Distance Vector RoutingProtocol (AODV) [23], and Temporally-Ordered Routing
Algorithm

A. AODV

AODV is a widely accepted on-demand routing protocolin ad hoc networks proposed by C. E. Perkins and E. M. Royer. Ad hoc On-demand Distance Vector (AODV) is a combination of both DSR and DSDV. It follows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing,sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop freedomat all times and by avoiding the Bellman-Ford “count-to infinity” problem offers quick convergence when the ad hocnetwork topology changes.

AODV finds routes only whenrequired and hence is reactive in nature. The major vulnerabilities present in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hopcount. Zapata [26] applies security extensions to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He introduced Secure- AODV (SAODV)where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation. AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or though ACK messages, the source and the destination nodes are notified (end nodes). The source node then reestablishes the route with the destination using higher layers. AODV does not provide any type of security.

B. TORA

The Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson. Temporarily ordered routing algorithm **(**TORA) is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes [28]. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. In comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks. TORA involves four major functions: creating, maintaining, erasing and optimizing routes. Since every node must have a height, any node which does not have a height is considered as an erased node and its height is considered as null. Sometimes the nodes are given new heights to improve the linking structure. This function is called optimization of routes.

C. DSR

DSR is an on-demand protocol designed by D. B. Johnson, Maltz and Broch to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. The distinguishing feature of Dynamic Source Routing (DSR) is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes then it uses that path to transmit the packet. Also it attaches its source address on the packet. If there is no entry in the cache or the entry is expired, the sender broadcasts a route request packet to all its neighbors asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If they have route information, they send back a route reply packet to the destination. Otherwise they broadcast the same route request packet. Once the route is discovered, the sender will send its required packets using the discovered route as well as insert an entry in the cache for future use. Also the node keeps the age information of the entry to recognize whether the cache is fresh or not. When any intermediate node receives a data packet, it first sees whether the packet is sent to itself or not. If it is the destination, it receives that else it forwards the packet using the path attached on the packet.

D. ARA

Gunes et al. present a novel technique for ad hoc routing by using concepts of swarm intelligence and the ant colonymeta-heuristic. This class of algorithms aims to solve thecomplex optimization and collaboration problems withoutdirect communication among the participants. Indirect communication is achieved by stigmergy, the process ofleaving traces in the environment, similar to the behaviorof ants leaving pheromone signals. Route discovery is done by flooding a forward ant to the destination, similarto Route Request in AODV. Duplicate packetsare identifiedby the use of a sequence number and are deleted bysystem.When a route is found to the destination, a backward ant iscreated similar to Route Reply in AODV. The backward ant follows the path with the shortest trip time detected by theforward ant. The amount of pheromone deposited by both ants is a function of route length associated with pheromone. The route maintenance phase is responsible for updating the routing information during the communication.The algorithm updates both the forward and the backwardpath with an equal amount of pheromone (presumed as 0.1).

ARA also allows for the evaporation of pheromones ARA achieves loop free paths using sequence numbers. If a Node receives a duplicate packet, it sets the DUPLICATE_ERROR flag and returns the packet to the Previous node, and removes the link. According to Gunes et al ARA performs comparatively better in terms of overhead ratio and delivery rate.

Parameters	AODV	DSR	TORA
Route Creation	By source	By source	Locally

Periodic updation	No	No	No
Performance Metrics	Speed	Shortness	Speed
Routing overhead	High	High	High
Caching overhead	Low	High	Medium
Throughput	High	Low	Low
Multipath	No	Yes	Yes
Route updation	Non-periodic	Non-periodic	High routing overhead

VI. HYBRID ROUTING PROTOCOLS

These protocols try to incorporate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; routing in general can be either flat or hierarchical. The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption. Some examples of Hybrid Routing Protocols include CEDAR, ZRP and SRP . In what follows, we present a few of the proposed routing protocols from each class developed for the ad hoc networks. The most important protocols and those which dominate recent literature are AODV, DSR, SRP, ZRP, DSDV and TORA.

A. ZRP

Haas and Pearlman proposed Zone Routing Protocol. ZRP is a hybrid routing protocol for mobile ad hoc networks which localizes the nodes into sub-networks (zones). It incorporates the merits of on-demand and proactive routing protocols. Within each zone, proactive routing is adapted to speed up communication among neighbours. The inter-zone communication uses on-demand routing to reduce unnecessary communication. The network is divided into routing zones according to distances between mobile nodes. Given a hop distance *d* and a node N, all nodes within hop distance at most *d* from N belong to the routing zone of N. Peripheral nodes of N are N's neighboring nodes in its routing zone which are exactly *d* hops away from N. An important issue of zone routing is to determine the size of the zone. An enhanced zone routing protocol, Independent Zone Routing (IZR), which allows adaptive and distributed reconfiguration of the optimized size of zone, is introduced in Furthermore, the adaptive nature of the IZR enhances the scalability of the ad hoc network. Every node periodically needs to update the routing information inside the zone. Additionally, some local route optimization is performed at each node, which includes the following actions: removal of redundant routes, shortening of routes, detecting of link failures.

B. ZHLS

ZHLS is based on hierarchical structure in which the network is divided into non-overlapping zones. According to Joa and Lu each node is assigned one unique node ID and a zone ID, which are calculated using geographical information. Hence the network follows a two-level topology structure: node level and zone level. Respectively, there are two types of link state updates: the node level LSP (Link State Packet) and the zone level LSP. A node level LSP contains the node IDs of its neighbors in the same zone and the zone IDs of all other zones. A node periodically broadcast its node level LSP to all other nodes in the same zone. Therefore, through periodic node level LSP exchanges, all nodes in a zone keep similar node level link state information. Before transmission, the source node first checks its intra-zone routing table. If the destination lies in its zone, the routing information is already present. Otherwise, the source sends a location request to all other zones through gateway nodes, which in turn replies with a location response containing the zone ID of the desired destination. The header of the data packets originated from the source contains the zone ID and the node ID of the destination node. ZHLS has a low routing overhead as compared to AODV and DSR. Also the routing path is adaptable to the dynamic topology as only node ID and zone ID are required for routing. So as long as the destination remains in the zone no further search is required.

C. CEDAR

Core Extraction Distributed Ad hoc Routing (CEDAR) proposed by Sivakumar, Sinha and Bharghavan is a partitioning protocol, integrates routing with QoS support. Each partition includes a core node called dominator node. A Dominator set (DS) of a graph is defined as a set of nodes in the graph such that every node is either present in DS or is a neighbor of some node present in DS. The core nodes use a reactive source routing protocol to outline a route from a source to a destination. CEDAR has three key phases:

1. The establishments and maintenance of self-organizing routing infrastructure (core) for performing route computations
2. The propagation of the link-states of high-bandwidth and stable links in the core
3. A QoS route computation algorithm that is executed at the core nodes using only locally available state. QoS routing in CEDAR is achieved by propagating the bandwidth availability information of stable links in the core sub-graph. To propagate the link information, slow moving increase-waves and fast moving decrease waves are used, which denotes increase of bandwidth and decrease of bandwidth respectively.

D. DDR

Nikaein et al. [44] propose a tree-based routing protocol without the need of a root node. In this strategy tree are constructedusing periodic beaconing messages, whichis exchanged by neighboring nodes only. These trees within the network form a forest withthe created gateway nodes acting as

links between the treesin the forest. These gateway nodes are regular nodesbelonging to separate trees but within transmission rangeof each other. A zone naming algorithm is used to assign aspecific zone ID to each tree within the network. Hence,the overall network now comprises of a number of overlappingzones The DDR algorithm comprise of the following sixphases: (i) preferred neighbor election;
(ii) intra-tree clustering;
(iii) inter-tree clustering;
(iv) forest construction;
(v) zone naming; and
(vi) zone partitioning.
To determine routes, hybrid ad hoc routing protocols (HARP) [45] is used. HARP uses the intra-zone and inter-zone routing tables created by DDR to determine a stable path between the source and the destination. The advantage of DDR is that unlike ZHLS, it does not rely on a static zone map to perform routing and it does not require a root node or a cluster-head to coordinate data and control packet transmission between different nodes and zones.

Table 3: COMPARISON BETWEEN THE THREE CATEGORIES OF ROUTING PROTOCOLS

Parameters	Proactive	Reactive	Hybrid
Storage Requirements	Higher	Dependent on no. of routes maintained or needed	Depends on size of each zone or cluster
Route Availability	Always Available	Computed as per need	Depends on location of destination
Periodic Route Updates	Required Always	Not Required	Used inside each zone
Delay	Low	High	Low for local destinations and high for Interzone
Scalability	100 nodes	> 100	> 1000
Control Traffic	high	low	Lower that other two types
Routing Information	Keep stored in table	Doesn't Store	Depends on requirement
Routing Philosophy	Mostly flat	Flat	Hierarchical

VIII. CONCLUSION

In this paper, we have presented and discussed the taxonomy of routing protocols in mobile ad hoc networks and provided comparisons between them. The protocols are divided into three main categories: (i) source initiated(reactive or on-demand), (ii) table-driven (pro-active), (iii) hybrid protocols. For each of these classes, we reviewed and compared several representative protocols. While there are still many challenges facing Mobile ad hoc networks related to routing and security. Each routing protocol has unique features. Based on network environments, we have to choose the suitable routing protocol. The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The main differentiating factor between the protocols is the ways of finding and maintaining the routes between source destination pairs. The comparison we have presented between the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. We hope that the taxonomy presented in this paper will be helpful and provide researchers a platform for choosing the right protocol for their work. At last we have provided the overall characteristic features of all routing protocols and described which protocols may perform best in large networks. Almost all the protocols we discussed in this paper have their own characteristic features and performance parameter combinations where they Out perform their competitors. Still mobile ad hoc networks have posed a great challenge for the researchers due to changing topology and security attacks, and none of the protocols is fully secured and research is going on around the globe.

REFERENCES

[1] A. K. Gupta and H. Sadawarti, "Secure Routing Techniques for MANETs," "*International Journal of Computer Theory and Engineering"*, vol. 1 no. 4, pp. 456-460, October 2009.
[2] C. E. Perkins, "*Ad hoc Networking*", Pearson Publication.
[3] P. G. Argyroudis and D. O'mahony, University Of Dublin, Trinity College, "*Secure Routing for Mobile Ad hoc Networks*".
[4] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, "*in Proceedings of ACM MOBICOM'02"*, 2002.
[5] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," "*EEE Network Magazine"* vol. 13, no.6, November/December 1999.
[6] A. K. Gupta, H. Sadawarti, and A. K. Verma, "A Review of Routing Protocols for Mobile Ad Hoc Networks," ""*SEAS Transactions on Communications"*, ISSN: 1109 2742, Issue 11 Vol.10, November 2011, pp. 331-340.
[7] P. Papadimitratos and Z. J. Haas. "Secure routing for mobile ad hoc networks," "*SCS Communication Networks and Distributed Systems Modeling and Simulation Conference* (CNDS 2002)", Jan 2002.
[8] M. Zapata, N. Asokan, "*Securing ad hoc routing protocols*", WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.
[9] E. M. Royer and Chai-Keong Toh, "*A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks*".
[10] N. S. Yadav and R.P. Yadav "Performance Comparison and Analysis of Table- Driven and On- Demand Routing Protocols for Mobile Adhoc Networks," "*International Journal of Information Technology"*,

Performance Analysis of TORA Protocol

Emanpreet kaur [1] , Abhinash Singla[2], Rupinder kaur [3]

[1] M.Tech (CSE) Student,Bhai Gurdas Institute of Engg. & Tech.,Sangrur.Punjab

[2] Assistant Professor (CSE), Bhai Gurdas Institute of Engg. & Tech.,Sangrur,Punjab, India,

[3] Assistant Professor (CSE), Bhai Gurdas Institute of Engg. & Tech.,Sangrur,Punjab, India,

[1]Sra_gagandeep@yahoo.co.in

[2]abhinash11@gmail.com

[3]Rupinder.walia84@gmail.com

***Abstract* – MANET is a collection of mobile nodes that communicate with each other over relatively bandwidth constrained wireless links . Network topology may change rapidly and erratically, so it can considerably affect packet routing in terms of network throughout, load and delay . In this we are presenting paper on performance comparison on tora routing protocol on MANET with varying network sizes and with increasing area and nodes sizes.this performance is measured by using "OPNET MODELLER 14.0" Simulator .the parameters taken for simulation is Throughput ,Network load and Delay .In the last conculsion is given for the performance of the TORA reactive protocol under varying network sizes .The final valuation is given at the end of this paper.**

Keywords- manet ,opnet, TORA ,simulation.

1.INTRODUCTION AND RELATED WORK

In the last couple of year, the use of wireless networks has become more and more familiar. A Mobile Ad-hoc Wireless Network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop network, maintaining connectivity in a decentralized manner[1]. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. Currently, the routing, power management, bandwidth management, radio interface, and security are hot topics in MANET research. The routing protocol is required whenever the source to transmit and delivers the packets to the destination. Many routing protocols have been proposed for mobile ad hoc network [2].

A. Proactive or table-driven routing protocols*:* In proactive protocols, each node maintains individual routing table containing routing information for every node in the network. Each node maintains consistent and current up-to-date routing information by sending control messages periodically between the nodes which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors. The drawback of proactive routing protocol is that all the nodes in the network always maintain an updated table. Some of the existing proactive routing protocols are DSDV and OLSR .

B. Reactive or On Demand Routing Protocol: In Reactive routing protocols, when a source wants to send packets to a destination, it invokes the route discovery mechanisms to find the route to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. Unlike table driven protocols, all nodes need not maintain up-to-date routing information. Some of the most used on demand routing protocols are DSR, TORA and AODV .

2. MANET ROUTING PROTOCOLS

There are several protocols proposed for wireless mobile ad-hoc networks. When we need to transfer the data from source to destination, we need a dedicated path or a route that is decided by various routing protocols. In this paper, we have used the TORA Routing Protocol

Temporally Ordered Routing Algorithm (TORA):

TORA is adaptive and scalable routing algorithm based on the concept of link reversal. It finds multiple routes from source to destination in a highly dynamic mobile networking environment. An important design concept of TORA is that control messages are localized to a small set of nodes nearby a topological change. Nodes maintain routing information about their immediate one-hop neighbors. The protocol has three basic functions: route creation, route maintenance, and route erasure . Nodes use a "height" metric to establish a directed cyclic graph (DAG) rooted at the destination during the route creation and route maintenance phases. The link can be either an upstream or downstream based on the relative height metric of the adjacent nodes. TORA's metric contains five elements: the unique node ID, logical time of a link failure, the unique ID of a node that defined the new reference level, a reflection indicator bit, and a propagation ordering parameter. Establishment of DAG resembles the query/reply process discussed in Lightweight Mobile Routing (LMR). Route maintenance is necessary when any of the links in DAG is broken. Figure 2. Denotes the control flow for the route maintenance in TORA . The main strength of the protocol is the way it handles the link failures. TORA's reaction to link failures is optimistic that it will reverse the links to re-position the DAG for searching an alternate path. Effectively, each link reversal sequence searches for alternative routes to the destination. This search mechanism generally requires a single-pass of the distributed algorithm since the routing tables are modified simultaneously during the outward phase of the search mechanism. Other routing algorithms such as LMR use two-pass whereas both DSR and AODV use three pass procedure. TORA achieves its single-pass procedure with the assumption that all the nodes have synchronized clocks (via GPS) to create a temporal order of topological change of events. The "height" metric is dependent on the logical time of a link failure [2, 3,8].

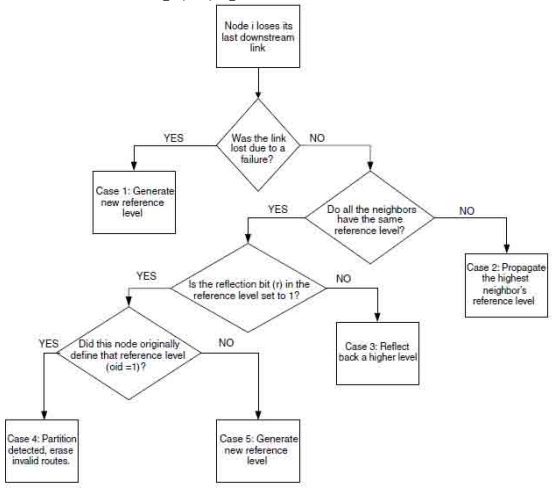


Fig 1. FLOW DIAGRAM OF ROUTE MAINTENANCE IN TORA

Advantages and Limitations :

The advantage of TORA is that the multiple routes are supported by this protocol between the source and destination node. Therefore, failure or removal of any of the nodes is quickly resolved without source intervention by switching to an alternate route to improve congestion. It does not require a periodic update, consequently communication overhead and bandwidth utilization is minimized. It provides the support of link status sensing and neighbor delivery, reliable in-order control packet delivery and security authentication. Also TORA consist some of the limitations like which depends on synchronized clocks among nodes in the ad hoc network. The dependence of this protocol on intermediate lower layers for certain functionality presumes that the link status sensing, neighbor discovery, in order packet delivery and address resolution are all readily available. The solution is to run the Internet MANET Encapsulation Protocol at the layer immediately below TORA. This will make the overhead for this protocol difficult to separate from that imposed by the lower layer.[3]

3. *SIMULATION PARAMETERS*

To analyse the performance of TORA OPNET 14.0 simulator is used. Scenario is created with 30 and 10 number of mobile nodes. Simulation parameters used for the implementation of TORA are listed in the Table 1.

Simulation Parameter	**Value**
Number of Nodes	**30 and 10**
Simulation Time	**300 sec**
Simulation Area (30 and 10 nodes)	**10 km *10 km**
Routing Protocols	**TORA**
Data Rate	**11mbps**
Application Name	**FTP (High load)**
Buffer size	**1024000**

Simulator	Opnet Modeller 14.0

4.*PERFORMANCE PARAMETERS* :
The following performance parameters are used to analyze the simulated result:-

Throughput [4]: Throughput is defined as the ratio of the total data reaches a receiver from the sender. The time consumed by the receiver to receive the last packet is called throughput. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).
Delay- The packet end-to-end delay is the average time of the packet passing through the network. It includes over all delay of the network like transmission time delay which occurs due to routing broadcasting, buffer queues. It also includes the time from generating packet from sender to destination and express in seconds.

Load- Load represents the total load in bit/sec submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network. When there is more traffic coming on the network, and it is difficult for the network to handle all this traffic so it is called the load. The efficient network can easily cope with large traffic coming in, and to make a best network, many techniques have been introduced[5].

Media Access Delay:- The Time taken by a node to access a media in order to transfer a data packet from source node to destination node is known as Media Access Delay

5. RESULTS AND ANALYSIS

1. Throughput: Fig **a** shows the throughput for each protocol. The maximum throughput for TORA protocol is at 7,500 bits/sec for 30 nodes and 1,500 nodes for 10 nodes after 300 sec

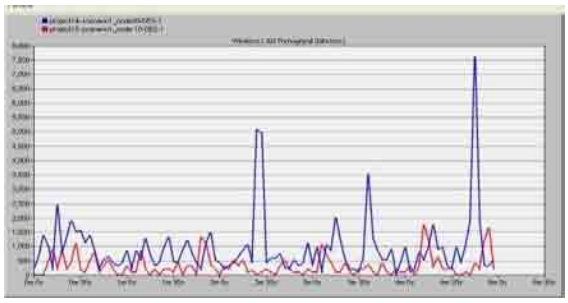


Fig a : Throughput of TORA for 10 and 30 nodes

Load: Fig. b shows the increase in network load for TORA for 30 and 60 nodes respectively. From fig it is observed that network load starts increasing and then reaches its maximum value at below 6,500 bits for 30 nodes whereas for 10 nodes it is somewhat below then 1,500 bits .

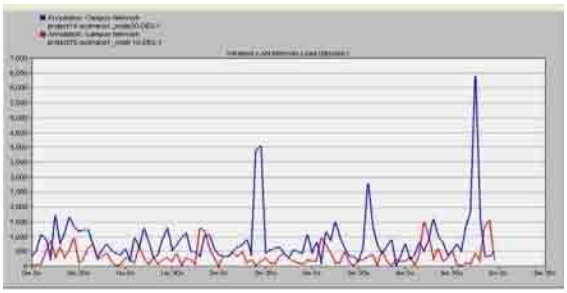


Fig b Load of TORA for 10 and 30 nodes

Media Access Delay: fig c shows the media acces delay of TORA protocol . for 30 nodes it is highest at 0.0020 bits

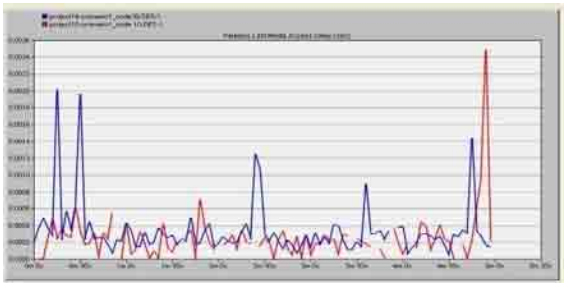
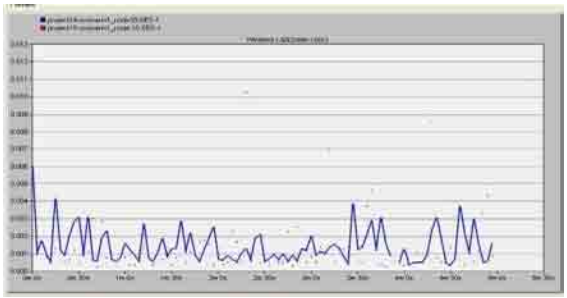


Fig c: Media Access Delay for 10 and 30 nodes

Wireless LAN Delay**:** fig d shows the delay for 30 and 10 nodes .for 10 nodes it is seen only as dots andfor 3o nodes its is highest at 0.006 bits .



'Fig d LAN Delay for 10 and 30 nodes

6. CONCLUSION

In this paper , performance of TORA is analysed using OPNET modeler 14.5 . as shown above Throughput is highest for 30 nodes whereas media acces delay is at its highest value for 10 nodes. Finally when overall performance is compared throughput is the main factor because it is the actual rate of data received successfully by nodes in comparison to the claimed bandwidth. Over the past few years, new standards have been introduced to enhance the capabilities of ad hoc routing protocols. As a result, ad hoc networking has been receiving much attention from the wireless research community. With regards to overall performance TORA performed good . The simulation study of this report consisted of routing protocol TORA deployed over MANET using FTP traffic analysing their behaviour with respect to five parameters i.e. delay, network load, throughput, media access delay

7. REFERENCES

1. Md.Masud Parvez1, Shohana Chowdhury2, S.M.Bulbul Ahammed3, A.K.M Fazlul Haque4, Mohammed Nadir Bin Ali5 "Improved Comparative Analysis of Mobile Ad-hoc Network" 1,2,3,4 Department of Electronics and Telecommunication Engineering 5Department of Computer Science Engineering

2. Tamilarasan-Santhamurthy "A Quantitative Study and Comparison of AODV, OLSR and TORA Routing Protocols in MANET" Department of Information Technology, LITAM, Dullipala (village), Sattenpalli (Mandal), Guntur, Andhra Pradesh, 522412, India

3. Pankaj Palta, Sonia Goyal " Comparison of OLSR and TORA Routing Protocols Using OPNET Modeler "Punjabi University Patiala

4. Ashish Shrestha Firat Tekiner" On MANET Routing Protocols for Mobility and Scalability" School of Computing, Engineering and Physical Sciences, University of Central Lancashire Preston, UK School of Computing, Engineering and Physical Sciences, University of Central Lancashire Preston, UK ftekiner@uclan.ac.uk

5. Gaganjeet Singh Aujla & Sandeep Singh Kang "Simulation Based Comparative Analysis Of TORA ,OLSR And GRP For Email And Video Conferencing Applications Over Manets " Department of CSE, Chandigarh Engineering College, Punjab, India.

6. P. Kuppusamy, K. Thirunavukkarsu and B. Kalavathi, "A study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad hoc Networks", Proceedings of 3rd IEEE Conference on Electronics Computer Technology (ICECT 2011), 8-10 April 2011

7. P.Kuppusamy, Dr. K. Thirunavukkarasu andDr. B .Kalaavathi, "A Study andComparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks",IEEE 2011.

8. C. Mbarushimana, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks", IEEE Journal on 21st International Conference on Advanced Information Networking and Application Workshops (AINAW'07), Volume 2, pp. 679-684, May 2007.

9. ER. SAURABH MITTAL*; PINKI** « PERFORMANCE EVALUATION OF AODV, DSR, DSDV AND TORA ROUTING PROTOCOLS « ZENITH International Journal of Multidisciplinary Research Vol.2 Issue 2, February 2012, ISSN 2231 5780

PERFORMANCE ANALYSIS OF ZONE ROUTING HYBRID PROTOCOL ON MANET

Rupinder kaur [1] , Abhinash Singla [2] , Emanpreet kaur [3]
[1]Assistant Professor (CSE), Bhai Gurdas Instituteof Engg. & Tech., Sangrur, Punjab, India
[2]Assistant Professor (CSE), Bhai Gurdas Institute of Engg. & Tech., Sangrur, Punjab, India
[3]M.Tech (CSE) Student, Bhai Gurdas Institute of Engg. & Tech., Sangrur.Punjab,India
[1] Rupinder.walia84@gmail.com
[2] abhinash11@gmail.com
[3] Sra_gagandeep@yahoo.co.in

Abstract:- MANET is combination of wireless mobile nodes that communicate with each other without any kind of centralized control or any device or established infrastructure. Therefore MANET routing is a critical task to perform in dynamic network. Without any fixed infrastructure, wireless mobile nodes dynamically establish the network.. A mobile ad hoc networks (MANET) is characterized by multihop wireless connectivity consisting of independent nodes which move dynamically by changing its network connectivity without the uses of any pre-existent infrastructure. MANET offers such flexibility which helps the network to form anywhere, at any time, as long as two or more nodes are connected and communicate with each other either directly when they are in radio range or via intermediate mobile nodes. Routing is a significant issue and challenge in ad hoc networks and many routing protocols have been proposed like OLSR, AODV, DSDV,DSR, ZRP, and TORA, LAR so far to improve the routing performance and reliability[9] This research paper provides the overview of ZRP by presenting its functionality. The performance of ZRP (Zone Routing Protocol) is analyzed on the basis of various parameters using simulator OPNET 14.0.

Keywords: MANET, Routing Protocols, ZRP

1.INTRODUCTION

Ad-hoc networks are self-organizing wireless networks composed of mobile nodes and requiring no fixed infrastructure. The limitations on power consumption imposed by portable wireless radios result in a node transmission range that is typically small, relative to the span of the network.

To provide communication throughout the entire network, each node is also designed to Serve as a relay. The result is a distributed multi -hop network with a time-varying topology. Because ad-hoc networks do not rely on existing infrastructure and are self-organizing, they can be rapidly deployed to provide robust communication in a variety of hostile environments. This makes ad-hoc networks very appropriate for providing tactical communication for military, law enforcement and emergency response efforts.

Ad-hoc networks can also play a role in civilian forums such as electronic classrooms, convention centers and construction sites. With such a broad scope of applications, it is not difficult to envision ad-hoc networks operating over a wide range of coverage areas, node densities and node velocities. A mobile ad hoc network may consist of only two nodes or hundred nodes or thousand nodes as well. The entire collection of nodes is interconnected in many different ways. As shown in Fig-1 there is more than one path from one node to another node. To forward a data packet from source to destination, every node in the hope must be willing to participate in the process of delivering the data packet. A single file is split it into a number of data packets and then these data packets are transmitted through the different paths. At the destination node, all these packets are combined in sequence to generate the original file. , routers.

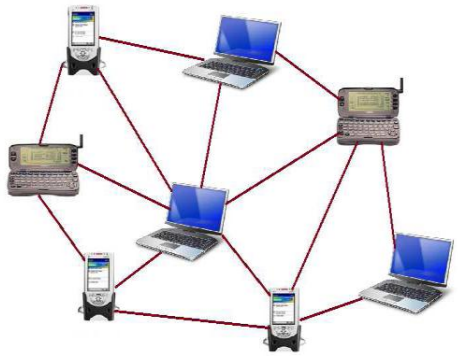


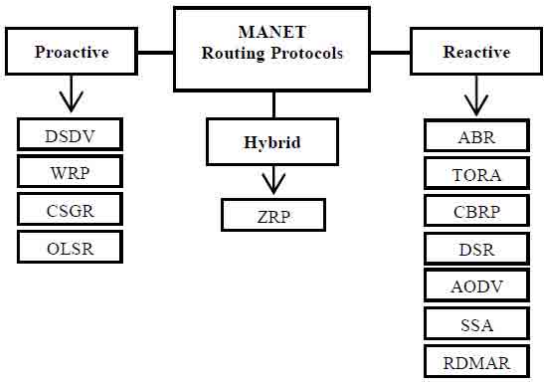
Fig-1: Mobile Ad hoc Network

2. ROUTING IN MANET

Routing [3] is the process of transferring a packet from source to its destination. In the routing process, a mobile node will search for a path or route to communicate with the other

node in the network. Protocols are the set of rules through which two or more devices communicate with each other. In MANET, routing tables are used for routing purpose. Routing tables contain the information of routes to all the mobile nodes .The routing protocols in MANET are broadly classified into three categories :

- Proactive or Table Driven Routing Protocols.
- Reactive or On-Demand Routing Protocols.
- Hybrid Routing Protocols.



2.1. Proactive or Table Driven Routing Protocols

In proactive protocols, each node maintains individual routing table containing routing information for every node in the network. Each node maintains consistent and current up-to-date routing information by sending control messages periodically between the nodes which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors. The drawback of proactive routing protocol is that all the nodes in the network always maintain an updated table. Some of the existing proactive routing protocols are DSDV and OLSR .

2.2. Reactive or On-demand Routing Protocols

In Reactive or On-Demand [1] Routing Protocols, routes are not predefined. For packet transmission, a source node calls for route discovery phase to determine the route. The route discovery mechanism is based on flooding algorithm which employs on technique that a node just broadcasts the packet to all its neighbours and intermediate nodes forwards the packets to their neighbours . Reactive protocols are Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA).

2.3. Hybrid Routing Protocols

Hybrid Protocols are the combination of both i.e. Table-Driven and On-Demand protocols. These protocols take the advantage of best features of both the above mentioned protocols. These protocols exploit the hierarchical network architecture and allow the nodes to work together to form some sort of backbone, thus increasing scalability and reducing route discovery . Nodes within a particular geographical area are said to be within the routing zone of the given node. For routing within this zone, Proactive i.e. table-driven approach is used. For nodes that are located outside this zone, Reactive i.e. an on demand approach is used. So in Hybrid Routing Protocols, the route is established with proactive routes and uses reactive flooding for new mobile nodes In Hybrid Routing protocols, some of the characteristics of proactive and some of the characteristics of reactive protocols are combined, by maintaining intra-zone information proactively and inter-zone information reactively, into one to get better solution for mobile ad hoc.

3.Zone Routing Protocol

Zone Routing Protocol or ZRP was the first hybrid routing protocol with both a proactive and a reactive routing component. ZRP was first introduced by Haas in 1997. ZRP is proposed to reduce the control overhead of proactive routing protocols and decrease the latency caused by routing discover in reactive routing protocols. ZRP defines a zone around each node consisting of its k-neighborhood (e. g. k=3). In ZRP, the distance and a node, all nodes within hop distance from node belongs to the routing zone of node. ZRP is formed by two sub-protocols, a proactive routing protocol: Intra-zone Routing Protocol (IARP), is used inside routing zones and a reactive routing protocol: Inter-zone Routing Protocol (IERP), is used between routing zones, respectively.

A route to a destination within the local zone can be established from the proactively cached routing table of the source by IARP, therefore, if the source and destination is in the same zone, the packet can be delivered immediately.

For each node a routing zone is defined separately. Within the routing zone, routes are available immediately but for outside the zone, ZRP employs route discovery procedure. For each node, a separate routing zone is defined. The routing zones of neighboring nodes overlap with each other's zone. Each routing zone has a radius ρ expressed in hops . The zone includes the nodes whose distance from the source node is at most ρ hops. In Fig-2, routing zone of radius 2 hops for node A is shown. Routing zone includes nodes all the nodes except node L, because it lies outside the routing zone node A. The routing zone is not defined as physical distance, it is defined in hops. There are two types of nodes for a routing zone in ZRP :

· Peripheral Nodes
· Interior Nodes

The nodes whose minimum distance to central node is exactly equal to the zone radius ρ are Peripheral Nodes while the nodes whose minimum distance is less than the zone radius ρ are Interior Nodes. In Fig. 2, Peripheral nodes are E, F, G, K, M and Interior Nodes are B, C, D, H, I, J.

The node L is outside the routing zone of node A.

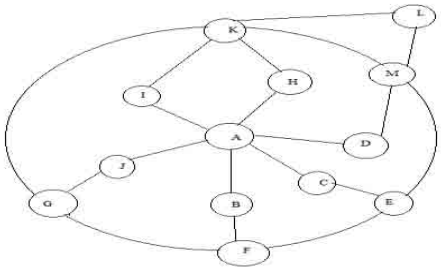


Fig-2: Routing Zone of Node A with Radius ρ=2 hop

4.SIMULATION PARAMETERS

To analyze the performance of ZRP OPNET 14.0 simulator is used. Scenario is created with 40 number of mobile nodes. The pause time and traffic load are kept constant under all the scenarios. Simulation parameters used for the implementation of ZRP are listed in the Table 1.

Parameters	Values
Simulator	OPNET 14.0
Protocol	ZRP
Simulation Time	600 sec
Simulation Area	800m *800 m
Data Rate	11 Mbps
Number of Nodes	40
Buffer Size	1024000

Table1:- Simulation ParameterS

4.1 Performance Metrics

The following performance metrics are used to analyze the simulated result:-

(a) Throughput [2]: Throughput is the average rate of successful data packets received at the destination .It is the measure of how fast we can actually send the packets through the network. It is measured in bits per second (bits/sec or bps) or data packets per second.

(b) Load [4]: Load in the wireless LAN is the number of packets sent to the network greater than the capacity of the network. When the load is less than the capacity of the network, the delay in packets is minimum. The delay increases when the load reaches the network capacity.

(c) Delay [7]: The packet end-to-end delay refers to the time taken for a packet to be transmitted across the network from source to destination. In other words, it is the time a data packet is received by the destination minus the time a data packet is generated by the source. It is measured in seconds. End. Lost packets due to delay have a negative effect on received quality.

5.RESULTS AND ANALYSIS

1.Load: From Fig-4 it is observed that load of ZRP is 50,000 bits per second with 20 nodes . Maximum load of 182,000 bits per second is observed with 40 nodes

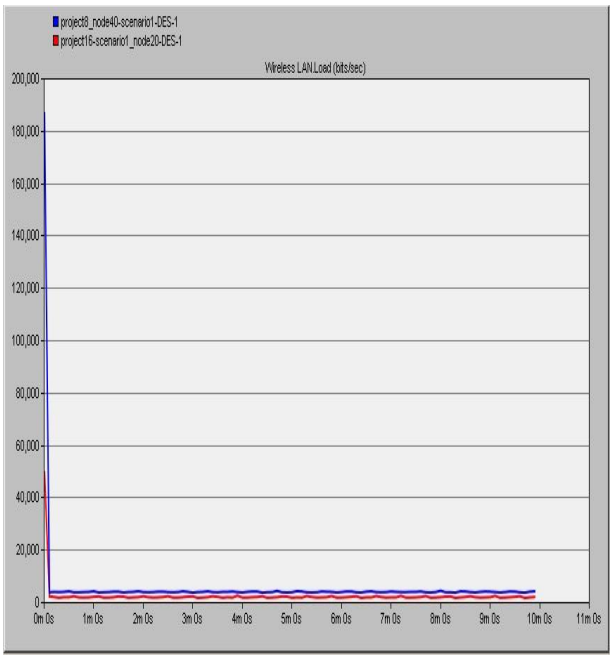


Fig: 3 Load over 20 and 40 nodes in ZRP

2.Throughput: It is observed from the Fig-4 that with 40 nodes the throughput of ZRP is about 3,550,000 bits per second in starting and 580,000 bits per second with 20 nodes.

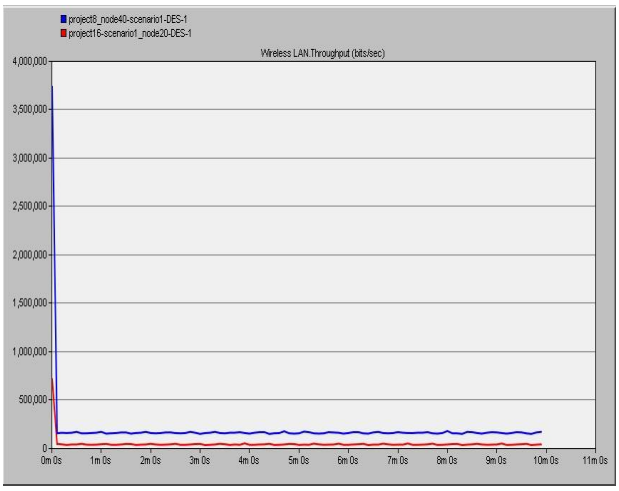


Fig: 4 Throughput over 20 and 40 nodes in ZRP

3.Delay: From Fig-5, it is observed that delay of ZRP is high at .0057 sec is observed with 40 nodes and .0033 second with 20 nodes

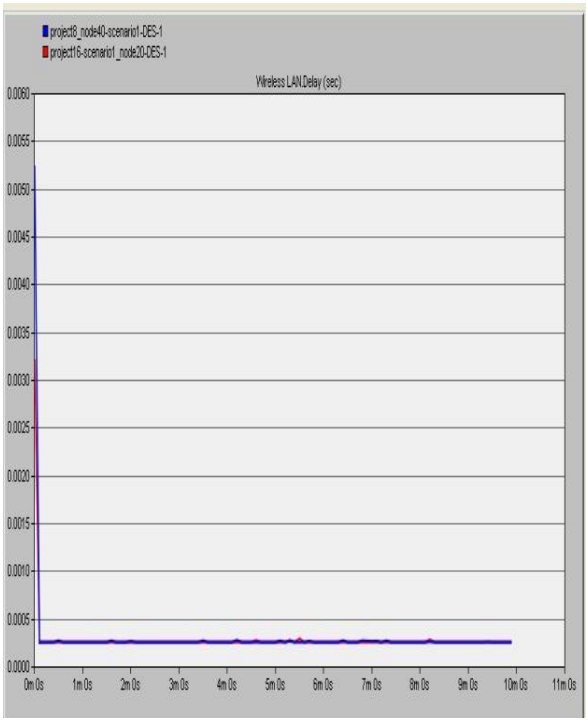


Fig: 5 Delay over 20 and 40 nodes in ZRP

6.CONCLUSION

The Zone Routing Protocol (ZRP) provides a flexible solution to the challenge of discovering and maintaining routes .The ZRP combines two radically different methods of routing into one protocol. Route discovery is based on a reactive route request / route reply scheme. This querying can be performed efficiently through the proactive maintenance of a local *routing zone* topology. In this paper, a performance analysis of ZRP routing protocols for mobile Ad-hoc networks is presented with 20 and 40 nodes. Performance of these routing protocol is evaluated with respect to four performance metrics such as delay, load and throughput .As observed from the results that when the simulation starts no data is dropped till one minute also the throughput is also less and throughput also increases till the end of the simulation. The simulation study of this report consisted of routing protocol ZRP deployed over MANET using Voice Conferencing Application analyzing their behavior. So the results of zrp is pretty good .

7. REFERENCES

[1] Nadia Qasim, Fatin Said, Hamid Aghvami, "Mobile Ad Hoc Networks Simulations Using Routing Protocols for Performance Comparisons", *Proc. of the World Congress on Engineering*, vol. 1, WCE 2008, July 2008.

[2] Kuncha Sahadevaiah, Oruganti Bala, Venkata Ramanaiah, "An Empirical Examination of Routing Protocols in Mobile Ad Hoc Networks", *Proc. Of* International Journal of Communications, Network and System Sciences, June 2010.

[3] Hongbo Zhou, "A survey on Routing Protocols in MANETs", Proc. of Michigan State University, MSUCSE- 03-08, March 2003.

[4] Kavita Panday, Abishek Swaroop, "A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid MANETs Routing Protocols", Proc. Of International Journal of Computer Sciences Issues, vol. 8, Issue 6, no. 3, Nov 2011.

[5] Zygmunt J. Haas, "The Zone Routing Protocol (ZRP) for Ad hoc Networks", Internet Draft, July 2002.

[6] Parma Nand, Dr. S.C. Sharma, "Comparative study and Performance Analysis of FSR, ZRP and AODV Routing Protocols for MANET*",* Proc. Of International Journal of Computer Applications, 2011.

[7] Ashish K. Maurya, Dinesh Singh, "Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocols in MANET", Proc. of Internationl Journal of Computer Applications, vol.12, no.2, November 2010.

[8]. Zygmunt J Haas, Marc R. Pearlman, and Prince Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", draftietf-manet-zone-zrp-04.txt,july,2002.

[9]. Hrituparna Paul1, Priyanka Sarkar2" a study and comparison of olsr, aodv and zrp routing protocols in ad hoc networks" ijret: international journal of research in engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308

Mobile Ad Hoc Networking: Imperatives and Challenges

Gurjeet Singh , Avtar Singh
Amritsar College of Engineering and Technology, Amritsar

ABSTRACT

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. The Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. It represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ‘‘ad-hoc’’ network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Ad hoc networking concept is not a new one, having been around in various forms for over 20 years.

Traditionally, tactical networks have been the only communication networking application that followed the adhoc paradigm. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of

MANET. This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies.Then, it reviews the latest research activities in these areas of MANET_s characteristics, capabilities and applications.

1. INTRODUCTION

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless

systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile adhoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile adhoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. An Ad-hoc network is a collection of wireless mobile nodes which

dynamically forming a temporary mobile nodes which dynamically forming a temporary network without the aid of any established infrastructure or centralized administration. The proliferation of mobile computing and communication devices (e.g., cell phones, laptops, handheld digital devices,

personal digital assistants, or wearable computers) is driving a revolutionary change in our information society.

We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ubiquitous Computing age in which a user utilizes several electronic platforms at a single instance through which he can access all the required information whenever and wherever needed. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations; tourists can use Global Positioning System (GPS) terminals installed inside rental cars to locate driving maps and tourist attractions, researchers can exchange files and other

information by connecting portable computers via wireless LANs while attending conferences; at home, users can synchronize data and transfer files between portable devices and desktops. Not only are mobile devices getting smaller, cheaper, more convenient, and

more powerful, they also run more applications and network services, commonly fueling the explosive growth of mobile computing equipment market. The exploding number of Internet and laptop users driving this growth further. Projections show that in the next two years the number of mobile connections and the

number of shipments of mobile and Internet terminals will grow yet by another 20–50%. With this trend, we can expect the total number of mobile Internet users soon to exceed that of the fixedline Internet users. Among all the applications and services run by mobile devices, network connections and corresponding data

services are without doubt the most demanded service by the mobile users.

According to a study, the number of subscribers to wireless data services will grow rapidly from 2.6 billion worldwide in 2009 to more than 3.3 billion in 2010, and the number of wireless messages sent per month will rise continuously. Currently, most of the connections among these wireless devices are achieved via fixed infrastructure-based service provider, or private networks

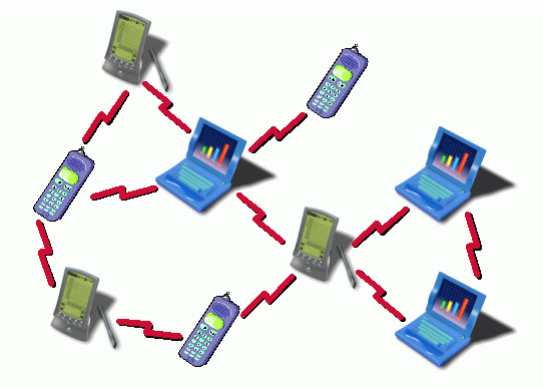


Fig. 1 : Mobile Network

There are, furthermore, situations where user required networking connections are not available in a given geographic area, and providing the needed connectivity and network services in these situations becomes a real challenge. More recently, new alternative ways to deliver the services have been emerging.

These arefocused around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile network that is both flexible and powerful. In this way, not only can mobile nodes communicate with each other, but can also receive Internet services through Internet gateway node, effectively extending Internet services to the non-infrastructure area. As the wireless network continues to evolve, these ad hoc capabilities are expected to become more important, the technology solutions used to support more critical and significant future research and development efforts can be expected in industry and academy.

Inside the ad hoc networking field, wireless sensor networks take a special role. A sensor network is composed of a large number of small sensor nodes, which are typically densely (and randomly) deployed inside the area in which a phenomenon is being monitored. Wireless ad hoc networking techniques also constitute the basis for sensor networks. However, the special constraints imposed by the unique characteristics of sensing devices, and by the application requirements, make many of the solutions designed for multi-hop wireless networks (generally) not suitable for sensor

networks. This places extensive literature dedicated to sensor networks beyond the scope of this paper; however, the interested reader can find an excellent and comprehensive coverage of sensor networks in a recent survey. This paper demonstrates the impetus behind mobile ad hoc networks, and presents a representative collection of technology solutions used at the different layers of the network.

2. AD HOC NETWORKING AND 4G

A major goal toward the 4G Wireless evolution is the providing of pervasive computing environments that can seamlessly and ubiquitously support users in accomplishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device. In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need.

The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the environment, without requiring any major change in the users behavior. This new philosophy is the basis of the Ambient Intelligence concept. The objective of ambient intelligence is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and ‘‘natural’’ interactions, a multitude of services and applications. Ambient intelligence places the user at the center of the information society. This view heavily relies on 4G wireless and mobile communications. 4G is all about an integrated, global network, based on an open systems approach. Integrating different types of wireless networks with wire-line backbone network seamlessly, and convergence of voice, multimedia and data traffic over a single IP-based core network are the main foci of 4G. With the availability of ultra-high bandwidth of up to 100 Mbps, multimedia services can be supported efficiently; ubiquitous computing is enabled with enhanced system mobility and portability support, and location-based services.

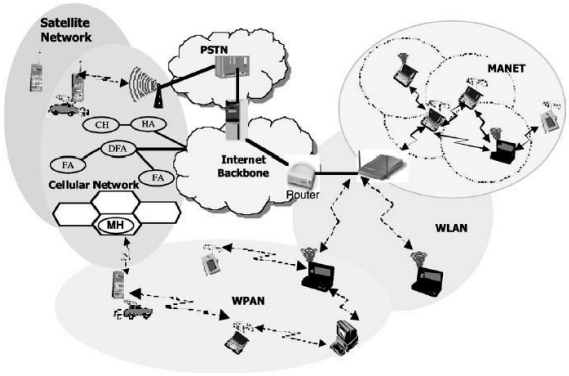


Fig.2 : 4G Networks

2.1 Evolution of MANET

In 1970, Normanl Abramson and his fellow researchers at the University of Hawaii invented ALOHAnet. In 1972 DARPA Packet Radio Network (PRNet) In 1980 Survivable Radio Networks (SURAN). During 1980 emergence of Internet Emerging Task Force (IETF), termed the mobile ad hoc networking group. In 1994 emergence of Bluetooth by Ericsson.

2.2 Characteristics of MANET

* Network is not depend on any fix infrastructure for

its operation.
* Easy of deployment Speed of deployment
* Dynamic Chanigng Topology of nodes
* Multi-hop network
* Each node is working as intelligent node
* Not any mediator networking device is required for Communicatons
* Each node is work as a DTE (Data Terminal Equipment) and DCE (Data Communication Equipment)

3. AD-HOC APPLICATIONS

Tactical networks : Military Communication automated Battle fields Sensor Network : Remote weathers for sensors, earth activities Emergency Services : Disaster recovery, earthquakes, crowd control and commando operations Educational Applications : Setup virtual class & conference rooms Entertainment : Multi-user games, robotics pets. Location Aware Services. Automatic Call forwarding, advertise location specific services, Location–dependent travel guide. In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. To present the huge amount of research activities on ad hoc networks in a systematic/organic way, we will use, as a reference, the simplified architecture shown in as shown in the figure, the research activities will be grouped, according to a layered approach into three main areas:

• Enabling technologies;
• Networking;
• Middleware and applications.

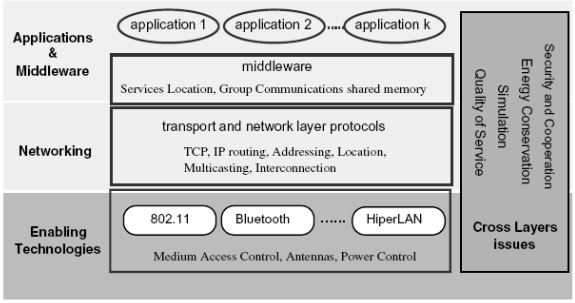


Fig 3. MANET Architecture

In addition, as shown in the figure, several issues (energymanagement, security and cooperation, quality of service, network simulation) span all areas, and we discuss them separately.

Ad hoc networks can be classified, depending on their coverage area, as : Body (BAN), Personal (PAN), Local (LAN), Metropolitan (MAN) and Wide(WAN) area networks. Ad-hoc singlehop BAN, PAN and LAN wireless technologies are already common on the market, these technologies constituting the building blocks for constructing small, multi-hop, ad hoc networks that extend their range over multiple radio hops. For these reasons, BAN, PAN and LAN technologies constitute the Enabling technologies for ad

hoc networking. The success of a network technology is connected to the development of networking products at a competitive price.

A major factor in achieving this goal is the availability of appropriate networking standards. Currently, two main standards are emerging for ad hoc wireless networks: the IEEE 802.11 standard for WLANs, and the Bluetooth specifications 3 for short-range wireless communications.

4. BLUETOOTH

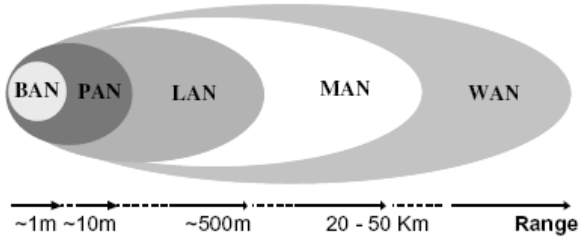


Fig. 4 : Bluetooth range

The Bluetooth technology is a de-facto standard for low-cost, short-range radio links between mobile PCs, mobile phones, and other portable devices. The Bluetooth Special Interest Group (SIG) releases the Bluetooth specifications. Bluetooth specifications were established by the joint effort from over two thousand industry leading companies including 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, Toshiba, etc. under the umbrella of Bluetooth SIG. In addition, the IEEE 802.15 Working Group for Wireless Personal Area Networks approved its first WPAN standard derived from the Bluetooth Specification. The IEEE 802.15.1 standard is based on the lower portions of the Bluetooth specification.

A Bluetooth unit, integrated into a microchip, enables wireless ad hoc communications, of voice and data between portable and/or fixed electronic devices like computers, cellular phones, printers, and digital cameras. Due to its low-cost target, Bluetooth microchips may become embedded in virtually all consumer electronic devices in the future.

5. IEEE 802.11 NETWORKS

In 1997, the IEEE adopted the first wireless local area network standard, named IEEE 802.11, with data rates up to 2 Mbps. Since then, several task groups (designated by the letters from _a_, _b_, _c_, etc.) have been created to extend the IEEE 802.11 standard. Task groups_ 802.11b and 802.11a have completed their work by providing two relevant extensions to the original standard, which are often referred to with the friendly name of Wireless Fidelity (Wi-Fi). The 802.11b task group produced a standard for WLAN operations in 2.4 GHz band, with data rates up to 11 Mbps and backward compatibility. This standard, published in 1999, has become an ‘‘overnight success’’, with

several IEEE 802.11b products available on the market currently. The 802.11a task group
created a standard for WLAN operation in the 5 GHz band, with data rates up to 54 Mbps. Among the other task groups, it is worth mentioning the task group 802.11e (attempting to enhance the MAC with QoS features to support voice and video over 802.11 networks), and the task group 802.11g (that is working to develop a higher speed extension to the 802.11b). The IEEE 802.11 standard defines two operational modes for WLANs: infrastructure-based and infrastructure-less or ad hoc. Network interface cards can be set to work in either of these modes but not in both simultaneously. Infrastructure mode resembles cellular infrastructure-based networks. It is the mode commonly used to construct the so-called Wi-Fi hotspots, i.e., to provide wireless access to the Internet. In the ad hoc mode, any station that is within
the transmission range of any other, after a synchronization phase, can start communicating.

6. MAC PROTOCOL

Bluetooth and IEEE 802.11 technologies exemplify the two main categories in which multiple access networks can be categorized into: random access (e.g., CSMA, CSMA/CD) and controlled access (e.g., TDMA, token passing schemes, etc.). The lack of an infrastructure, and the peer-to-peer nature of ad hoc networking, make random access protocols the natural choice for medium access control in ad hoc networks. Indeed, most proposals of MAC protocols for ad hoc networks are based on the random access paradigm; in addition, the CSMA/CA scheme was selected (due to the inherent flexibility of this scheme) by the IEEE802.11 committee as the basis for its standards. On the other hand, demand assignment access schemes (even though generally more complex) are more suitable for environments that need guarantees
on the Quality of Service (QoS) perceived by its users. Several controlled access schemes exist, e.g., TDMA, CDMA, token-passing, etc. Among these, TDMA is the most commonly used in ad hoc networks. In the TDMA approach, the channel is generally organized in frames, where each frame contains a fixed number of time slots. The mobile hosts negotiate a set of TDMA slots in which to transmit. The mobile multi-hop ad hoc environment brings fresh challenges to TCP protocol. The dynamic topologies, and the interaction of MAC protocol mechanisms (e.g., 802.11 exponential back-off scheme) with TCP mechanisms (congestion control and time-out) lead in a multihop environment to new and unexpected phenomena.

7. NETWORK SECURITY AND COOPERATION

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design. Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers_ control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. Finally, the security of routing protocols in the MANET dynamic environment is an additional challenge. The self-organizing environment introduces new security issues that are
not addressed by the basic security services provided for
infrastructure based networks. Security mechanisms that solely enforce the correctness or integrity of network operations would thus not be sufficient in MANET. A basic requirement for keeping the network operational is to enforce ad hoc nodes contribution to network operations, despite the conflicting tendency (motivated by the energy scarcity) of each node towards selfishness.

8. SECURITY ATTACKS

Securing wireless ad hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Ad hoc networks have to cope with the same kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context The complexity and diversity of the field (different applications have different security constraints) led to a multitude of proposals that cannot be all surveyed in this article. Detailed analyses of ad hoc networking security issues and solutions can be found in. Below we summarize only the main directions of security
in ad hoc networks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active attacks can be easily performed against an ad hoc network. These attacks can be grouped in: Impersonation, Denial of service, and Disclosure attack. Secure routing : Secure routing protocols cope with malicious nodes that can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. Recent studies brought up also a new type of attack that goes under the name of wormhole attack mentioned earlier. Cooperation enforcing : A basic requirement for keeping an ad hoc network operational is to enforce ad hoc nodes contribution to basic network functions such as packet forwarding and routing. Unlike networks using dedicated nodes to support basic network functions including packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This difference is at the core of some of the security problems that are specific to ad hoc networks. As opposed

to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. For example, routing is vulnerable in ad hoc networks because each device acts as a router. Forwarding mechanism is cooperative, as well. Communications between nodes, more than 1-hop away, are performed by exploiting intermediate relaying nodes. A node that does not cooperate is called a misbehaving node. Routing–forwarding misbehaviors can be caused by nodes that are malicious or selfish. A malicious node does not cooperate because it wants to intentionally damage network functioning by dropping packets. On the other hand, a selfish node does not intend to directly damage other nodes, but is unwilling to
spend battery life, CPU cycles, or available network bandwidth to forward packets not of direct interest to it, even though it expects
others to forward packets on its behalf. Such a node uses the network but does not cooperate.

9. SIMULATION AND PERFORMANCE EVALUATION

There are two main approaches in system performance evaluation: the first uses measurements; the second is based on a representation of the system behavior via a model Measurement techniques are applied to real systems, and thus they can be applied only when a real system, or a prototype of it, is available. Currently, only few measurements studies on real ad hoc testbeds can be found in the literature. The Uppsala University APE testbed is one of the largest, having run tests with more than thirty nodes. The results from this testbed are very important as they are pointing out problems that were not detected by preceding simulation studies. An important problem, related to the different transmission ranges for 802.11b control and data frames, is the so-called communication gray zones problem. This problem was revealed by a group of researchers at the Uppsala University, while measuring the performance of their own implementation of the AODV routing protocol in an IEEE 802.11b ad hoc network. Observing an unexpected large amount of packets_ losses, mainly during route changes, it was found that increase in packet loss occurred in some specific geographic areas termed called ‘‘communication gray zones’’. In such zones, the packet loss experienced by a station may be extremely high, up to 100%, thus severely affecting the
performance of applications associated with a continuous packet flow (e.g., file transfers and multimedia streaming). It was also found that the reason for this phenomenon is that a station inside a gray zone is considered (using the routing information) reachable
by a neighboring station, while actual data communication between the stations is not possible. The same problem was found to affect other routing protocols, such as OLSR. It is important to point out that communication gray zone problem cannot be revealed by commonly used simulation tools (e.g., NS-2, Glomosim), as in these 802.11 models both unicast and broadcast transmissions are performed at 2 Mbps, and hence have the same transmission range. Constructing a real ad hoc network testbed for a given scenario is typically expensive and remains limited in terms of working scenarios, mobility models, etc. Furthermore,
measurements are generally non-repeatable. For these reasons, protocols scalability, sensitiveness to users mobility patterns and speeds are difficult to investigate on a real testbed. Using a simulation or analytic model, on the other hand, permits the study of system behavior by varying all its parameters, and considering a large spectrum of network scenarios.
Evaluating system performance via a model consists of two steps:
(i) defining the system model, and (ii) solving the model using analytical and/or simulative techniques. Analytical methods are often not detailed enough for the ad hoc networks evaluation and in terms of accounting for mobility, in their infancy.
On the other hand, simulation modeling is a more standardized, mature, and flexible tool for modeling various protocols and network scenarios, and allows (by running the simulation model) collection and analyses that fully characterize the protocol performance in most
cases. Mobility models. The ability of ad hoc networks protocols to correctly behave in a dynamic environment, where devices position may continuously change, is a key issue Network simulators : Most MANET simulative studies are based on simulation tools. The main advantage of these tools is that they provide libraries containing predefined models for most communication protocols.

10. QUALITY OF SERVICE

Providing Quality of Service (QoS), other than best effort, is a very complex problem in MANETs, and makes this area a challenging area of future MANET research. Network_s ability to provide QoS depends on the intrinsic characteristics of all the network components, from transmission links to the MAC and networklayers. MANET characteristics generally lead to the conclusion that this type of network provides a weak support to QoS. Wireless links have a (relatively) low and highly variable capacity, and high loss rates. Topologies are highly dynamic with frequent links
breakages. Random access-based MAC protocols, which are commonly used in this environment (e.g., 802.11b), have no QoS support. Finally, even after resource reservation, QoS still cannot be guaranteed due to the frequent disconnections and topology changes. Several QoS routing algorithms were published recently with a variety of QoS requirements and resource constraints, for example, CEDAR, ticket-based probing, Predictive Location-Based QoS Routing, Localized QoS routing and QoS routing based on bandwidth calculation.

11. CONCLUSIONS

In coming years, mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed nternet infrastructure, appears inevitable. Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self-administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET
technology. Finally, I would like to state that in the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-hoc Networks. So, it becomes the best solution of different problems of network.

12. REFERENCES

[1] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.

[2] A. Ahuja et al., Performance of TCP over different routing protocols in mobile ad-hoc networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC 2000), Tokyo, Japan, May 2000.

[3] B. Kalaavathi, et. Al, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1470874 Raj Kamal, Mobile Computing, Oxford University Press, 2009.

[4] Proceedings IT in Academics, Sinhgad Institute of Management, Pune, India, 2009.

[5] G. Anastasi, M. Conti, E. Gregori, A. Passarella, A power saving architecture for web access from mobile computers, in: Proceedings of the Networking 2002, Lecture Notes in Computer Science, vol. 2345, Springer, Berlin, 2002.

[6] S. Basagni, Distributed and mobility-adaptive clustering for multimedia support in multi-hop wireless networks, in: Proceedings of the IEEE Vehicular Technology Conference (VTC) 1999, Amsterdam, The Netherlands, September 19– 22, 1999.

Multicast Routing Protocols in Mobile Adhoc Network

Er.Kirandeep Kaur

M.tech research Scholars

Amritsar College of Engineering & Technology, Amritsar,

Email-id:-kiranthind991@gmail.com

ABSTRACT:-By using mobile and ad hoc network (MANNETs) the interactions in the group members of distributed wireless network environment may be easiest. As audio/video conferencing, e-commerce, education, management of disasters, battlefields are the some group oriented applications. Under user mobility, the dynamic construction of efficient and reliable multicast routes are the demands of the Group communication. The multicast routing mechanisms have been improved by researchers in various performance measures such as ratio of packet delivery, life time of networks, reliability, Quality of service(QOS),Delays and Security .The multimedia communication over MANETS uses most reliable and QOS based multicast routing mechanisms. The mechanisms are used in mesh, tree, zone and hybrid topologies.

*Keywords:*MANET, Quality of Service,Reliability, Topologies, Multicast Routing

I .INTRODUCTION

Mobile hoc network is a class of wireless communication networks. It does not have fixed-infrastructure. The disaster situations like tsunami, earthquake, terrorist activities, landslides, Battlefields are tackle by the concept of MANET. The applications such as online education, gaming, business etc. are later extended by the concept of MANET.As compared to other networks like WiFi, WiMAX, The MANET nodes do not provides reliable services and QOS(Quality of services)guarantees. The measurement of unreliability increases when we need to communicate real- time multimedia traffic where Quality Of Service (QOS) parameters are to be satisfied. To evaluate MANET, QOS is one of the significant component .QOS restricts the bounds on bandwidth, delay, bandwidth delay product, jitters and packet loss. Reliable multicast routing includes the mechanism such as error detection, Signaling of error messages to source and destination and retransmission method of lostpackets.

For reliable communication some of the parameters are node stability,link stability, route stability, survivability, mobility etc. Node Stability in MANET depends on parameters such as mobility, battery life, memory data transmission rate and number of interfaces currently being used. With higher mobility, a node become less stable and losses its connectivity. longer battery life provides more stability to the node under higher data transmission rates

Link stability depends on wireless link Characteristics such as link failures, packet loss rate, channel sensing rate, bit error rate, bandwidth, environmental effects. Checksum and sequence numbering for error control and some form of negative or missing positive acknowledgement with packet transformation for error recovery, is used by existing systems.

Route stability relies on the performance of source, destination and intermediate nodes and the wireless channel connecting end to end route. The reliability of end to end delivery may be enhanced with alternate routes between source and destination, if the life time of route decreases. There is a mesh based

and multipath routing techniques to enhance the route stability.

Network Survivabilityis the ability of a network to continue to functioning during and after failure. It consists of both network failure duration and failure impact on the network.

Now we have to define the various QOS parameters such as bandwidth, delay, jitter, bandwidth delay product and synchronization .

Bandwidth is the amount of data to be transferred every second i.e data transmission rate

Delay incurred between multimedia data generation at a source and its presentation at a destination is subject to have stringent bounds. End to end delay may be split into four contributing delays:

- source compression and packetization delay
- transmission delay
- synchronization delay
- sinkdecompression, depacketizationand output delay. Among these delays Transmission delay is a random delay.

In multi-hop networks there is an important parameter in MANETs which is called Bandwidth delay product. It provides measure of end to end network pipe in multi-hop networks. In the wire-line systems Bandwidth delay product is well understood concept. To fill network pipe, it defines enough number of in-flight packets. Bandwidth delay product which bounds multimedia applications becomes difficult to maintain end-to-end connectivity.

Jitter:The difference between the inter-generation times and inter-arrival times of adjacent packets is defined as a Jitter.Due to random network delays, Jitters are introduced and incurred by the sequence of packets of a continuous multimedia stream. By the use of buffers Jitters can be reduced in the end systems. The buffers used in the end system require very large memory resources and large buffers. Two types of Jitters can be used during data transmission i.e negative and positive Jitters. Negative Jitter reduces the inter-arrival time of the packet whereas positive buffer increases the inter-arrival time of the uffer. Downstream node congestion consecutive packet loss is the result of a sequence of negative jitter.Significant Delays are the result of a sequence of positive jitters

To solve throughout running of a multimedia application for a smooth and efficient playout, Synchronization and resynchronization of multimedia streams is a crucial task. To facilitate the better quality of presentation to the users ,it is necessary to address synchronization problem.

The level of QOS and associated parameters are also different from application to application. For E.g. the bandwidth and delay are the key parameters in multimedia applications. Whereassecurity and reliability are the additional requirements of military applications.

IIMethodology of Multicast routing mechanism in MANNETs

On the basis of topology and services within a topology multicast routing mechanisms are categorized The topology classification.

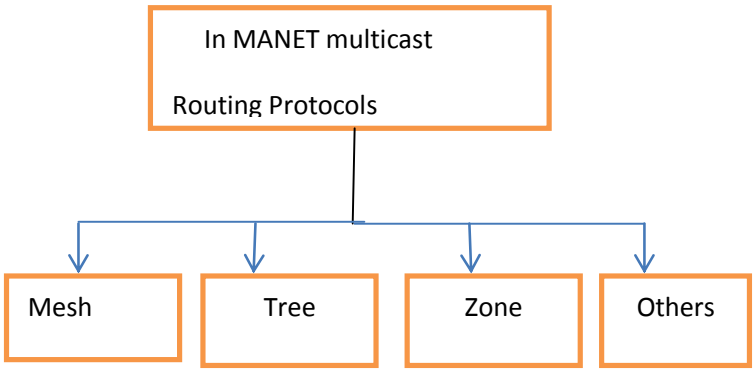
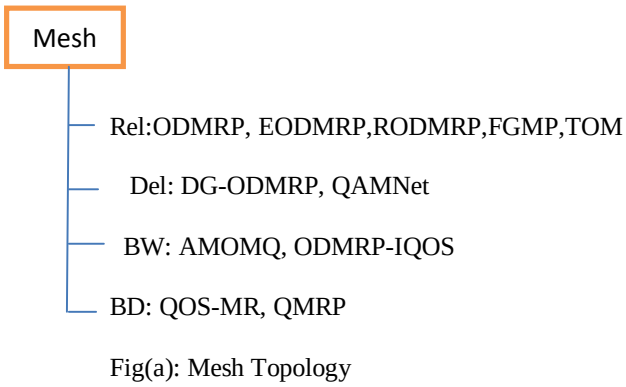


Fig1: Topology classification



Fig(a): Mesh Topology

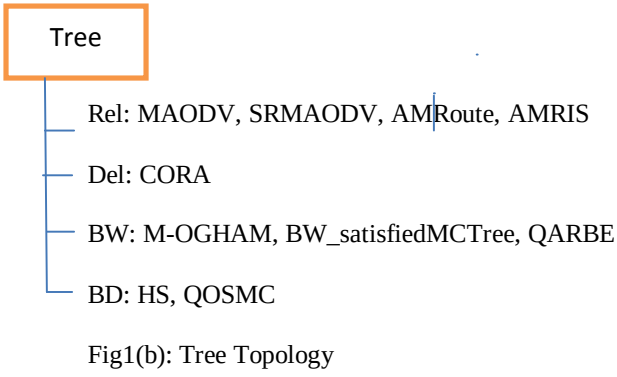


Fig1(b): Tree Topology

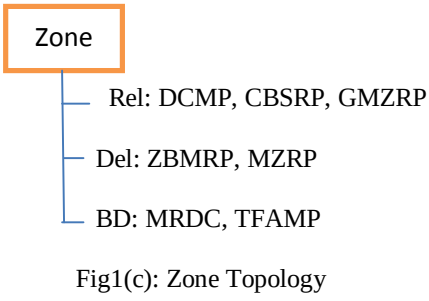


Fig1(c): Zone Topology

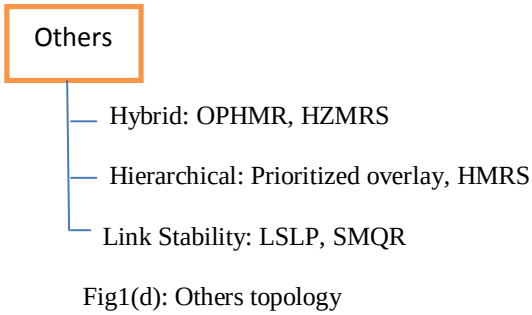


Fig1(d): Others topology

III. Multicast routing mechanism based on Mesh Topology:

A high redundancy in connectivity among nodesare created by Mesh based routing mechanism. The mechanism which creates routes among nodes aremore robust to link and node failures,Since the alternative routes facilitate the reliability of data transmission. Researchers Proposed several mesh based multicast routing mechanisms that provides reliable and QOS based Services.

Reliable Multicast Routing

The Reliable Multicast Routing Mechanism have the objective to deliver reliable data packets are as follows:

1. All the data packets are delivered to all the group members which are generated at the source
2. For a Source-destination pair; packets are delivered in –order
3. The total order is maintained if all the multicast group members receive packets in-order

Mesh based reliable multicast routing mechanism have the following principles for reliable communication:

- forming a mesh of forwarding groups to forward multicast packets;
- To reduce the control overhead and enhance reliability,controlled broadcasting is used
- In two tier hierarchical structure,construction of mesh among team leaders
- Backbone construction
- From source to destination, creating multiple paths.
- Creating a mesh of tree structure by multiple source based tree formation

Table1:Mesh Based Routing Protocols

Protocol	Operations	Advantages	Disadvantages	Applications
OD MRP	With control packets forwarding groups are formed	Less overhead, very robust to route failuresunicast and multicast	Needs Periodic refresh less scalable, more overhead because of more nodes	Video conferencing, defence Services
EODMRP	Computers rebroadcast probability and neighbor node density to find routes and to forward a packet	More Robust More Packet Delivery Less packet losses	More Processing overhead, Needs Periodic refresh More Delays	Real-Time Multimedia Services
RODMRP	To enhance reliability in ODMRP Clusters Authenticate packets	More Reliable under high mobility conditions	Processing and common overhead is more	Seamless services for live multimedia steaming
FGMP	Forwarding group is responsible for multicast routing	It is Robust due to its soft rate maintenance	High Control Overhead	Reliable Multicast for light weight sessions
TOM	Team is headed by Team leader, small group of nodes defined as a team	Two-Tier Architecture enhances robustness and reliability	To have intra and inter team communication ,control overhead is more	For military and Real-Time Services and tactical services it provides QOS Support
STORM	Nodes are putt into a team with similar mobility patterns	For Packet Delivery it enhance reliability	Uses less memory, Control overhead is High	Military and Tactical Services
DGODMRP	Multi-rate Transmission to meet Delay guarantee in ODMRP using SINR	Better Prediction of Network Load	Difficult End-to-End delay prediction	Constrained Delay Services
QAMNet	Extension to ODMRP for Service Differentiation between Real-time,best effort services	Lower Delays for Real Time Multicast flows	High admission control overhead	Interactive Multimedia services

IV. Multicast Routing Mechanisms Based on Tree

In tree based mechanism, multiple trees are constructed with root and branches. Roots of the tree as a source node and branches are terminate at each destination. The number of sources is equivalent to number of tree structures where some of the branches are common to more than one tree and forms a mesh tree. Data is originated from every source and all the trees transmit data independently. There is only one path between these approaches i.e Source-destination pair and the union of the paths from the source to the destination forms the multicast tree. This is done using either source based trees or shared trees. A Single multicast tree is maintained per source in Source based trees. A Single tree is shared by all the sources in multicast group by shared based trees. High data forwarding efficiency and low overhead is provided by Tree-based routing mechanism but in highly mobile environments it is not robust

Table 2: Tree Based Routing Protocols

Protocol	MAODV	SRMAODV	AM Route	AMRIS	CORA	QOSMC	QUARBE
Operation	For every multicast group shared trees are created. RREQ,RREP and sequence numbers are used	Bidirectional shared multicast trees maintained in a network	Using unicast tunnels creates multicast trees	Nodes have ID-numbers source has smallest ID ID increases with hops	Cooperative neighbor nodes keep short term data cache and form a core of forwarding nodes	Bandwidth based routes are calculated using listen and hello methods	Bandwidth delay based Hexagonal cells are created for routing
Advantages	Bandwidth utilization is maximum and space complexity is minimum	Support scalability For On-line routing of delivery guaranteed multicasts	With changes of network topology, Multicast tree unchanged ,more robust	No loops Link brakes local repair simplicity	Localized recovery is used and within bounded latency packet recovery	To meet QOS requirements it offers bandwidth guaranteed multicasting	Less communication and processing overhead, provides scalability
Disadvantages	Under mobility poor packet delivery	To select new group leader, group leader table must be updated frequently	Loop formations Inefficient in large networks ,Inefficient in high mobility ,waste of bandwidth	Rejoin scheme is slow increased hop distance	Due to low bandwidth and limited power Communication overhead is expensive	Non-availability of routes due to Channel condition and node failures triggers	Less robust and overhead is more for route maintenance
Application S	Video conference and group communication	Video on-demand services	Low response time require for interactive apps	Rapid recovery required by MultimediaApps	Low loss low delay with multicast multimedia delay	Real-time multimedia services constrained Bandwidth	Group oriented services and Multimedia

V Multicast Routing Mechanisms Based on Zone Topology:

To make Multicast routing decisions Simple and efficient, Zone based multicast routing mechanisms are used to form the clusters of nodes. All the nodes within clusters are connected to a cluster head. Nodes are connected either by a single hop or multiple hop within a cluster to the cluster head. To establish connection within a cluster different routing mechanisms are used:

Table3: Features of Zone Based Protocols:

Protocol	DCMP	CBSRP	GMZRP	DCM	CAMP	ZBMRP	MRDC	TFZMP
Advantages	Due to controlled Bandwidth less control overhead	Less latency and control overhead reduces	In terms of query packets and better PDR less overhead	Less overheads and better PDR	Control overhead is less, PDR is High, floods are avoided	Reduces overheads by controlling packet flooding inside zones	Under link and node failure better recovery is there	Data overhead decreases
Disadvantages	Per group multiple packets are controlled	Bottleneck on brodcasting cluster-head nodes	Protocol complexity is more	Parameters of stringent depends on group size, no. of sources	Cause significant packet losses due tocore node failures	Difficult to control dynamic refresh rate	Complex task to maintain core	For large scale networks poor scalability
Applications	Reliable services	Reliable services	Video conferencing services	Reliable multicast services	Reliable multicast services	In limited services delay constrained services	Group oriented services	For small scale networks

VI. Others Multicast Routing Protocol

There are many multicast routing mechanisms which fit into more than one category, Apart from the wide variety of multicast routing mechanisms discussed in the previous sections. we have discussed somepossible multicast routing mechanism proposed by Research community.

VII. Conclusion: In this paper we have to present the review of the multicast routing mechanism which is used to clarify the main design and implementation principles of the field of MANET multicast routing. In routing decisions the physical topology of nodes and the services offered by the nodes plays an important role. Hence the review of multicast routing mechanism focused upon the topology and their services. Topology includes Mesh based, tree based, zone based and others. These topologies are classified further such as reliability, bandwidth, delay, bandwidth delay. The other topologies are classified as hybrid, hierarchical and link stability.

Some of the improvements in the multicast routing mechanisms are as follows:

Enhancement in the bandwidth: By designing various schemes at physical layer link bandwidth can be improved. Bandwidth can be improved by directional antennas and mechanisms of interaction.

Heterogeneity: In terms of QOS Constraints nodes in the MANET are expected to be heterogeneous. Both hardware and software technologies provide support for heterogeneity.

Energy Consumption: For group communication among mobile devices multicast routing protocols for MANETs are designed. Energy consumption can be reduced by batteries solar energy or some other methods. It extends the lifetime of the nodes by adopting software and hardware component management.

Mobility: Nodes may move out of range of their neighbors and come within range of new nodes and are not able to communicate with old neighboring nodes. Hence the problem of fault tolerance is introduced by the mobility. When some of the intermediate nodes are moved from their neighbors range, an ideal multicast routing protocol is able to deliver packets from source to destination. This introduces the additional routing overhead as this complicates the design of the routing protocol.

Unification: Due to the diverse nature and wide range of operating conditions for each application, we find that there is no optimal multicast routing protocol for various types of group communication. Such multicast routing protocols are needed that adapt well to network conditions such as: traffic load, scalability, mobility, heterogeneity etc.

Scalability: Multicast routing protocols are designed to work for various sizes of networks. The size of the network increases and the number of nodes are also increases. Based on required parameters it provides better performance. To overcome scalability researchers proposed following methods:

- To provide scalability, it uses geographical information
- To provide scalability, it uses hierarchical routing structure.
- Provides scalability with caching mechanism.

References:

[1]. Ali MA, El-Sayed A, Morsi IZ. A survey of multicast routing protocols for ad-hoc wireless networks. Minutiae Journal of Electronic Engineering Research (MJEER) 2007;17(2):185–98.

[2]. Baburaj E, Vasudevan V. An intelligent mesh based multicast routing algorithm for MANETs using particle swarm optimization. International Journal of Computer Science and Network Security 2008;8(5):214–8.

[3]. Badarneh OS, Kadoka M. Multicast routing protocols in mobile ad hoc networks: a comparative survey and taxonomy. EURASIP Journal on Wireless Communications and Networking 2009:1–42.

[4] Badis H. A QoS aware multicast routing protocol for multimedia applications in mobile ad hoc networks. In: Proceedings of the international symposium on modeling, analysis and simulation of wireless and mobile systems, Vancouver, British Columbia, Canada, 2008a. p. 244–51.

[5] Badis H. A QoS aware multicast overlay spanning tree protocol for multimedia applications in MANETs. In: Proceedings of the international telecommunication networking workshop on QoS in multiservice IP networks (IT-NEWS), Venice, Italy, 2008b. p. 242–7.

[6] Bheemarjuna Reddy T, Karthigeyan I, Manoj BS, Siva Ram Murthy C. Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. Ad Hoc Networks 2006;4:83–124.

[7] Biradar RC, Manvi SS. A reliable bandwidth delay product based multicast routing scheme in MANET. In: Proceedings of the international conference on advances in communication, network and computing (CNC 2010), Calicut, India, October 2010. p. 70–4.

[8] Biradar RC, Manvi SS. Agent-driven backbone ring-based reliable multicast routing in mobile ad hoc networks. IET Communications 2011a;5(2): 172–89.[9] Biradar RC, Manvi SS. Reliable neighbor based multipath multicast routing in MANETs. In: Proceedings of the first international conference on computer science and information technology CCSIT 2011, Communications in computer and information science. Lecture notes in computer science, vol. 132. Banga- lore, India; January 2–4, 2011b. p. 33–43.

[10] Biradar RC, Manvi SS. Ring mesh based multicast routing scheme in MANET using bandwidth delay product. Wireless Personal Communications, in press. dui: 10. 1007/s11277-011-0329-0.

[11] Biradar RC, Manvi SS, Reddy M. Link stability based multicast routing scheme in MANET. Elsevier, Computer Networks 2010;54:1183–96.

[12] Biswas J, Barai M, Nandy SK. Efficient hybrid multicast routing protocol for ad-hoc wireless networks. In: Proceedings of the annual IEEE international conference on local computer networks (LCN), Bonn, Germany, 2004. p. 180–7.

[13] Bommaiah E, Liu M, McAuley A, Talpade R. AMRoute: ad-hoc multicast routing protocol. Internet Draft; 1998.

[14] Chen L, Heinzelman W. QoS-aware routing based on bandwidth estimation for mobile ad hoc networks. IEEE Journal SeleIEEE Journal Selected Areas in Communication 2005;23(3):561–72.

[15] Biradar Rajashekhar C. "Mobile and Ad hoc network In Multicast Routing Protocols" journal of Network and computer applications 35 (2012) 221-239

ENHANCED ENERGY EFFICIENT POSITION BASED ROUTING PROTOCOL FOR MOBILE AD HOC NETWORK

Dr. Tanu preet Singh
HOD Department of Electronics & Communication, ACET Amritsar
tanupreet.singh@gmail.com
Er. Harwant Singh Gill
Department of Computer Applications, GIMET Amritsar, Punjab
harwantgill@gmail.com

Abstract*— MANET is a collection of mobile nodes interacting and transferring data with each other to route a packet from the original source to their final destinations. A MANET is used to support dynamic routing techniques in absence of fixed or wired infrastructure and centralized control. In this types of networks, less power in mobile communication nodes is a big matter of concern. So energy efficient techniques should be implemented with existing routing protocols to reduce link network failure and improve network lifetime and performance . This paper is presenting an Enhanced Energy-Efficient Position Based Routing protocol. The protocol deals with various parameters as Residual Energy, Bandwidth, Load and Hop Count for route discovery. It will improve the utilization of link on the basis of combining residual energy at each node and number of hops in a particular route.

***Keywords*— Load, Residual Energy, Bandwidth, Hop Count.**

1. Introduction

Mobile ad hoc networks (MANETs) are composed of a set of mobile nodes which can move anywhere freely and communicate with each other using a wireless data transfer medium .So, limited energy capacity, absence of fixed infrastructure, dynamic topology and unstable links are special features for MANET when compared to other wired networks. MANET does not have centralized controllers, which makes it different from other wireless networks [1].

The topology of mobile ad-hoc network is dynamic and depends upon the movement of the nodes. Mobile ad-hoc networks have to suffer many challenges at the time of routing. The nodes in the MANET are battery operated. Failure of some nodes operation can greatly impede performance of the network and even affect the basic availability of the network, i.e., routing. The movement pattern, location, direction of movement, pause distribution, speeds and acceleration change over time of the mobile nodes can be described by their mobility models. Some of the mobility models are :

1) Random Waypoint Mobility Model
2) Random Walk Mobility Model
3) Random Direction Mobility Model

The random waypoint mobility model introduces specific pause times between movements i.e. changes in direction and speed. The random waypoint model [3] is the most popular mobility model employed in contemporary research, and can be considered a foundation for building other mobility models. In this work, random way point mobility model is used the random walk mobility model is the simplest mobility model, generating completely random movement patterns. It was designed for simulations in which the movement patterns of mobile nodes are completely unpredictable. In Random Direction Mobility Model, mobile nodes using the Random Waypoint Mobility Model often choose new destinations, and the probability of choosing a new destination that is located in the centre of the simulation area, or requires travel through the middle of the simulation area, is high[4].

MANET can be used in several areas. Some of them are: wireless mesh networks, wireless sensor network, military applications, hybrid wireless network architectures,

collaborative and distributed computing, emergency operations[2].

Unlike other routing protocols, our protocol uses no periodic routing overhead messages, so by reducing bandwidth of network; it uses dynamic source routing to route packets in an adhoc network. According to source routing technique the source node determines the entire sequence of nodes through which a packet has to pass from source to destination. The source node puts the list of addresses of all the intermediate nodes in the header of the packet, so that the packet is reached at destination through those specified nodes. Source routing is done using a technique called route discovery. Whenever a node want to send a packet to some other node, the sending node initiates the route discovery. Each node maintains a cache called route cache to store the information about all routes it has gathered to different destinations. To support efficient routing in energy constrained ad hoc networks, power aware routing policies can be integrated and evaluated with existing features of routing protocol.[5]

2. Classification of Routing Protocols

Classification of routing protocols in mobile ad hoc network can be categorized in many ways, but most of these are considered on the basis of routing strategy and network structure [6][7][8]. The routing protocols can be categorized as flat routing protocol, hierarchical routing protocol and position assisted routing protocol while depending on the type of network structure. Flat routing protocols are divided into two types; the first type is proactive routing (table driven) protocols and second type is reactive (on-demand) routing protocols. Proactive routing is mostly based on link-state while on-demand routing is based on distance-vector. proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently. Examples of proactive routing protocols are:

A) Destination-Sequenced Distance Vector (DSDV)
B) Fish Eye State Routing (FSR)
C) Optimized Link State Routing

Reactive routing protocols were intended for these types of environments where mobility of the nodes leads the topology of the network to change regularly. Reactive protocols set routes for data transfer on-demand. The routing protocol establish a route, whenever a node wants to start communication with another node to which it has no any route. Types of reactive protocols are:

A) Ad hoc on Demand Distance Vector Routing (AODV)
B) Dynamic Source Routing (DSR)
C) Temporally Ordered Routing Protocol (TORA)

3. Existing and Related Work

The routing mechanism basically involves two activities first, to find optimal routing routes and secondly, transferring data packets through network. There are various Energy-Efficient routing protocols which deal with this technique but in this paper DSR is used as base protocol. The DSR protocol is a type of reactive routing protocol for MANET. It uses source routing which means that the sender must know the complete hop-by hop route sequence to the destination node. These all routes are stored in a route cache. DSR is composed of two passes that work together to perform the route discovery and route maintenance of source routes in the ad hoc network. When a node in an ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery mechanism to dynamically find such a route. Route discovery works by flooding the network with route request RREQ packets. Each node that receive a request rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the request with a route reply RREP packet that is routed back to the original source. Route request and reply packets are also source routed. The request builds up the path traversed so far. The reply routes itself back to the source by traversing this path backward. The route carried back by the reply packet is cached at the source for future use. If any link on a source route is broken detected by the failure of an attempted data transmission over a link, route error RERR packet is generated. Route error packet is sent back toward the sender which erases all entries in the route caches along the path that contains the broken link. A new route discovery must be initiated by the source, if this route is still needed and no alternate route is found in the cache. But sometimes an alternative path is selected from already available routes if source still want to interact with destination and another path should not have that error causing node. Route Maintenance is performed by each node that originates or forwards a data packet along a source route. Each such node is responsible for confirming that the packet has been received by the next hop along the source route given in the packet; the packet is retransmitted until this confirmation of receipt is received.. A DSR is able to learn routes by overhearing packets not addressed to it using promiscuous mode. DSR-PR disabling the interfaces addresses by filtering and causing the network protocol to receive all packets that the interface overhears. These packets are scanned for useful source routes or Error messages and then discarded [4].

3.1 Energy Efficient Position Based Routing Protocol

This approach selects a route that contains nodes having maximum available residual energy so that the energy usage among all nodes can be balanced because underutilized nodes

usually have more energy than utilized nodes. The approach compares not only energy but all the parameters such as bandwidth, load and hop Count for the route selection so this may result in small, best and energy-rich routes for routing packets. Thus, ensures long network lifetime. [5]

In this protocol the method of broadcasting the RREQ packet for Route Discovery is same as the DSR, only the difference is in the RREQ packet format.
The intermediate node which receives the RREQ packet performs the following task:

1) It checks in its Route Cache for the availability of a route for the destination node, if it found then it attach that route in a RREP packet and sends back to the source node.

2) If the node finds its own address as actual destination, then the packet reached the final target.

3) Otherwise, that node appends its own address in that Route Record and its available residual energy in RREQ and rebroadcasts it to all its neighbor nodes.

All the routes are defined along with number of intermediate nodes from source to destination called hop count. Then minimum value of all parameters like hop count, bandwidth, residual energy and load is calculated. Then position count is calculated in final position table on the basis of next mentioned four rules. A specific route is selected having minimum value of position count. That specific route will be best suitable from all aspects like having maximum available residual energy and bandwidth etc.

The best route is selected on the basis of following rule set on the basis of minimum value of all parameters [5]:

Rule 1: If two or more than two routes have equivalent energy
Then
Route with maximum available bandwidth will be accepted.

Rule 2: If two or more than two routes are of same energy and equivalent bandwidth:
Then
Route having minimum Load will be considered.

Rule 3: If two or more than two routes have equivalent energy, equivalent bandwidth and equal load also
Then
Route with minimum hop count value is considered

Rule 4: If all the available routes are not of equal energy:
Then
Route with maximum residual energy, maximum bandwidth, minimum load and minimum hop count should be given priority. The preference order for selecting optimal route is as follows [5].

Energy > Bandwidth > Load > Hop Count

One best route having minimum value of position count is considered and all other remaining routes are taken as backup and used later on in case of failure of transmission of data packets in first best route

4. Enhanced Energy Efficient Position Based Routing Protocol

The selection of best route from all available routes is dependent upon given rule set. In enhanced energy efficient position based routing protocol while selecting a route instead of using energy first rule [5] a combination of residual energy and hop count is used. This will increase the overall energy of network and improve lifetime of network. If a route is selected according to old rule set then hop count is considered at last. A route having maximum available residual energy is selected that have hop count is not equal to minimum available hop count. When a packet will transfer from source to destination through intermediate nodes, for transmitting packet to final node in route cache energy of every intermediate will be consumed. So as the number of intermediate nodes will increase (hop count) the energy consumed for one transmission will also increased. So it is necessary to select a route having maximum residual energy but minimum hop count .In new proposed technique while selecting a route combination of energy first rule and minimum hop count is used. New proposed rule set is as follows:

1) If routes are of equivalent energy and equal hop count then route with maximum available bandwidth will be considered.

2) If routes are of equivalent energy, equal hop count and equal bandwidth then route with minimum load is considered.

3) If the routes are not of equivalent energy and equal hop count then route with maximum energy and minimum hop count is considered.

4) If route has equal load then select the route with maximum energy and minimum hop count.

5. Conclusion

In this paper, we presented an enhanced energy efficient position based routing protocol for MANETs with an emphasis on selecting an optimal route on the basis of combination of residual energy and hop count. If number of nodes in a route will be more then energy consumed at each intermediate node will increase the overall energy consumption of that route. But limited battery power is also a main matter of concern in MANET. So enhanced energy efficient position based routing protocol is helpful for selecting best route having minimum hop count, maximum residual, minimum load and maximum bandwidth. Due to any reason if that selected optimal route stop transferring data then another alternative route is selected from final route table that is without sinking node , if sender still want to communicate with destination. If not a such route is available in final route table then again RREQ packet is transmitted to all neighbor nodes as mentioned previously that find all routes to transmit data from source to destination

6. References

[1] Lijuan Cao, Teresa Dahlberg and Yu Wang, "Performance Evaluation of Energy Efficient Ad Hoc Routing Protocols", IEEE 2007.

[2] C. Siva Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks Architecture and Protocols", 2nd Edition, Pearson Education, 2005.

[3] Bor rong chen and C.Hwa Chang. Mobility impact on adhoc networks, IEEE 2003 proceedings.

[4] P. Sivasankar, C. Chellappan, S. Balaji "Optimised Energy Efficient Routing Protocols and their Performance Comparison for MANET"

[5] Supriya Srivastava, A.K. Daniel, R. Singh and J.P. Saini "Energy-Efficient Position Based Routing Protocol for Mobile Ad Hoc Networks" IEEE 2012

[6] Sonam Jain, Sandeep Sahu "Topology vs Position based Routing Protocols in Mobile Ad hoc Networks: A Survey", IJERT 2012.

[7] P. Sivasankar, C. Chellappan, S. Balaji "Optimised Energy Efficient Routing Protocols and their Performance Comparison for MANET"EJSR 2012

[8] N.Kumar, Dr.C.Suresh Gnana Dhass,"A Complete Study on Energy Efficient Routing Protocols DSR, ZRP and DSDV In Mobile Ad Hoc Networks", IJES 2012

Wi-Fi and its Security Aspects

[1]Er. Ridhima Khanna, [2]Er. SumanBala
[1,2]Assistant Professor, Computer Science & Engineering Department,
GNDU Amritsar Campus, Amritsar, Punjab (INDIA)
[1]ridhima.khanna885@yahoo.com
[2]sharma.suman027@gmail.com

Abstract
These days wireless communication is an emerging field.Although there are many advantages of wireless communications like no use of wires,fast data rate,standardization,easy deployment,etc.This paper discusses Wi-Fi introduction,itsworking,various 802.11 standards, advantages of Wi-Fi,limitations of Wi-Fi, security requirements in Wi-Fiand Wi-Fi security measures,Home wireless threats and their protection,Public wireless threats and their protection.

Keywords: Attacks, security, Wi-Fi, WEP, WPA, WPA2, wireless,Home Wireless Threats,Public Wireless Threats.

I. INTRODUCTION

Wi-Fi is a short form for wireless fidelity. Any product or service using 802.11 technologies comes under Wi-Fi.Wi-Fi networks use unlicensed 2.4 and 5 GHz radio bands. With its help, any two devices can communicate wirelessly.This is done with the help of access points. It is being used at organizational as well as personal level.It is specified from the Institute of Electrical and Electronics Engineers (IEEE).It has standards like 802.11 a,802.11 b,802.11g,802.11n and these standards use Carrier Sense Multiple Access/Collision Avoidance for path sharing[2].As it is a wireless network, it is prone to various security risks like active and passive attacks, unauthorized access, replaying, etc[8].

Figure A: Wi-Fi Logo

II. WORKING of Wi-Fi

Radio waves are used for communication purpose in Wi-Fi.It is a two-way radio communication:-

1. Data is translated into radio signal by computer's wireless adapter and an antenna transmits it.

2. The signal is received by a wireless router and decoding is done by it.The information is sent to the internet by the router through a physical, wired Ethernet connection.

When the router receives information from the internet, the process works in reverse. Therouter translates into radio signal and sends it to the computer's wireless adapter.

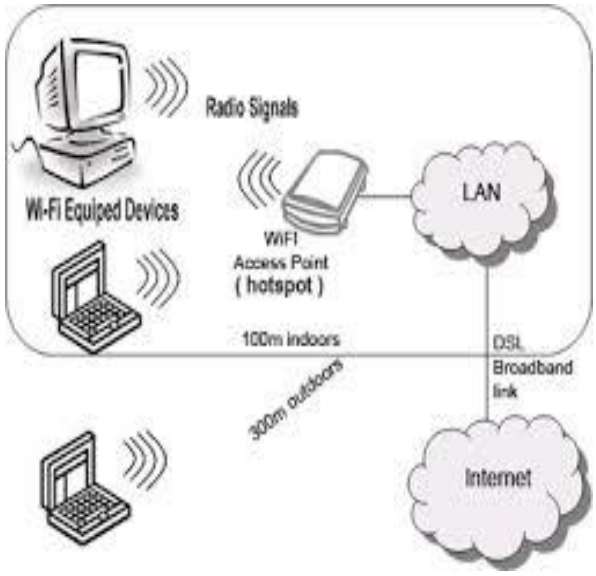


Figure B: Wi-Fi Working

III. VARIOUS 802.11 STANDARDS

Various 802.11 standards are compared in the following table:-

	802.11b	802.11g	802.11 a	802.11 n
IEEE Ratified	1999	2001	1998	2008
Frequency(GHz)	2.4	2.4	5	2.4 &5
Non-Overlapping channels	3	3	12	3 & 12
Baseline bandwidth per channel(Mbps)	11	54	54	65 &65
Number of	1	1	1	2,3* or

spatial streams				4* & 2,3*,4*
Channel Bonding	No	No	No	No & Yes
Max Bandwidth per channel	11	54	54	130 & 270

Table A: Comparison between 802.11 Standards

IV. ADVANTAGES OF Wi-Fi

The various advantages of Wi-Fi have been discussed below:-

A. No use of Wires

It does not make use of wires as it is a wireless medium .It can merge together multiple devices.

B.Easy deployment

It is easy and fast to deploy. It can be deployed in areas where wires cannot run.

C.Fast Data transfer rates

It has fast data transfer rates.

D. Standardized

It allows you to connect to the network in any country, although there are still little features of its application.

V. LIMITATIONS OF Wi-Fi

The various limitations of Wi-Fi have been discussed below:-

A. No physical protection

As there is no physical medium is present in it, so it is more prone to attacks like eavesdropping, replaying, etc.

B. Broadcast communication

Due to the broadcast nature of communication, signals can be overheard.

C.Passive and Active attacks

Passive Attacks

In this, the communication between two parties is monitored or listened by an unauthorized attacker.

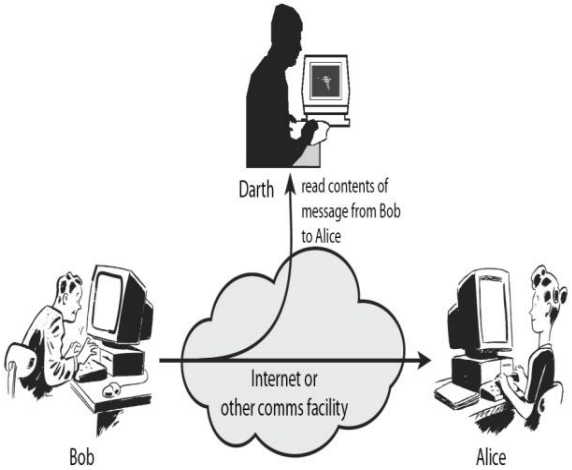


Figure C: Passive Attacks

Active Attacks

In this, unauthorized change of system is attempted. It includes masquerading, denial of service, messagereplaying, etc.

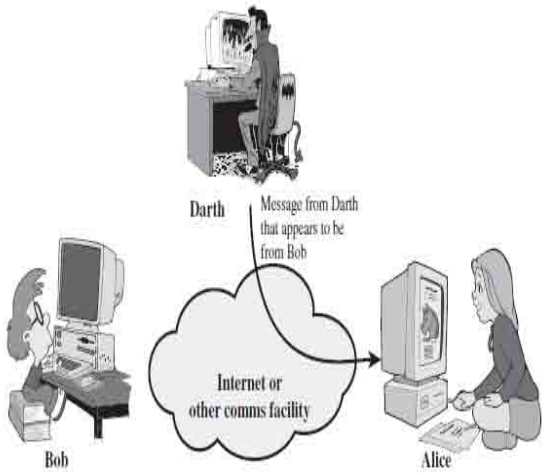


Figure D: Active Attacks

D.High Power Consumption

It uses high power making battery life a concern.

VI. SECURITY REQUIREMENTS FOR Wi-Fi COMMUNICATION

A. Confidentiality

In this, information is protected from disclosure to unauthorized parties.

B.Authenticity

In this, identity of an individual is verified.

C.Integrity

In this, information cannot be modified by unauthorized parties.

D.Access Control

Access to network services should be provided to only legitimate users[11].

VII. Wi-Fi Security Measures

A. SSID hiding

In this,the Service Set Identifier (SSID) is hided but it is an ineffective method as it provides little protection against intrusion efforts.

B.MAC ID Filtering

In this,access is allowed from known,pre-approved MAC addresses.The MAC address of an authorized client can be snipped by an attacker and the attacker can spoof this address.In order to prevent accidental associations from ignorant bystanders,it is used.

IP addresses are provided to clients via DHCP(Dynamic Host Configuration Protocol) by the wireless access points.In this,clients set their own addresses which make it difficult to a casual intruder to log into a network but little protection is provided for a sophisticated intruder [10].

C.Wired Equivalent Privacy(WEP)

It was developed by IEEE in 1997 in order to provide data confidentiality comparable to that of traditional wired network.It makes use of RC-4 encryption which is simple,fast and easy to implement in cheap hardware.It suffers from numerous flaws and is no longer secure.

D.Wi-Fi Protected ACCESS(WPA)

It became available in 2003.In order to access WEP vulnerabilities,WPA was designed.It uses temporal key integrity protocol(TKIP).WPA is supported by a WEP compatible hardware.In this,drivers are updated.Although it is more secure than WEP,it has known vulnerabilities.

E.WPA-2

It was introduced in 2004.It is more secure than WPA and it uses AES(Advanced Encryption standard).It is supported by most new Wi-Fi-devices.It is fully compatible with WPA.It is used for IEEE 802.11i standard [7].

F.Wi-Fi Protected Setup

In 2007, a flaw in a feature was added to Wi-Fi called Wi-Fi protected setup.In this,in many situations,it allows WPA and WPA-2 security to be bypassed and effectively broken in many situations.The possiblesolution of this as developed in late 2011 isto turnoff Wi-Fi Protected Setup which is not always possible [4].

G. Keep your AP firmware up-to-date

Vendors usually release a patch to fix the problem whenever vulnerability in the AP software is discovered.

H.Enable secure guest Wi-Fi access

Before giving them guest access, have a system in place to authenticate users. If guest access over Open Wi-Fi, use higher layer security such as secure socket layer (SSL) used in HTTPS to securely authenticate users and avoid leakage of credentials.

I.Promote endpoint security practices

Promote awareness among end users to follow wireless endpoint security practices such as: keeping their Wi-Fi driver software up-to-date, using virtual private network (VPN) over Open Wi-Fi hotspots, disable the ad-hoc connection mode, etc.

JConduct Wi-Fi security audits regularly

Detect presence of unauthorized devices and activity in your premises by scanning the airspace in and around your premises to avoid gaps in your Wi-Fi security posture and regulatory compliance.

K*Consider use of a WIPS for 24x7 monitoring and complete protection*

WIPS can also be repurposed as a cost-effective solution for conducting Wi-Fi security audits for regulatory compliance. A wireless intrusion prevention system (WIPS) provides comprehensive protection against all kinds of wireless threats including unmanaged devices (e.g., Rogue APs).

VIII. WEP,WPA AND WPA-2 – A COMPARISON

The comparison between these three is presented in the form of table below:-

	WEP	WPA	WPA2
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authenticati on	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity Code (MIC))	Cipher block chaining message authentication code (CBC-MAC)

Key Management	Lack of key management	Provides robust key management and keys are generated through four way handshake.	Provides robust key management and keys are generated through four way handshake.
Hardware Compatibility	Works on existing hardware	Works on existing hardware through firmware upgrades on NIC	Supported in Wi-Fi devices certified since 2006, Does not work with older NIC
Attacks/ Vulnerabilities	Chopchop, Bittau's fragmentation, FMS and PTW attack, DoS attacks	Chopchop, Ohigashi-Morii, WPA-PSK, Beck-Tews and Michael Reset Attack and Hole 196 vulnerability, DoS attacks	Hole 196 vulnerability, DoS attacks due to unencrypted management and control frames, MAC address spoofing due to Deauthentication, Offline dictionary attacks in WPA2-Personal
Deployment complexity	Easy to setup and configure	Complicated setup required for WPA-enterprise	Complicated setup required for WPA2-enterprise
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	48 bit packet number prevents replay attacks

Table B:Comparison of WEP,WPA and WPA2

IX. HOME WIRELESS THREATS AND THEIR PROTECTION

Home Wireless Threats

Some of the home wireless threats are:-

A.Piggybacking

Anyone with a wireless-enabled computer within range of your wireless access point can hop a on the internet over your wireless connection, If you fail to secure your wireless network. Failure to secure your wireless network can lead to following problems:-

• Service violations: The limit provided by internet service provider could be exceeded.

• Bandwidth shortages: Users piggybacking on your internet connection might slow your connection by using the bandwidth.

• Abuse by malicious users: It can be used by malicious users.

• Monitoring of your activity: Your passwords and other important information can be steeled.

• Direct attack on your computer: Your files can be accessed and computer systems can be hacked.

B.War driving

War driving is a specific kind of piggybacking. Savvy computer users know about your internet connections in the street, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna— searching for unsecured wireless networks. This practice is nicknamed "war driving." They can put this information on websites.Soto mask their identities, they can perform illegal actions on your connections.

Protecting Home Wireless

Following ways can be used to protect from the home wireless threats:-

A. Make Your Wireless Network Invisible

Wireless access points can announce their presence to wireless-enabled computers. This is referred to as "identifier broadcasting."You need to make your network invisible.

B.Rename Your Wireless Network

SSID name need to be changed in order to make our network unguessable to others.

C.Encrypt Your Network Traffic

By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.

D.Use File Sharing with Caution

Any file which needs to be shared should be password protected,

E.Keep Your Access Point Software Patched and Up to Date

Manufacturer's web site should be regularly checked for any updates or patches for your device's software.

F.Check Your Internet Provider's Wireless Security Options

Check the customer support area of your provider's web site or contact your provider's customer support group.

X. PUBLIC WIRELESS THREATS AND THEIR PROTECTION

Public Wireless Threats

These are discussed below:-

A.Evil Twin Attacks

In an evil twin attack, information about a public access point is gathered by an attacker, and thenhe/she sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the bogus signals.

B.Wireless Sniffing

Malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers as your connection is being transmitted "in the clear".

C.Peer-to-Peer Connections

An ad-hoc network is created between two computer systems.Unauthorized access to your sensitive files can be gained byan attacker with a network card configured for ad hoc mode and usingthe same settings as your computer.

D.Unauthorized Computer Access

A malicious user could access any directories and files you have allowed for sharing.

E.Shoulder Surfing

If close enough, they can simply glance over your shoulder as you type or they could be peering through binoculars from an apartment window across the street. They steal your personal information by simply watching you.

Safe Wireless Networking in Public Spaces

It can be done in following ways:-

A.Watch What You Do Online

Use VPN, otherwise avoid

- Online banking
- Online shopping
- Sending email
- Typing passwords or credit card numbers

B.Connect Using a VPN

Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted.

C.Disable File Sharing

To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point.

D.Be Aware of Your Surroundings

You need to be bewaring of your surroundings and connect to the internet only if required.

XI. CONCLUSION

It is a cost-effective way to connect to the internet but there are some security issues which need to be addressed. In this paper, Wi-Fi working, itsstandards, itslimitations, security requirements in Wi-Fi communication, Wi-Fi security measures, comparison between WEP,WPA and WPA-2,home wireless threats and its protection and public wireless threats and its protection have been discussed.

REFERENCES

[1] Arash Habibi Lashkari, Masood Mansoori, Amir Seyed Danesh, ―Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)‖, in ICCDA Singapore Conference, 2009.

[2] Frank H. Katz, ―WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?‖ in 2010 4th Annual Computer Security Conference (CSC 2010), April 15-16, 2010, Coastal Carolina University, Myrtle Beach, SC.

[3]Lehembre, Guillaume. ―Wi-Fi security –WEP, WPA and WPA2‖, Article published in number 1/2006 (14) of hakin9 Publication on www.hsc.fr

[4]K. Benton, ―The evolution of 802.11 wireless security‖, INF 795, April 18th, 2010. UNLV Informatics-Spring 2010

[5]Yang Xiao*,Chaitanya Bandela,Xiaojiang (James) Du,Yi Pan,Edilbert Kamal Dass,Int. J. Wireless and Mobile Computing, Vol. 1, Nos. 3/4.

[6] "The six dumbest ways to secure a wireless LAN", George Ou, ZDNet.

[7] "Understanding WEP Weaknesses". Wiley Publishing. Retrieved 2010-01-10.

[8]Viehbock, Stefan (26 December 2011). "Brute forcing Wi-Fi Protected Setup".

[9] "Network Security Tips". Cisco. Retrieved 2011-04-19.

[10]"Weaknesses in the Key Scheduling Algorithm of RC4" by Fluhrer, Mantin and Shamir.

[11]"FBI Teaches Lesson In How To Break Into Wi-Fi Networks", informationweek.com

A review paper on blackhole attack and its countermeasures on AODV Protocol

Er. Pooja rani ,AP RBU (poojashrm27@gmail.com)

Navjot , M.tech student(navjot.bedi62@gmail.com)

Abstract*—Network Wireless attack is one of the serious routing attacks amongst all the network layer attacks launched on MANET. Wormhole attack is launched by creation of tunnels and it leads to total disruption of the routing paths on MANET. In this paper, MLDW - a multilayered Intrusion Detection Prevention System approach is studied to detect and isolate wormhole attack on MANET. The routing protocol used is Adhoc On Demand Distance Vector (AODV).As the black holes refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. MLDW has a layered framework consisting of link latency estimator, intermediate neighbor node discovery mechanism, packet drop calculator, node energy degrade estimator followed by isolation technique.

***Keywords*—**

I. INTRODUCTION

All communications in MANETs take place over the wireless medium. The wireless channels are open, shared and with relatively less power. First, due to the "open" nature of wireless medium, the wireless communication in MANETs is susceptible to eavesdropping that may lead to critical information leakage. The requirement of promiscuous mode raised by many MANET protocols, i.e. continuous monitoring of the shared medium, further facilitates the practicality of eavesdropping. Additionally, wireless transmissions can be intercepted. Once capturing ongoing transmission, adversaries with sufficient knowledge of MANET protocols can meaningfully perform various malicious behaviors. Some typical examples are: alter key information in packets, discard and/or forge messages, inject malicious messages, generate floods of spurious messages, and replay control and data traffic. Such misbehaviors have severe impact on MANETs. For example, MANET routing process requires all nodes dutifully participate in forwarding packets and provide valid routing information. Adversaries who perform either of above malicious behaviors' can ruin the routing functionality [1] and [3]. By supportive infrastructure, we mean entities (or authorities) that perform administrative and management functionalities in MANETs. In a pure at MANET, there is no particular node that is designated as a central authority to execute administrative and management functionalities. Instead, all network operations, including security related control, are on the self-configuration base and in a decentralized way. Whether the security control (e.g., authentication and authorization) or not can be achieved heavily relies on the cooperation of network nodes. However, in the fully distributed and open environment of ad hoc networking, nodes trustworthy are fairly difficult to identify. This provides possible opportunities for misbehaving nodes to harm the security control operation. Meanwhile, the absence of administrative or domain boundaries make the enforcement of any security measures an even more complex problem. In this paper we discussed a survey of performance based secure routing protocol techniques in MANET.

(A)Advantages of manet -

1.Mobility- With the emergence of public wireless network, users can access internet even outside their working environment.[2]

2.Convenience- The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment. [2]

3.Expandibility- Ad-hoc networks can serve suddenly increased number of clients without affecting the existing equipment.[2]

4.Rapid set-up time- Ad hoc network requires the installation of radio NICs in the user devices.[2]

(B)Applications of manet-

1.Disaster relief- Infrastructure typically breaks down in disaster areas. Emergency teams can relay on infrastructure that they can set themselves.[3]

2.Military battlefield- Ad hoc network allow military to take advantage of commonplace network topology to maintain an information network between the soldiers , vehicles etc.[3]

3.Effectiveness- Services provided by existing infrastructure might be too expensive for certain application. Registration procedure might take too long, and communication overheads might be too high with existing networks. Application- tailored ad-hoc networks can offer a better solution.[3]

Routing Protocol is used to find valid routes between communicating nodes. They do not use any access points to connect to other nodes[1]. It must be able to handle high mobility of the nodes. Routing protocols can be mainly classified into 3 categories

-Centralized versus Distributed
-Static versus Adaptive
-Reactive versus Proactive
- Hybrid Routing

In centralized algorithms, all route choices are made by a central node, while in distributed algorithms, the computation of routes is shared among the network nodes. In static algorithms, the route used by source destination pairs is fixed regardless of traffic condition. It can only change in response to a node or link failure. This type of algorithm cannot achieve high throughput under a broad variety of traffic input patterns. In adaptive routing, the routes used to route between source-destination pairs may change in response to congestion.

A. Proactive (Table-Driven) Routing Protocols

In this family of protocols, nodes maintain one or more routing tables about nodes in the network. These routing protocols update the routing table information either periodically or in response to change in the network topology. The advantage of these protocols is that a source node does not need route-discovery procedures to find a route to a destination node. On the other hand the drawback of these protocols is that maintaining a consistent and up-to-date routing table requires substantial messaging overhead, which consumes bandwidth and power, and decreases throughput, especially in the case of a large number of high node mobility. There are various types of Table Driven Protocols: Destination Sequenced Distance Vector routing (DSDV), Wireless routing protocol (WRP), Fish eye State Routing protocol (FSR), Optimized Link State Routing protocol (OLSR), Cluster Gateway Switch Routing protocol (CGSR), Topology Dissemination Based on Reverse Path Forwarding (TBRPF).

B. Reactive (On-Demand) Routing Protocols

For protocols in this category there is an initialization of a route discovery mechanism by the source node to find the route to the destination node when the source node has data packets to send. When a route is found, the route maintenance is initiated to maintain this route until it is no longer required or the destination is not reachable. The advantage of these protocols is that overhead messaging is reduced. One of the drawbacks of these protocols is the delay in discovering a new route. The different types of reactive routing protocols are: Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector routing (AODV), Adhoc On-demand Multipath Distance Vector Routing Algorithm (AOMDV) and Temporally Ordered Routing Algorithm (TORA).

C. Hybrid Routing Protocols

Both of the proactive and reactive routing methods have some advantages and shortcomings. In hybrid routing a combination of proactive and reactive routing methods are used which are better than the both used in isolation. It includes the advantages of both protocols. As an example facilitate the reactive routing protocol such as AODV with some proactive features by refreshing routes of active destinations which would definitely reduce the delay and overhead so refresh interval can improve the performance of the network and node. These protocols can incorporate the facility of other protocols without compromising with its own advantages. Examples of hybrid protocols are Zone Routing Protocol, Hazy Sighted Link State[3].

D. ENERGY EFFICIENT ROUTING PROTOCOLS

A. Energy consumption model

Wireless network interface can be in one of the following four states: Transmit, Receive, Idle or Sleep. Each state represents a different level of energy consumption[2]. • Transmit: node is transmitting a frame with transmission power Ptx ; • Receive: node is receiving a frame with reception power Prx. That energy is consumed even if the frame is discarded by the node (because it was intended for another destination, or it was not correctly decoded); • Idle (listening): even when no messages are being transmitted over the medium, the nodes stay idle and keep listening the medium with P idle ; • Sleep: when the radio is turned off and the node is not capable of detecting signals. No communication is possible. The node uses P sleep that is largely smaller than any other power. The typical values of consumption for a wireless interface (measured for a Lucent Silver Wavelan PC Card) are reported. Transmit P tx = 1.3W Receive P rx = 0.9W Idle P idle = 0.74W Sleep P sleep = 0.047W The energy dissipated in transmitting (Etx) or receiving (Erx) one packet can be calculated as: Etx =Ptx X Duration Erx =Prx X Duration (1) Where Duration denotes the transmission duration of the packet. When a transmitter transmits a packet to the next hop, because of the shared nature of wireless medium, all its neighbours receive this packet even it is intended to only one of them. Moreover, each node situated between transmitter range and interference range receives this packet but it cannot decode it. These two problems generate loss of energy. Energy is a limiting factor in case of Ad-hoc networks. Energy efficient routing protocols are the only solution to above situation. Most of the work of making protocols energy efficient has been done on "on demand routing protocols" because these protocols are more energy efficient rather than proactive protocols. Energy efficiency can also be achieved by sensible flooding at the route discovery process in reactive protocols. And energy efficiency can also be achieved by using efficient metric for route selection such as cost function, node energy, battery level etc. Here energy efficiency doesn‟t mean only the less power consumption here it means increasing the time duration in which any network maintains certain performance level. We can achieve the state of energy efficient routing by increasing the network lifetime and performance.

II. ROUTING ATTACKS IN MANET

Routing protocols (Network layer protocols) extend connectivity from neighboring 1-hops nodes to all other nodes in MANET. The connectivity between mobile hosts over a potentially multi-hop wireless link strongly relies on cooperative reactions among all network nodes. A variety of attacks targeting the network layer have been identified and heavily studied in research papers. By attacking the routing protocols, attackers can absorb network traffic; inject themselves into the path between the source and destination,

and thus control the network traffic flow, as shown in Figure 1 (a) and (b), where a malicious node M can inject itself into the routing path between sender S and receiver D. The traffic packets could be forwarded to a non optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a nonexistent path and get lost. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation.

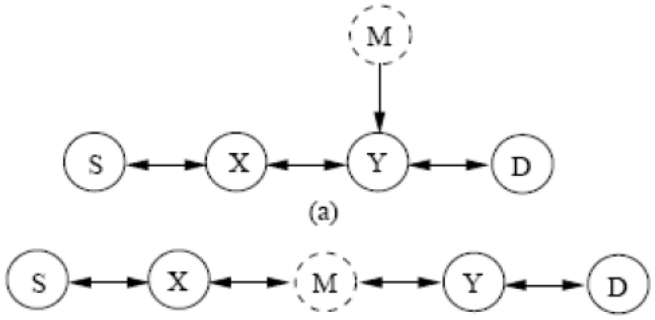


Fig 1 Illustration of Routing Attack

Attacks at the routing maintenance phase:

There are attacks that target the route maintenance phase by broadcasting false control messages, such as link-broken error messages, which cause the invocation of the costly route maintenance or repairing operation. For example, AODV and DSR implement path maintenance procedures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the upstream node of the broken link broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. Attackers could take advantage of this mechanism to launch attacks by sending false route error messages.

Attacks at data forwarding phase

Some attacks also target data packet forwarding functionality in the network layer. In this scenario the malicious nodes participate cooperatively in the routing protocol routing discovery and maintenance phases, but in the data forwarding phase they do not forward data packets consistently according to the routing table. Malicious nodes simply drop data Packets quietly, modify data content, replay, or flood data packets; they can also delay forwarding time sensitive data packets selectively or inject junk packets.

III. SURVEY OF SECURE ROUTING TECHNIQUES

Trust Based Secure Routing in AODV Routing Protocol

A.Menaka Pushpa et. al. introduced a perfect trust model in the network layer, and established secure route between source and destination without any intruders or malicious nodes. In this paper, existing AODV routing protocol has been modified in order to adapt the trust based communication feature. Proposed trust based routing protocol is equally concentrates both in node trust and route trust. In this proposed model, route trust plays an equal role with node trust. Using trust value, secure route can be established in the MANET. Here, network security enhancement is completely performed in the lime light of trust value. In the dynamic environment, node can change its characteristics at any time. After successful participation in the route establishment process, the neighbor may behave like as a malicious node. To avoid this, route trust process (one of the process in the modified protocol) continuously monitor the active routes and calculate the current route trust value or the status of the route. But most of the previous works have been concentrated only in the node trust for establishing communication. This paper explains three main operations; Node trust calculation, Route trust calculation and Trust based route establishment and route monitoring process. This model requires some adequate changes in the existing source initiated routing protocol, AODV. Modified AODV routing protocol establishes route among nodes based on the trust value.

DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation Wenchao Huang, Yan Xiong, Depin Chen et. al. proposed a novel secure routing protocol DAAODV which is based on Ad-hoc On-demand Distance Vector routing (AODV). DAAODV takes full advantage of trusted computing technology, particularly the Direct Anonymous Attestation (DAA) and Property-based Attestation (PBA) protocols. DAAODV is an anonymous protocol without requirement of Trusted Third Party (TTP). Moreover, we propose an efficient signing and verification scheme to overcome the potential DoS attacks triggered by the low efficiency of DAA and PBA. In the simulation, the results show that DAAODV is still efficient in discovering secure routes compared with AODV protocol. In this paper, based on AODV and proposed a novel secure ad hoc routing protocol DAAODV which is anonymous and avoids TTP, and prevents from malicious nodes and selfish nodes. The basic idea is to use Direct Anonymous Attestation (DAA) to accomplish full anonymity in the routing protocol and use issuer instead of TTP, and to use property based attestation (PBA) to guarantee that only nodes whose platform is trusted can join the group. The main challenge of implementing this protocol is the cost of DAA and PBA protocol is a little high, so we choose an efficient DAA protocol and propose a new light weighted signing and verifying protocol to ease the problem. Experiments proves that it is still very efficient compared with AODV protocol.

AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security

Cuirong Wang, Shuxin Cai et. al. proposed a secure routing protocol based on multipath routing technology, namely AODVsec, which divides a data unit into several data pieces and transmits these pieces through different paths. By setting security level on each node, AODVsec limits the maximum number of data pieces an intermediate node can forward. In this way, the malicious node cannot get enough data information for breaking the encryption algorithm. Simulation results show that AODVsec improves security with negligible

routing overhead by comparison of the traditional multipath AODV routing protocols.

IV. CONCLUSION

In this research paper an efficient approach for the detection of the Black hole attack in the Mobile Ad Hoc Networks on AODV routing protocol is proposed. The beauty of this algorithm is that it can detects the black hole nodes in both of the cases when a node is not idle and when node is idle(i.e., there is no communication for a defined interval). And it detects the single Black hole node and cooperative Black hole nodes.

These two implementations made the approach very secure and efficient. The comparison graphs show the results in both the cases, i.e., when there are more than one attacker nodes and when there are only one attacker node.

As the future work, this algorithm can be implemented for some other dangerous network layer attacks such as Grey hole or Wormhole attack etc.

V. REFERENCES

[1] A.Menaka Pushpa, "Trust Based Secure Routing in AODV Routing Protocol", IEEE 2009.

[2] Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", 2009 International Conference on Computational Science and Engineering, IEEE 2009, pp. 809-916.

[3] Cuirong Wang, Shuxin Cai, and Rui Li, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", 2009 International Conference on Multimedia Information Networking and Security, IEEE 2009, pp. 401-404.

[4] Zeyad M. Alfawaer and Saleem Al_zoubi, "A proposed Security subsystem for Ad Hoc Wireless Networks", 2009 International Forum on Computer Science-Technology and Applications, IEEE Computer Society 2009, pp. 253-255.

[5] Muhammad Naeemv, Zah ir Ahmed, Rashid Mahmood, and Muhammad Ajmal Azad, "QOS Based Performance Evaluation of Secure On-Demand Routing Protocols for MANET's", 2010 IEEE, ICWCSC 2010X.

[6] Preeti Bhati, Rinki Chauhan and R K Rathy, "An Efficient Agent-Based AODV Routing Protocol in MANET", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 7 July 2011, pp. 2668-2673.

[7] Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009, pp. 449-460.

[8] D. Suganya Devi and Dr. G.Padmavathi, "IMPACT OF MOBILITY FOR QOS BASED SECURE MANET", International journal on applications of graph theory in wireless ad hoc networks and sensor networks, pp. 46-57.

A review paper on blackhole attack and its countermeasures on DSR Protocol

Er. Pooja rani ,AP RBU (poojashrm27@gmail.com)

Prabhjot, M.tech student(prabhjot.bedi62@gmail.com)

Abstract*—Ad hoc network maximize the total network throughput by using all available nodes for routing and forwarding. MANETs are highly vulnerable to attacks than wired networks due to the open medium, dynamically changing network topology, cooperative algorithms, and lack of centralized monitoring. Hence, a node can misbehave and fail to establish route or route the data due to its malicious activity to decrease the performance of ad hoc network. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. This paper studies black hole attack impact in ad hoc networks with DSR routing protocol when the nodes are mobile. The studied routing is based on DSR and is modified with detection algorithm. It is divided into two phases: Detection before route establishment and avoidance of malicious nodes during data forwarding. The silent feature of proposed scheme is its simplicity and effectiveness in detecting malicious nodes.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration [1]. MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes [2]. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Because these networks are temporary, they can be attacked from within, due to being constructed without protection, in poor conditions. Attacks are also launched if nodes are compromised. Another issue is the node number. Hundreds/thousands of nodes might be required in a network and security measures undertaken must be efficient and cost effective for a vast network. Exchange of topological information among nodes is facilitated by routing protocols to establish routes and this is used by attackers for acts including bogus routing, incorrect forwarding, lack of error messages, restricted reply time, thereby leading to retransmission and inefficient routing[3]. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. Common attacks faced by networks include blackhole, grey hole and wormhole attacks, and IP spoofing[4]. Black hole attacks are malicious nodes that refuse to forward traffic[5]. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus such malicious insiders who may even operate in a group may use the standard security means to actually protect their attacks. These kind of malicious parties are called compromised nodes, as their actions compromise the security of the whole ad hoc network. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way, attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [6, 7]. The method how malicious node fits in the data routes varies. Figure 1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as

soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

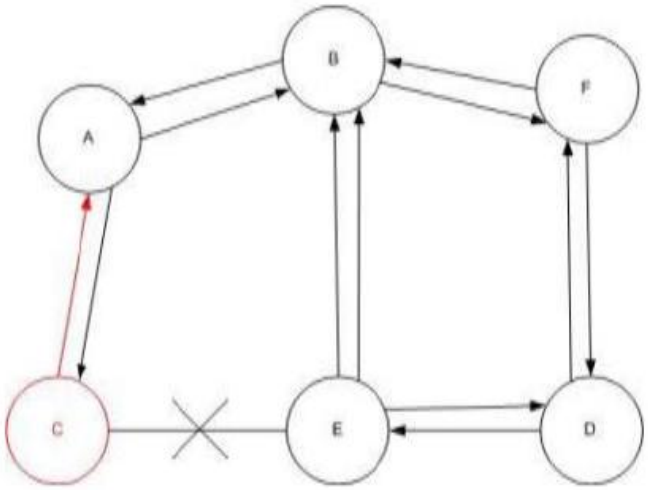


Figure 1: Black Hole Attack

(A)Advantages of manet -

1.Mobility- With the emergence of public wireless network, users can access internet even outside their working environment.[2]

2.Convenience- The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment. [2]

3.Expandibility- Ad-hoc networks can serve suddenly increased number of clients without affecting the existing equipment.[2]

4.Rapid set-up time- Ad hoc network requires the installation of radio NICs in the user devices.[2]

(B)Applications of manet-

1.Disaster relief- Infrastructure typically breaks down in disaster areas. Emergency teams can relay on infrastructure that they can set themselves.[3]

2.Military battlefield- Ad hoc network allow military to take advantage of commonplace network topology to maintain an information network between the soldiers , vehicles etc.[3]

3.Effectiveness- Services provided by existing infrastructure might be too expensive for certain application. Registration procedure might take too long, and communication overheads might be too high with existing networks. Application- tailored ad-hoc networks can offer a better solution.[3]

Routing Protocol is used to find valid routes between communicating nodes. They do not use any access points to connect to other nodes[1]. It must be able to handle high mobility of the nodes. Routing protocols can be mainly classified into 3 categories

-Centralized versus Distributed

-Static versus Adaptive

-Reactive versus Proactive

- Hybrid Routing

In centralized algorithms, all route choices are made by a central node, while in distributed algorithms, the computation of routes is shared among the network nodes. In static algorithms, the route used by source destination pairs is fixed regardless of traffic condition. It can only change in response to a node or link failure. This type of algorithm cannot achieve high throughput under a broad variety of traffic input patterns. In adaptive routing, the routes used to route between source-destination pairs may change in response to congestion.

A. Proactive (Table-Driven) Routing Protocols

In this family of protocols, nodes maintain one or more routing tables about nodes in the network. These routing protocols update the routing table information either periodically or in response to change in the network topology. The advantage of these protocols is that a source node does not need route-discovery procedures to find a route to a destination node. On the other hand the drawback of these protocols is that maintaining a consistent and up-to-date routing table requires substantial messaging overhead, which consumes bandwidth and power, and decreases throughput, especially in the case of a large number of high node mobility. There are various types of Table Driven Protocols: Destination Sequenced Distance Vector routing (DSDV), Wireless routing protocol (WRP), Fish eye State Routing protocol (FSR), Optimized Link State Routing protocol (OLSR), Cluster Gateway Switch Routing protocol (CGSR), Topology Dissemination Based on Reverse Path Forwarding (TBRPF).

B. Reactive (On-Demand) Routing Protocols

For protocols in this category there is an initialization of a route discovery mechanism by the source node to find the route to the destination node when the source node has data packets to send. When a route is found, the route maintenance is initiated to maintain this route until it is no longer required or the destination is not reachable. The advantage of these protocols is that overhead messaging is reduced. One of the drawbacks of these protocols is the delay in discovering a new route. The different types of reactive routing protocols are: Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector routing (AODV), Adhoc On-demand Multipath Distance Vector Routing Algorithm (AOMDV) and Temporally Ordered Routing Algorithm (TORA).

C. Hybrid Routing Protocols

Both of the proactive and reactive routing methods have some advantages and shortcomings. In hybrid routing a combination of proactive and reactive routing methods are used which are better than the both used in isolation. It includes the advantages of both protocols. As an example facilitate the reactive routing protocol such as AODV with some proactive features by refreshing routes of active destinations which would definitely reduce the delay and overhead so refresh interval can improve the performance of the network and node. These protocols can incorporate the facility of other protocols without compromising with its own advantages. Examples of hybrid

protocols are Zone Routing Protocol, Hazy Sighted Link State[3].

D. ENERGY EFFICIENT ROUTING PROTOCOLS

A. Energy consumption model

Wireless network interface can be in one of the following four states: Transmit, Receive, Idle or Sleep. Each state represents a different level of energy consumption[2]. • Transmit: node is transmitting a frame with transmission power Ptx ; • Receive: node is receiving a frame with reception power Prx. That energy is consumed even if the frame is discarded by the node (because it was intended for another destination, or it was not correctly decoded); • Idle (listening): even when no messages are being transmitted over the medium, the nodes stay idle and keep listening the medium with P idle ; • Sleep: when the radio is turned off and the node is not capable of detecting signals. No communication is possible. The node uses P sleep that is largely smaller than any other power. The typical values of consumption for a wireless interface (measured for a Lucent Silver Wavelan PC Card) are reported. Transmit P tx = 1.3W Receive P rx = 0.9W Idle P idle = 0.74W Sleep P sleep = 0.047W The energy dissipated in transmitting (Etx) or receiving (Erx) one packet can be calculated as: Etx =Ptx X Duration Erx =Prx X Duration (1) Where Duration denotes the transmission duration of the packet. When a transmitter transmits a packet to the next hop, because of the shared nature of wireless medium, all its neighbours receive this packet even it is intended to only one of them. Moreover, each node situated between transmitter range and interference range receives this packet but it cannot decode it. These two problems generate loss of energy. Energy is a limiting factor in case of Ad-hoc networks. Energy efficient routing protocols are the only solution to above situation. Most of the work of making protocols energy efficient has been done on "on demand routing protocols" because these protocols are more energy efficient rather than proactive protocols. Energy efficiency can also be achieved by sensible flooding at the route discovery process in reactive protocols. And energy efficiency can also be achieved by using efficient metric for route selection such as cost function, node energy, battery level etc. Here energy efficiency doesn‟t mean only the less power consumption here it means increasing the time duration in which any network maintains certain performance level. We can achieve the state of energy efficient routing by increasing the network lifetime and performance.

II. DYNAMIC SOURCE ROUTING (DSR)

The Dynamic Source Routing (DSR) protocol is an on-demand routing protocol. DSR protocol maintains the route cache to store the route to the mobile node it is aware [14, 15]. This protocol composed of two major phases: route discovery and route maintenance. Whenever any node has the data to send, first it checks the route cache for the route to the destination. If it has the unexpired route, then it use it otherwise initiate a route discovery process by broadcasting the RREQ (Route Request) packet which contains the source address and destination address. Whenever any intermediate node receives the RREQ, and it does not have the route to the destination it adds its own address in the route record and forward to its neighbor. RREP (Route Reply) is generated whenever RREQ reaches to destination node or intermediate node which has the route to destination in its route cache. Route maintenance mechanism is used to detect whether the path to the destination exist or not. Route maintenance uses the route error message and acknowledgement. Route error (RERR) message is initiated whenever the destination's data link layer recognize any transmission error. DSR is suited for small to medium sized networks as its packet overhead can scale all the way down to zero when all nodes are relatively stationary [16]. The packet data overhead will increase significantly for networks with larger hop diameters as more routing information will need to be contained in the packet headers. The DSR protocol is composed of two main mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- **Route Discovery** is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- **Route Maintenance** is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, scan attempt to use any other route it happens to know to D, or it can invoke Route Discovery again to find a new route for subsequent packets to D. Route Maintenance for this route is used only when S is actually sending packets to D.

III. BLACKHOLE ATTACK

Black hole attack is dangerous active attacks on the Mobile Ad hoc Networks. A black hole attack is performed by a single node or combination of nodes. This attacker node is also called selfish node. In Black hole attack an attacker node sends a fake Route reply (RREP) message to the source node which initiates the route discovery procedure order to find the route to the destination node. When the source node received multiple RREP, it selects the greatest one as the most recent routing information and selects the route contained in that RREP packet[5]. In case the sequence numbers are equal it selects the route with the smallest hop count. the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node. Then the attacker drops all data packets rather than forwarding them to the destination node. As shown in Figure 4 below, source node 1 broadcasts an RREQ message to discover a route for sending packets to destination

node 3. An RREQ broadcast from node 1 is received by neighboring nodes 2, 4and 5. However, malicious
node 5sends an RREP message immediately without even having a route to destination node 3. The RREP message sent by the malicious attacker node is the first message reaches to the source node .When the source node receive the message sent by the malicious attacker node, updates its routing table for the new route for the intended destination node and then also discards any RREP message from other neighboring nodes even from an actual destination node. When the Source node gets the route, it starts sending the buffered data packets immediately from that route which is provided by the malicious attacker node. Nevertheless, a Black hole node drops all data packets rather than forwarding them on.

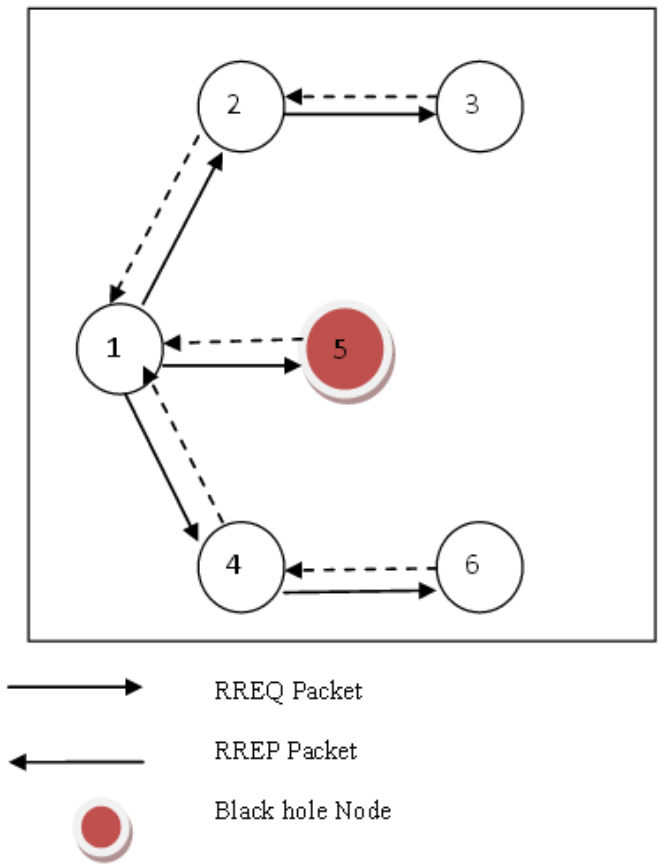


Fig 4: Example of Blackhole attack

IV. LITERATURE SURVEY

Black hole attack is one of the most dangerous attacks. Many researchers did their work on this attack and try to provide the solution for this attack. The researchers provide a lot of solution based on different technologies, concepts and terms. Some important approaches are described below:

Ramaswamy et al. [3] proposed a solution to defending against the cooperative black hole attacks. But no simulations or performance evaluations have been done. Ramaswamy et al. studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black hole nodes. In this paper, we evaluate the performance of the proposed scheme in defending against the collaborative black hole attack.

In DPRAODV [4], they have designed a novel method to detect black hole attack: DPRAODV, which isolates that malicious node from the network. The agent stores the Destination sequence number of incoming route reply packets (RREPs) in the routing table and calculates the threshold value to evaluate the dynamic
training data in every time interval as in [5].the solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. DPRAODV does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet.

P. Agrawal et al [6] proposed a technique for detecting chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc network. In this technique initially a backbone network of strong nodes (capable of tuning its antenna to short (normal) as well as to long ranges) is established over the ad hoc network. Each strong node is assumed to be a trustful one. These trustful strong nodes detect the regular nodes (having low power antenna) if they act maliciously. With the assistance of the backbone network of strong nodes, the source and the destination nodes carry out an end-to-end checking to determine whether the data packets have reached the destination or not. If the checking results in a failure then the backbone network initiates a protocol for detecting the malicious nodes. For detecting malicious node strong node associated with source node broadcast a find chain message to the network containing the id of the node replied to RREQ. On receiving find chain message strong node associated with destination node Initialize a list GrayHole Chain to contain the id of the node replied to RREQ. It then instructs all the neighbors of that node to vote for the next node to which it is forwarding packets. If the next node id is null then the node is a black hole node. Then the GrayHole removal process is terminated and a broadcast message is sent across the network to alert all other nodes about the nodes in GrayHole Chain to

be considered as malicious. Else strong node will elect the next node to which replied to RREQ is forwarding the packets based on reported reference counts. Then again broadcast the find chain message containing the id of the elected node. The main disadvantages of this algorithm are the difference between the regular node and backbone node in the network in terms of power, antenna range which makes it unsuitable for all types of mobile ad hoc network. Also it is not proved that backbone network is optimal in terms of minimality and coverage. Algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong nodes are always trusted node.

In [7] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park proposed two different approaches to solve the blackhole attack. In first proposal the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. The idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route are identified. Once a safe route has identified, these buffered packets will be transmitted. But the main drawback of this algorithm is time delay. In the second proposal every node stores the last sent packet sequence number and last received packet sequence number. When a node receives a RREP from another node it checks the last sent packet sequence number and received packet sequence number, if there is any mismatch then it generates an alarm indicating the existence of a blackhole node. But drawback of this algorithm is if the network is large, mismatch in the sequence numbers does not guarantee the existence of a blackhole node.

In [8] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch used two additional control packets for collecting the neighborhood information for detecting the blackhole node. The formats of these packets are RQNS,RPNS The basic idea of this approach is that the neighbor set difference of one node at different time instance is less than or equal to one, and the probability that the neighbor set difference of two nodes at same time instance is very small. After getting RREP from more than one node the sender sends the RQNS packet. After receiving more than one RPNS packet the sender node compare the received neighbor set, if the difference is larger than some pre defined threshold value then the current network is affected by blackhole attack. But the drawback of this approach is after comparing the neighbor set they use a cryptographic method to identify the actual infected node. This is a costly and less reliable technique in case of adhoc network.

In [9] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang proposed a distributed and cooperative procedure to detect blackhole node. First each node detects the local anomalies, then after finding the local anomalies the sender node calls for a cooperative detective by sending a message to the neighbor of the infected node. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. They use a voting scheme to identify the blackhole node. If all the nodes vote for the infected node, then the node is declared as blackhole node. The drawback of this algorithm is it cannot detect the cooperative blackhole attack and the voting scheme is complex one.

In [10], Deng et al. proposed a solution for individual black holes. But they have not considered the cooperative black hole attacks. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution can not prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply "yes" for both questions. Then the source will trust on next hop and send data through the replied node which is a black hole node.

In [11], Yin et al. proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further.

Hesiri Weerasinghe and Huirong Fu [12] simulated the algorithm proposed by [3] with several changes to improve the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the process. They also simulated AODV [17] and the solution proposed by [3] and compared them with [10].

Ramaswamy et al.	proposed a solution to defending against the cooperative black hole attacks. But no simulations or

	performance evaluations have been done. Ramaswamy et al. studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black hole nodes. In this paper, we evaluate the performance of the proposed scheme in defending against the collaborative black hole attack.
P. Agrawal et al	proposed a technique for detecting chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc network. In this technique initially a backbone network of strong nodes (capable of tuning its antenna to short (normal) as well as to long ranges) is established over the ad hoc network.
Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park	proposed two different approaches to solve the blackhole attack. In first proposal the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. The idea of this solution is to wait for the RREP packet to arrive from more than two nodes.
Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch	used two additional control packets for collecting the neighborhood information for detecting the blackhole node. The formats of these packets are RQNS,RPNS The basic idea of this approach is that the neighbor set difference of one node at different time instance is less than or equal to one, and the probability that the neighbor set difference of two nodes at same time instance is very small.
Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang	proposed a distributed and cooperative procedure to detect blackhole node. First each node detects the local anomalies, then after finding the local anomalies the sender node calls for a cooperative detective by sending a message to the neighbor of the infected node.
Deng et al.	proposed a solution for individual black holes. But they have not considered the cooperative black hole attacks. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination.
Yin et al.	proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further.
Hesiri Weerasinghe and Huirong Fu	simulated an algorithm proposed with several changes to improve the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the process. They also simulated AODV.

V. CONCLUSION

MANET networks are systems of mobile ad hoc networks which are presented dynamically and self-organized in

temporary topologies. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. The DSR routing is modified to include a Trap Header to identify malicious nodes. Experimental results demonstrate that the proposed DSR performance better than DSR in the presence of black hole attack under dynamic conditions.

VI. REFERENCES

[1] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," *IEEE Communications*, vol. 10, no. 40, October 2002, pp. 60-68. Digital Object Identifier 10.1109/MCOM.2002.1039858

[2] Bracha Hod, "Cooperative and Reliable Packet-Forwarding On top of AODV", *www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005*

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard,"Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks", www.cs.ndsu.nodak.edu/~nygard/research/BlackHoleMANET.pdf 2003

[4] Payal N. Raj, Prashant B. Swadas "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet" IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009

[5]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007

[6] Piyush Agrawal and R. K. Ghosh "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks "Proceedings of the 2nd international conference on Ubiquitous information management and communication, Suwon, Korea, ISBN: 978-1-59593-993-7, Pages: 310- 314, 2008.

[7] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04,April 2-3,2004,Huntsville,AL,USA.

[8]Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch "Detecting Black-hole Attack in Mobile Ad Hoc Network". 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495

[9]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magazines, vol. 40, no. 10, October 2002*.

[11] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", *IEEE SUTC 2006 Taiwan, 5-7 June 2006.*

[12]Hesiri Weerasinghe and Huirong Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" *International Journal of Software Engineering and Its Applications* ,pp 39-54,Vol. 2, No. 3, July 2008

[13] C.E.Perkins and E.M.Royer "Ad hoc on demand distance vector routing", *Proceedings of IEEE Workshop on Mobile computing systems and Applications 1999*, pp. 90- 100, February 1999.

[14] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness and robustness in Mobile ad hoc networks. *In proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network–based processing*, Pages 403 – 410. Canary Islands, Spain. January 2002. IEEE Computer Society.

[15] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in Mobile ad hoc networks. *In Proceedings of MOBICOM 2000.* Pages 255- 265, 2000.

[16] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, " Detection and Prevention of Blackhole Attack in MANET Using ACO", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012 21

[17] Sarita Choudhary, Kriti Sachdeva, "Discovering a Secure Path in MANET by Avoiding Black Holes", International Journal of Recent Technology and Engineering (IJRTE) SSN: 2277 - 3878, Volume - 1, Issue - 3, August 2012 .

[18] M. Umaparvathi, Dharmishtan K. Varughese, "Two Tier Secure AODV against Black Hole Attack in MANETs", European Journal of Scientific Research ISSN 1450-216X Vol.72 No.3 (2012), pp. 369-382

Lean Six Sigma Frameworks:

"An Improvement in Cycle Time"

Tannu Vats
CSE/IT Dept., ITM University
Gurgaon , India
tannuvats31@gmail.com

Ms Sujata
CSE/IT Dept., ITM University
Gurgaon , India
sujata@itmindia.edU

***Abstract*— Cycle time improvement in the project implementation is an important key process area. According to researches Lean Six Sigma approaches has been constantly used for reducing cycle time and waste from product or service to achieve quality. Lean and Six Sigma techniques are used in almost every industries and each process. This paper discusses how the Lean Six Sigma approach can be worthy for educational institutes to improve the teaching learning process. In this paper author uses both methodology/tools to improve the cycle time of the project implementation.**

Keywords - Lean, Six Sigma, Cycle Time, DMAIC.

I. INTRODUCTION

Lean Six Sigma is a managerial rule, amalgam of two methodologies: Lean and Six Sigma. Lean Six Sigma focuses on removing eight sorts of wastes/muda (transport, inventory, motion, overproduction, defects, waiting, over processing). Its focus is to rapidly attain quality from the viewpoint of the clients. Lean is about client's satisfaction. Lean evacuates waste and enhances quality, along these lines making more value according to the client with less work. While Lean concentrates on the division of 'quality included' from the 'non-value added' development and focuses on quick basic considering, Six Sigma looks to diminish process assortment by recognizing and removing the purpose behind flaws. It gives two basic tools called DMAIC (Define Measure-Analyze Identify Control) and DMADV (Define Measure-Analyze Design Verify) [3] [7].

Lean or Six Sigma separately can't achieve quality or pace. Lean Six Sigma is the combination of the two ideas: Lean is a collection of various techniques which help to reduce waste and time from the product or services and Six Sigma is about quality. So combination of these two approaches helps organization to work more effectively and efficiently.

The Lean Six Sigma concepts were first introduced in the book named Lean Six Sigma: "Combination Six Sigma with Lean Rate by Jordan George and Peter Vincent" in [2002] [3] [10]. Lean Six Sigma uses the DMAIC levels in same way as in Six Sigma but with adding some value. Lean Six Sigma has number of tools. Some tools used frequently but not all of them are proved to be as worthy as others. The DMAIC toolkit of Lean Six Sigma comprises most of the Lean and Six Sigma tools. DMAIC toolkit involves various tools like 5S tool, Project Charter, Process Analysis and Value Stream Mapping etc. The 5s tool is a basic yet compelling tools to diminishing diversions in the working environment [3] [7] [10]. The tools decidedly influence deceivability of a methodology, security, and specialist execution. The Value Stream Map was firstly introduced by Toyota Motor Co. This mapping tool is used as many other tools but the main use of this tool is to remove waste and improve the cycle time [10] [11].

II. LEAN SOFTWARE DEVELEOPMENT

Lean concept was firstly introduced in 1980's by a research team headed by the Jim Womack, Ph.D., at MIT's International Motor Vehicle Program [3]. Earlier Lean methodology was used for the manufacturing industries but now Lean can be applied in almost every business and every process. Lean is a method of acting and thinking for entire organization [9] [11].

The core idea is to amplify client's value worth while minimizing waste. Basically, Lean means making more esteem value clients with fewer assets. A Lean association comprehends client value and focuses its key methodologies to constantly expand it. The only objective is to give ideal value to the customer by method for a perfect quality creation process that has zero waste [9].

To endeavor, Lean thinking changes the center of organization from improving separate advances, possessions, and vertical offices to advancing the stream of items and administrations through whole value streams that streams that flow horizontally over assets, technologies and departments to customer. Reducing waste along whole value streams, rather than at isolated focuses, makes forms that need less human exertion, less space, less time to make items, less capital and administrations at significantly less expenses and with much

defects, weighed against conventional business frameworks [5][9]. Organizations can answer changing client wishes with high mixture, high caliber, modest, and with amazingly quick throughput times. Additionally, data administration gets to be much less demanding and more exact. Lean principle stays one of the finest assets for comprehension in light of the fact that it depicts the manner of thinking, the all-encompassing key standards that must guide your activities when applying Lean procedures and tools. Lean is more understandable by the Lean software development principles as given in table-1 [4].

III. SIX SIGMA

The Six Sigma concept was introduced MOTOROLLA in 1986. Further in 1995 General Electric made this approach central of their business strategy [7] [11]. Six Sigma is typically identified with the number of 3.4 defects for every million opportunities. Individuals frequently view Six Sigma as quality control mechanism. Today Six Sigma is conveying business magnificence, higher client fulfillment, and prevalent benefits by drastically enhancing each procedure in a venture, whether budgetary, operational or creation. Six Sigma has turned into successful methodology of a wide range of businesses, from medicinal services to protection to information transfers to programming. The driving force behind any Six Sigma project originates from its essential center - "acquiring breakthrough enhancements a precise way by managing variation and diminishing deformities". The goal is to stretch , and stretch rationally not physically. To make it more Six Sigma methodology can be used for its implementation [7] [9].

TABLE I: THE SEVEN LEAN PRINCIPLE OF SOFTWARE PROGRAMMING [4].

PRINCIPLE	DESCRIPTION
Eliminating Waste	Identification and elimination of wastes should not be rare event.
Build Quality In	Construct quality in. Create it in as ahead of schedule as would be possible to maintain a strategic distance from quality issues emerging.
Create knowledge	Learning is vital, and helps the more extended term profit and adaptability of the group.
Defer Commitment	Choose as late as would be possible, especially for choices that are irreversible, or at any rate will be illogical to turn around.
Deliver fast	Conveying quick is that, if there is as little time as could reasonably be expected between the Product Owner expressing the prerequisites and the group conveying the item, there is less risk of the necessities evolving.
Respect people	Reacting to individuals promptly, listening attentively, considering their assumptions.
Optimize the whole	Putting all of this together with better enhanced workflow, the profits or arranging along these lines might be to a great degree critical.

Characteristics that set Six Sigma separated from past quality change activities include [12]:

- A clear focus is on accomplishing measurable and quantifiable monetary
- Comes back from any Six Sigma venture.
- An expanded stress is on solid and enthusiastic administration authority and backing.
- A reasonable responsibility to resolve on choices on the premise of certain information and

measurable systems, as opposed to presumptions and ambiguity.

IV. LEAN SIX SIGMA TO IMPROVE CYCLE TIME OF PROJECT IMPLEMENTATION

For the evaluation purpose author has conducted a survey in the reputed university which results in improvement of cycle time. Cycle Time improvement in students project provide results which enhanced experience. Cycle time improvement could also translate into monetary benefits as we can easily attain our goals for increasing its revenue. The earlier methodology was not that much effective and beneficial, since we were not achieving quality without waste. Students waste their time on gathering the wrong information due to lack of methodology/guidelines. Students are not able to submit their project on or before the deadline.

So what's the gap in the existing approach?

- Students do not focus on the process improvement. One without the other is a large portion of an answer that does not reliably accomplish its objectives of moving forward Communication and data stream.
- Many students take data that is not acceptable by everyone.
- Students waste their time in capturing the irrelevant information as they do not focus on the technical as well as administrative aspects due to which they miss opportunities to collaborate,
    - Sharing knowledge and improve project work.

TABLE II: STUDY OF VARIOUS APPLICATION AREAS OF LEAN SIX SIGMA [7].

Area of Research	Methodology	Source
Lean Six Sigma Applied to a Process Innovation in a Mexican Health Institute's Imaging Department [2].	Use Kaizen identification	García-Porres J.,Ortiz-Posadas M.R M.R., Pimentel-Aguilar A.B (2008)
Lean Six Sigma (LSS) project to a winemaking process in a high-quality, Italian winery [5].	LSS is a highly disciplined method that helps to focus on developing Near perfect product and services.	Riccardo Bettini, Giorgetti, Enrico Cini, Paolo (2010)
Medical equipment inventory control Is conducted at Albert Einstein Hospital [1].	Apply Lean Six Sigma tools in order to analyze wastes in order to Guarantee process quality.	A. P. S. Silva, J. M. Palermo (2012)
Lean Six Sigma Implementation in Equipment Maintenance Process [13].	DMAIC (2012)	XueWang,Yuquan,Wang,Dan
Supplier recovery management using Lean and Six Sigma [8].	Apply EN process	Wang YingchuneD, LiuWeiweieD (2012)
The Implementation of Lean and Six Sigma in Healthcare Focusing on Pharmaceutical Products. [6]	Apply LSS tools	Tanaporn Punchaipetch Jirapan Liangrokapart (2012)

A. Lean Six Sigma methodology

Lean Six Sigma methodology is used to improve the data stream and quality without waste. We have done a brief study to know more about the Lean Six Sigma methodology as described in table 2. Lean Six Sigma methodology has shown tremendous result till now in every application areas. So, author has used DMAIC approach step towards it to improve the teaching learning process.

1) Define phase

The first result attained by this methodology was the formal definition from the student's 'point of view' for the objective of the project, project targets and project boundaries.
Project Objective: - Improve the cycle time of the student project to provide result with enhance experience.
Project target: - 97% Project completed on time.

Project Boundaries Another purpose of this phase was to clearly define what should be extracted and what should not be extracted from the project scope. All the critical points and criteria were identified which could affect the quality such as rewrite data, unavailable data and waiting. As the project advances and more data is gathered in future stages, the issue created in the Define stage was refined [2].

2) Measure phase

A measure is quantified value or characteristics. In this phase students collected the quantitative and qualitative data to have a clear view on of the current state [10] [11] [12]. Team established a process performance baseline. The size of the project team is considered to be of 5. The cycle time of the project is considered to be of 3 months. A baseline was set, so that the gap between current performance and the required performance could be filled. Four types of possible errors and defects (specified in table.3) were identified within the requirement [13]. All the errors listed, identified and resolved within the development of product. As this phase is little bit complex so it is always better to consider the measure phase along with the define phase. So that the some of the problem or errors are known to developer at the beginning of this phase.

TABLE III: Capture Error and Defects [13]

Error #	Description
Error1	Irrelevant requirements added
Error2	Incorrect project planning
Error3	Incorrect order of task
Error4	Incorrect constraint evaluation

3) Analysis phase

In this step root cause was selected, identified and validated. An extensive number of potential root causes (procedure inputs, X) of the undertaking issue are distinguished through underlying driver dissection (for instance a fishbone chart). The main 3-4 potential root causes were choose utilizing multi-voting or different tool for further approval. An information accumulation arrangement was made and information was gathered to make the relative commitment of each one root cause to the undertaking metric, Y. This procedure was repeated until "valid" root causes might be distinguished. Inside Six Sigma, frequently perplexing examination instruments were utilized. It is satisfactory to utilize fundamental strategy if these are suitable of the valid root cause [10] [12].

- Potential causes were listed and identified.
- To improve the step potential root causes were prioritized.
- Causes and effects are analyzed to understand the magnitude of contribution of root cause and effect of causes as shown in fig.1.

X's are the cause of the problem that has been faced during the development and Y's that will be affected by the causes. If students get the late response for their doubts then it directly lead to the increase in the cycle time of the project implementation. The result of the proposed research has been explained with the help of the cause-effect diagram given in fig1.

4) Improve phase

The motivation behind this step was to recognize, test and actualize an answer for the issue; to some extent. Recognize inventive answers for wipe out the key underlying drivers so as to alter the issues found

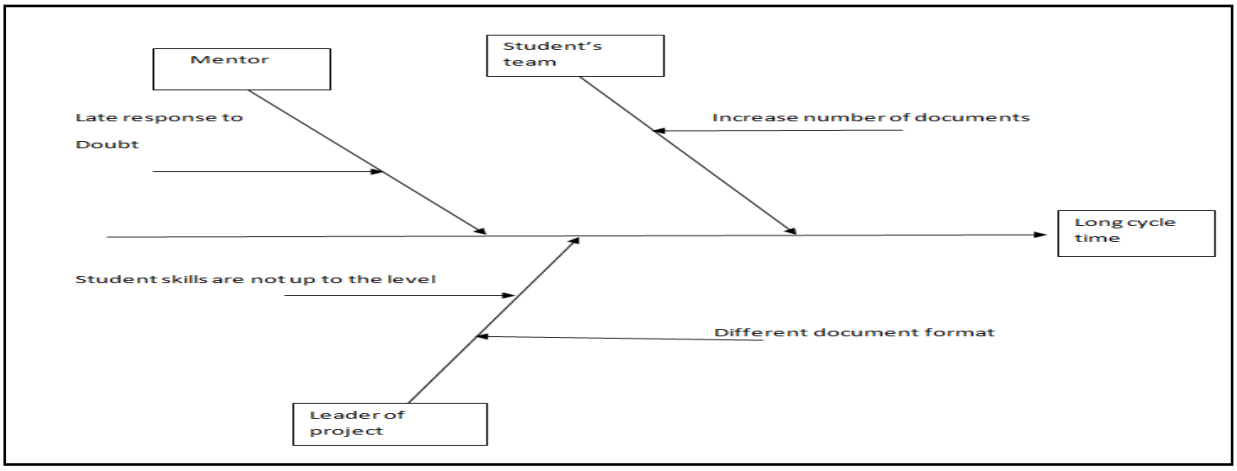


Fig.1.Cause and Effect Diagram of Long Cycle Time

PDCA cycle iteratively manage the process using management process used in controlling and continuously improving the processes. PDCA Cycle helped to come closer to our aim, usually an ideal operation and output [10].

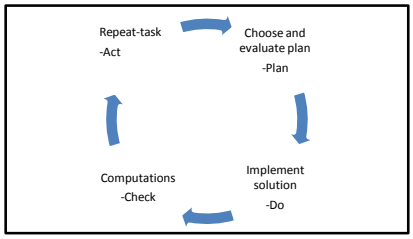


Figure2. Plan-Do-Check-Act cycle [10].

5).Control phase

The reason for this step was to maintain the benefit . Screen the upgrades to guarantee maintainable achievement. Make a control plan. Redesign report, business process and preparing report as needed. This phase enhanced the confident in the user as at this level were identified and removed. A control plan was prepared and for the entire newly designed task verification [2] [3] .

[2] García-Porres J., Ortiz-Posadas M.R., Pimentel-Aguilar A.B " Lean Six Sigma Applied to a Process Innovation in a Mexican Health Institute's Imaging Department " : (30th Annual International IEEE EMBS Conference Vancouver, British Columbia), Canada, August 20-24, 2008

[3] Jordan George, Peter Vincent book Lean Six Sigma: "Combination Six Sigma with Lean Rate" in [2002]

[4] Kelly Waters "7 Key Principles of Lean Software Development": 16 August 2010 | Lean Development http://www.allaboutagile.com/7-key-principles-of-Lean-software-development-2/

[5] Riccardo Bettini, Alessandro Giorgetti, Enrico Cini, Paolo Citti "The Lean Six Sigma approach for process improvement: a case study in a high quality tuscany winery" : (j. of Ag. Eng.) - Riv. di Ing. Agr. (2010), 4, 1-7.

[6] Tanaporn Punchaipetch, Jirapan Liangrokapart "The Implementation of Lean and Six Sigma in Healthcare Focusing on Pharmaceutical Products" Proceedings of the Asia Pacific Industrial Engineering & Management Systems Conference 2012 V. Kachitvichyanukul, H.T. Luong, and R. Pitakaso Eds.

V. CONCLUSIONS

Lean Six Sigma has proven its effectiveness in various application areas. This paper focuses on how Lean Six Sigma can be used to increase efficiency by reducing effort and improving quality. In this paper author tries to reduce the cycle time by using Lean Six Sigma. Various tools and techniques have been used by the students and experiment shows the fact of cycle time improvement. The future scope of this paper is to come up with detail implementation of the above said problem with detail data used to improve the process of Lean Six Sigma

REFERENCES

[1] A. P. S. Silva1, J. M. Palermo1, A. Gibertoni1, J. A. Ferreira2, R. M. A. Almeida2, L. Marroig3[2012] "Inventory Quality Control in Clinical Engineering: A Lean Six Sigma Approach": IEEE MARCH 26 - 31, 2012, MIAMI, FLORIDA

[7] "The Inventors of Six Sigma". Archived from the original on 2005-11-06. Retrieved 2006-01-29.

[8] Wang YingchuneD, Liu WeiweieD, Tong lingeD Wang Yingchun, Liu Yongxian[2010] : "Research on the Lean Six Sigma Supplier Recovery Management" IEEE (2nd International Conference on Industrial and Information Systems) 978-1-4244-8217-7110

[9] Womack and Dan Jones book about Lean : "Lean Thinking" in [2003]

[10] www.wikipedia.org/wiki/Lean_Six_Sigma

[11] www.wikipedia.org/wiki/Lean

[12] www.wikipedia.org/wiki/Six_Sigma

[13] Xue Wang, Yuquan Wang, Dan Xu [2012];"Lean Six Sigma Implementation in Equipment Maintenance Process" in IEEE (Proceedings of the Asia Pacific Industrial Engineering & Management Systems Conference)978-1-4673-0788-8/12 .

Impact of cyber-crime on virtual banking

NEELESH L.CHOURASIYA
Asst. Professor
Department of Computer Engineering
M.E.Society's College of Engineering, Pune-411001
Email id -
neelesh.chourasiya@mescoepune.org

GAURAV CHAURASIA
MS (Cyber Law & Information Security)
National law institute university Bhopal, India 462001
Email id – gauravmsclis@gmail.com

MANMEET KAUR
Assistant Professor
Department of MCA
A.C.E.T. Amritsar
Email id - mink_manu@yahoo.com

Abstract - Here we will discuss about the cyber-crime and impact of cyber-crime on virtual banking. In cyber-crime most of the victim is not aware what happed with them?

Now a day's most of banks are doing transaction throw the internet because banking company provides the facility to the customer by the internet. A person who is customer of the bank he can transfer money, pay bills, mobile recharge, online shopping and many more. There are many technologies available to counteract intrusion, but currently no method is absolutely secured. The most dangerous frauds that causes in day to day banking activity is phishing, a criminal activity using social engineering techniques. Phishers attempt to fraudulently fetch sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

Keywords- cyber-crime, victim, virtual banking, transaction, online shopping, phishing, electronic.

1. INTRODUCTION

"Digital technology and new communication system have made dramatic changes in our lives. Business transaction are being made with the help of computers"[1]

The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity occurred in banks- namely ATM frauds, Money Laundering and Credit Card Fraud[2].
For the majority of businesses and organizations, information is considered to be an asset, and so worthy of protection. Information security can support a wide variety of objectives like[3]-

i. Compliance[4] with laws and regulations.
ii. Reducing the risk of fraud or other falsification of data to an acceptable level
iii. Reducing the risk of unauthorized access[5] or disclosure to an acceptable level

Now a day in Indian banking system, the authentication[6] is done through password that is not up to the level of high security measure. There is an urgent need to acclimatize the security measure in the banking system[7].

2. WHAT IS CYBER-CRIME

"Any illegal act involving a computer, its systems, or its applications"

Cybercrimes can be basically divided into 3 major categories:[8]

i. Cyber-crimes against persons: Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, phishing and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today.

ii.Cyber-crimes against property: These crimes include computer vandalism (destruction of others' property), transmission of harmful programs.

iii.Cyber-crimes against government: The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international

[1]The information technology ACT, 2000 page 1
[2] Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law By Susan W Brenner
[3] Impact of cyber-crime on Banking- Dr.S.Arumugaperumal
[4]Compliance is either a state of being in accordance with established guidelines, specifications, or legislation or the process of becoming so. Software, for example, may be developed in compliance with specifications created bysome standards body, such as the Institute of Electrical and Electronics Engineers (IEEE).
[5]Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner.
[6]Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.
[7] Impact of cyber crime on Banking- Dr.S.Arumugaperumal
[8] An introduction to cyber crime investigation by v.p.srivastav

governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

"Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime."

3. VIRTUAL BANKING

Virtual banking exists in the forms of ATM, phone banking, home banking and Internet banking[9]. In virtual banking the traditional paradigm of a customer's integration with the bank is replaced by an electronic paradigm, which is new and innovative in banking sectors. Customer demands, commercial motivation and technological developments are the key drivers of virtual banking. In the changing environment adaptation to market realities as well as technology is causing the virtual banking revolution[10].

Factors to be considered in virtual banking

i. The routine banking transaction was becoming both costly and time consuming. The banks resorted to computerization to cut cost and time overheads in handling routine transactions

ii. The introduction of automated teller machine (ATM) impart flexibility to bank customers and gave further boost to virtual banking

iii. The introduction of credit cards and debit cards helps both the consumers and retailers to be free from cash handling[11].

4. CYBER CRIME IN BANKING SECTOR

Credit card Fraud- A major kind of electronic crime is „credit card fraud. Indian banking sector is introducing new innovations against counterfeiting and fraud, which are highly sophisticated to profiting from or beating these systems. Most of the credit card fraud is committed with the use of counterfeited cards. Credit card fraud is also termed as „Identity Theft" in which a person may use the identity of other person for exercising fraud or deception. Credit card fraud in banking sector can be committed as[12] -

Use of unauthorized account or personal information to consider as an act of criminal deception

Illegal or unauthorized use of account for personal gain

i. Misrepresentation of account information to obtain services

ii. Several new security measures are introduced to gradually to reduce the credit card fraud in one part but it swiftly shifts to other part. Therefore, the problem of credit card fraud is serious and occurring by stealing the cards and the accompanying information at the time of transaction delivery.

iii. *Money Laundering*:IT and Internet technologies have reached each one nook and corner of the world. E-commerce has come into existence due to the attributes of Internet like ease of use, speed, anonymity and its International nature. Internet has transformed the planet into a frontier excluding market place that never sleeps. Computer networks and Internet authorize relocate of funds electronically between trading partners, businesses and consumers. This shift can be done in many ways like use of credit cards, Internet banking, e-cash, etc. for example, smart cards. In some other forms of computer-based e-money[13], there is no upper limit[14].

iv. *ATMs Frauds*:Over the past three decades, large number of banking customers depends on the ATM to conveniently meeting their banking needs. In the recent years, there have been a large number of accidents of ATMs frauds. It is necessary to manage the risk associated with ATM fraud.

The prevailing contemporary time has replaced long-established monetary instruments from a paper and metal based currency to "plastic money" in the form of credit cards, debit cards, etc. This has resulted in the escalating utilize of ATM all over the world. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of "ATM FRAUDS" that is an international problem. The use of plastic money is increasing for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills. The convenience and safety that credit cards carry with its use has been instrumental in increasing both credit card volumes and usage. This growth is not only in positive use of the same but as well as the negative use of the same. The world at large is struggling to increase the convenience and safety on the one hand and to reduce it misuse on the other. A few of the accepted techniques used to carry out ATM crime in banks are[15]:

ATM card reader is tampered with in order to trap a customer's card through card jamming.

[9] Internet Banking is a product of e-commerce in the field of banking and financial services.

[10] Impact of cyber crime on Banking- Dr.S.Arumugaperumal.

[11] Impact of cyber crime on Banking- Dr.S.Arumugaperumal.

[12] Impact of Electronic crime in Indian Banking Sector – An Overview by Dr. M. Imran Siddique, Sana Rehman

[13] Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server. One common type of e-money is the 'electronic purse', where users store relatively small amounts of money on their payment card or other smart card, to use for making small payments.

[14] Impact of Electronic crime in Indian Banking Sector – An Overview by Dr. M. Imran Siddique, Sana Rehman

[15] Impact of Electronic crime in Indian Banking Sector – An Overview by Dr. M. Imran Siddique, Sana Rehman

i. Card Skimming[16] is the unlawful technique of stealing the card's security information from the card's magnetic stripe.

ii. Card Swapping, is another technique in which customer's card is swapped with another card without the knowledge of cardholder.

iii. Website Spoofing[17], here a fresh fabricated site is prepared which looks valid to the user and customers are asked to give their card number PIN and other information, which are used to reproduce the card for use at an ATM.

iv. ATM machine is physical attacked for removing the cash.

5. PHISHING ATTEMPTS USING VOICE

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Voice phishing sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization. This style of identity theft is becoming more popular[18].

For ex.-You get a phone call from your bank saying that they have noticed some suspicious or fraudulent activities on your bank account, and asking you to either phone back (because most of the time the voice is pre-recorded) and/or give your bank account number, credit card number etc.

6. IMPACT

i. *Potential Economic Impact* - Many people have the attitude that cyber-crime is a fact of doing business online As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud[19].

ii. *Impact on Market Value* - The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies that provide cyber-risk policies[20].

iii. *Impact on Consumer trust* -Since cyber-attackers intrude into others space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on along termbasis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths. The perception that the Internet is popular with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce[21].

7. SUGGESTIONS

It is always necessary to take some preventive measures to prevent banking transactions from banking frauds and other threats. For this, the following suggestions can be made[22] -

i. Make sure web servers in a row public site are physically separate and individually confined from in-house corporate network.

ii. Bring into play latest anti-virus software, operating systems, Web browsers and email programs

iii. Place firewall and develop your content off line.

iv. Forward credit card information just to safe and sound web sites

v. If Web site serves up active content from a database, consider putting that database behind a second interface on your firewall, with tighter access rules than the interface to your server.

vi. Systematically confirm out the site to business regularly.

vii. Don not forgets to verify out the site you are doing business carefully

viii. Don't transmit credit card information to unfamiliar sites

ix. Don't reveal password with other people

8. CONCLUSION

Researchers know that now a day's technology has dramatically change day to day .Today every organization doing business by the help of internet. Internet provides the platform for business means today we can sale or purchase most of the item online. We can book rail ticket, bus ticket, and hotel and online shopping, money transfers within

[16] 'Card skimming' is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam.

[17] **Website spoofing** is the act of creating a website, with the intention of misleading readers that the website has been created by a different person or organization. Normally, the spoof website will adopt the design of the target website and sometimes has a similar URL.

[18] Impact of cyber-crime on Banking- Dr.S.Arumugaperumal.

[19] Cyber-Crimes and their Impacts: A Review by HemrajSaini, Yerra Shankar Rao, T.C.Panda

[20] Cyber-Crimes and their Impacts: A Review by HemrajSaini, Yerra Shankar Rao, T.C.Panda

[21] Cyber-Crimes and their Impacts: A Review by HemrajSaini, Yerra Shankar Rao, T.C.Panda

[22] Impact of Electronic crime in Indian Banking Sector – An Overview by Dr. M. Imran Siddique, Sana Rehman

second. Now a day e-commerce is growing day by day. Most of them people done transaction by the internet and pay from the credit card/debit card, Professional criminals are successfully using phishing techniques to steal personal finances and conduct identity theft at a global level. The popularity which virtual banking services have won among customers, owning to the speed, convenience and round-the-clock access they offer, is likely to increase in the future. However, several issues of concern would need to be pro-actively attended. While most of electronic banking has built-in security features such as encryption, prescription of maximum monetary limits and authorizations, the system operators have to be extremely vigilant and provide clear-cut guidelines for operations. On the larger issue of electronically initiated funds transfer, issues like authentication of payments instructions, the responsibility of the customer for secrecy of the security procedure would also need to be addressed.

VENTURE CAPITAL FINANCING IN INDIA

PROF. GURPREET SINGH

ASSISTANT PROFESSOR IN COMMERCE

RSD COLLEGE, FEROZPUR CITY

Contact detail:gsg2100@yahoo.co.in

ABSTRACT

A new entrepreneur or company which does not want to take finance from traditional institutions or public market may have their eyes on venture capital. Venture capital is provided to any business firm by those who are willing to invest in new ideas, vision & projects or ventures that are risky but have a promising future prospect. Such funds are known as venture capital funds. Venture capital financing has now gained a certain degree of densification, maturity & edification in the western countries. The phenomenon of venture capital is new for the Indians but it was one of the much talked things about financing alternatives in India. In this research paper we will talk about the venture capital financing in India , current status of venture capital, growth prospects of venture capital, problems of venture capital financing & future outlook of venture capital in India.

KEY WORDS :Venture capital financing , hot areas ,current status , growth prospects , problems & future outlook of VC.

INTRODUCTION

Venture capital is money provided by professionals who invest alongside management in young, rapidly growing companies that have the potential to develop into significant economic contributors. Venture capital is an important source of equity for start-up companies. Professionally managed venture capital firms generally are private partnerships or closely-held corporations funded by private and public pension funds, endowment funds, foundations, corporations, wealthy individuals, foreign investors, and the venture capitalists themselves.

LITERATURE REVIEW

ICFAI (2004) explored that the Government of India in an attempt to bring the nation at par and above the developed nations has been promoting venture capital financing to new, innovative concepts & ideas, liberalizing taxation norms providing tax incentives to venture firms, giving a Philip to the creation of local pools of capital and holding training sessions for the emerging VC investors.

MS. RIDHIMA MEHER concluded that VCF is in its nascent stages in India. The emerging scenario of global competitiveness has put an immense pressure on the industrial sector to improve the quality level with minimization of cost of products by making use of latest technological skills. The implication is to obtain adequate financing along with the necessary hi tech equipments to produce an innovative product which can succeed and grow in the present market condition.

KPMG STUDY (2012) find out the fact hat There are large sectors of the economy that are ripe for VC investors, like, I.T, Pharmacy, Manufacturing. Telecom, Retail franchises, food processing and many more. The nation awaits for the burgeoning VC business in India in spite of the existing shortcomings in the Indian infrastructure. Looking ahead for a bright future for India Inc.

OBJECTIVES OF THE STUDY

The present paper is concerned with fulfilling the following objectives:-

(1)To explore out the current status of VC industry in India

(2)To find out the emerging challenges in context to VC industry in India

RESEARCH METHODOLOGY

This research paper is based on secondary data and by reviewing various authentic research papers from online databases of peer reviewed, official websites of mutual funds and investment management, in-depth studies conducted by specialized agencies as well as their views.

CURRENT STATUS OF VENTURE CAPITAL FINANCING IN INDIA

The phenomenon of venture capital has now reached a take off stage in India. When we compare to potentials & opportunities in India, risk capital in all forms is becoming available more freely. some of the important facts in context to venture capital financing in India are as follows :-

(1)Number of players – the number of venture players is growing at a very rapid rate in India . At present , more than 400 VC firms are active in India , out of which 180 VC firms are registered under SEBI(VENTURE CAPITAL FUNDS) REGULATIONS,1996

(2) Hot areas- Proffered regions of VC investment in India are Mumbai, Delhi & bungler. Among the three, Mumbai attains the top slot with more than 108 investments against 63 investments in Delhi & 49 investments in bungler.

(3)Key growth drivers- Key growth drivers in India are healthy GDP growth, growing middle class, vibrant entrepreneurial ecosystem. Such factors are contributing towards healthy growth & development of VC in India.

(4)Prevailing sectors – IT sector & domestic consumption sector prevailing sectors in India in context to VC investments in India

(5)Investment rounds increase in India - India bucked the declining global trend in VC investment activity in 2012. The number of investment rounds increased by 17 % 10 205, the third successive year of increasing activity. Total capital invested declined from US $ 1.7 b in 2011 to US $ 1.4 b in 2012.the figures for 2011, however, contained a few large investments with a combined value of between US $ 400 M to US $ 500 m. & if these are excluded, the year on year comparison looks far healthier

(6)Economic development is supporting VC growth The growing wealth of Indian economy & the accompanying increase in consumerisation is underpinning the growth of the VC industry in India. The two predominant themes from a demand perspective are the Company addressing the changing consumer behaviour- the largest proportion of the total pool of VC backed companies is in consumer services (170 out of the pool of a pool of 528) & the introduction of new technology , particularly internet based applications such as cloud & mobile. From a supply perspective, rising economic prosperity has increased the pool of entrepreneurs willing to take risk on VC investment & the entrepreneurial ecosystem which is becoming more developed as the availability of higher education.

(7) Late stage investments dominates in India the Indian VC industry is heavily weighted towards later stage investment. The proportion of deals in the revenue generating stage as 87 % in 2012, up from 83 % in 2011 & 81 % in 2010. The reason for predominance of late stage investment is that, compared with Silicon Valley, Indian companies are focused less on innovation & more on application development & efficient development models, which takes less time to develop into revenue generating phase.

(8) M&A is more likely than IPO to exit – strategic buyers are a more likely exit route for Indian VC backed companies than IPO'S . the very low level of IPO exists (two in both 2011 & 2012) reflects the absence of a junior stock market .

(9)Confidence – From opportunities perspective, fund managers confidence in India is apparent in their willingness to seed & help manage new businesses in their formative years. This is especially true for sectors that have not been much VC activity in the past, such as consumer products, financial services & logistics. This is a departure from the conventional VC model of "FIND & FUND"

(10)More deals , but smaller size Median round size decreased from US $ 5.5 m in 2011 to US $ 3.6 m in 2012. The decrease in part reflects the influence on the VC market, with a preference for lower investment sizes

PROBLEMS WITH VCS IN THE INDIAN CONTEXT

One can ask why venture funding is so successful in USA and faced a number of problems in India. The biggest problem was a mindset change from "collateral funding" to high risk high return funding. Most of the pioneers in the industry were people with credit background and exposure to manufacturing industries. Exposure to fast growing intellectual property business and services sector was almost zero. All these combined to a slow start to the industry. The other issues that led to such a situation include:

(1)License Problems Till early 90s, under the license raj regime, only commodity centric businesses thrived in a deficit situation. To fund a cement plant, venture capital is not needed. What was needed was ability to get a license and then get the project funded by the banks and DFIs. In most cases, the promoters were well-established industrial houses, with no apparent need for funds. Most of these entities were capable of raising funds from conventional sources, including term loans from institutions and equity markets.

(2)Traditional Mindset Venture capital as an activity was virtually non-existent in India. Most venture capital companies want to provide capital on a secured debt basis, to established businesses with profitable operating histories. Most of the venture capital units were offshoots of financial institutions and banks and the lending mindset continued. True venture capital is capital that is used to help launch products and ideas of tomorrow. Abroad, this problem is solved by the presence of `angel investors'. They are typically wealthy individuals who not only provide venture finance but also help entrepreneurs to shape their business and make their venture successful.

(3)Multiplicity of Regulators There is a multiplicity of regulators like SEBI and RBI. Domestic venture funds are set up under the Indian Trusts Act of 1882 as per SEBI guidelines, while offshore funds routed through Mauritius follow RBI guidelines. Abroad, such funds are made under the Limited Partnership Act, which brings advantages in terms of taxation. The government must allow pension funds and insurance companies to invest in venture capitals as in USA where corporate contributions to venture funds are large.

(4)Exit Routes The exit routes available to the venture capitalists were restricted to the IPO route. Before deregulation, pricing was dependent on the erstwhile CCI regulations. In general, all issues were under priced. Even now SEBI guidelines make it difficult for pricing issues for an easy exit. Given the failure of the OTCEI and the revised guidelines, small companies could not hope for a BSE/ NSE listing. Given the dull market for mergers and acquisitions, strategic sale was also not available.

(5)Valuation Mismatch The recent phenomenon is valuation mismatches. Thanks to the software boom, most promoters have sky high valuation expectations. Given this, it is difficult for deals to reach financial closure as promoters do not agree to a valuation. This coupled with the fancy for software stocks in the bourses means that most companies are proponing their IPOs. Consequently, the number and quality of deals available to the venture funds gets reduced.

(6) Corporate venturing Even though corporate venturing is an attractive alternative, most companies find it difficult to establish systems, capabilities and cultures that make good venture capital firms. Corporate managers seldom have the same freedom to fund innovative projects or to cancel them midstream. Their skills are honed for managing mature businesses and not nurturing startup companies. If a firm is to apply the venture capital model, it must understand the characteristics of the model and tailor its venture capital program to its own circumstances without losing sight of these essentials.

FUTURE OF VENTURE CAPITAL FINANCING IN INDIA

Future of venture capital financing in India is very bright. Experts believe that from 2010 to 2015 , total venture capital financing in India will be US $ 10 billion against US $ 3.3 billion from 2005-2009.In India. The number of venture of VC exits is very good, the multiples on return on technology investment have been excellent and, more importantly, the majority of the exits were in the valuations of US $ 100 million to US $ 500 million. From 2004 to 2010, there were 142 venture based exits in India, out of those exits, 100 were technology companies:-

- *IT COMPANIES*
- *SOFTWARE PRODUCTS*
- *BUSINESS PROCESS OUTSOURCING*
- *KNOWLEDGE BASED OUTSOURCING*

Moreover, domestic consumption is a key theme VC funds are closely pursuing companies that are capitalising on the proliferation of wealth, a burgeoning middle class , greater financial inclusion & differentiated health care delivery models. Such trends are expected to continue, with VC funds trying to invest a cross sectors that allow them to tap into the rapid growth in domestic consumption

CONCLUSION

In nutshell, the nature & scope of venture capital financing in India is vast. IT sector, health care sector & domestic consumption sector are the most dominating & prevailing sectors. greater attention should be provided to these sectors. The growth & number of venture capital deals, investments & players is increasing at a very rapid rate.

REFERENCES

(1) Bergemann, D. & Hege, U., 1997. "**Venture Capital Financing, Moral Hazard and Learning**," Discussion Paper 1997-108, Tilburg University, Center for Economic Research.

(2) Joshua Lerner, 1994. "**The Syndication of Venture Capital Investments**," Financial Management, Financial Management Association, vol. 23(3), Fall.

(3) Samuel Kortum & Josh Lerner, 1998. "**Does Venture Capital Spur Innovation?**," NBER Working Papers 6846, National Bureau of Economic Research, Inc.

(4) Thakor, Anjan V., 1998. "**Comment on Trester**," Journal of Banking & Finance, Elsevier, vol. 22(6-8), pages 700-701, August.

(5) Bygrave, William D., 1987. "**Syndicated investments by venture capital firms: A networking perspective**," Journal of Business Venturing, Elsevier, vol. 2(2), pages 139-154.

(6) Klaus M. Schmidt, 2003. "**Convertible Securities and Venture Capital Finance**," Journal of Finance, American Finance Association, vol. 58(3), pages 1139-1166, 06.

(7) Schmidt, Klaus M., 1999. "**Convertible Securities and Venture Capital Finance**," CEPR Discussion Papers 2317, C.E.P.R. Discussion Papers.

(8) Klaus Schmidt, 1999. "**Convertible Securities and Venture Capital Finance**," CESifo Working Paper Series 217, CESifo Group Munich.

(9) Berglof, Erik, 1994. "**A Control Theory of Venture Capital Finance**," Journal of Law, Economics and Organization, Oxford University Press, vol. 10(2), pages 247-67, October.

(10) Kaplan, Steven & Strömberg, Per Johan, 2000. "**Financial Contracting Theory Meets The Real World: An Empirical Analysis Of Venture Capital Contracts**," CEPR Discussion Papers 2421, C.E.P.R. Discussion Papers.

(11) Steven N. Kaplan & Per Stromberg, 2003. "**Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts**," Review of Economic Studies, Wiley Blackwell, vol. 70(2), pages 281-315, 04.

(12) Steven N. Kaplan & Per Stromberg, 2000. "**Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts**," NBER Working Papers 7660, National Bureau of Economic Research, Inc.

Steven N. Kaplan & Per Strömberg, 2000.

(13) **Financial Contracting Theory Meets the Real World: An Empirical Analysis of Venture Capital Contracts**," CRSP working papers 513, Center for Research in Security Prices, Graduate School of Business, University of Chicago.

(14) Bergemann, Dirk & Hege, Ulrich, 1998. "**Venture capital financing, moral hazard, and learning**," Journal of Banking & Finance, Elsevier, vol. 22(6-8), pages 703-735, August.

(15) Bergemann, Dirk & Hege, Ulrich, 1997. "**Venture Capital Financing, Moral Hazard and Learning**," CEPR Discussion Papers 1738, C.E.P.R. Discussion Papers.

(16) Grossman, Sanford J & Hart, Oliver, 1985. "**The Cost and Benefits of Ownership: A Theory of Vertical and Lateral Integration**," CEPR Discussion Papers 70, C.E.P.R. Discussion Papers.

(17) Grossman, Sanford J & Hart, Oliver D, 1986. "**The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration**," Journal of Political Economy, University of Chicago Press, vol. 94(4), pages 691-719, August.

(18) Grossman, Sanford J. & Hart, Oliver D., 1986. "**The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration**," Scholarly Articles 3450060, Harvard University Department of Economics.

(19) Oliver Hart & Sanford Grossman, 1985. "**The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration**," Working papers 372, Massachusetts Institute of Technology (MIT), Department of Economics.

(20) Christopher B. Barry, 1994. "**New Directions in Research on Venture Capital Finance**," Financial Management, Financial Management Association, vol. 23(3), Fall.

POSTAL SERVICES IN INDIA

PROF. BALWEEN KAUR

ASSISTANT PROFESSOR IN COMMERCE

DAV COLLEGE FOR WOMEN, FEROZPUR CANTT.

Contact details: balween@ymail.com

ABSTRACT

A post office is a public department or corporation forming part of a national postal system. It is an office or station of a government postal system at which mail is received and sorted, from which it is dispatched and distributed, and at which stamps are sold or other services rendered. The organized systems of post office providing variety of mail-related and courier service seems quite ancient, although sources vary as to precisely who initiated the practice of post office. This paper laid emphasis on the postal as well as financial services provided by post office in India.

INTRODUCTION

Today post office has reached everywhere. We can find it in almost every locality in a town or city. Significantly every village tool has a post office. It is a very important building as it is the centre of all postal activity in a locality and letters remain the most widely used mode of communication in India. The large number of post offices today are a result of a long tradition of many disparate postal systems which were unified in the Indian union post independence . Owing to this far-flung reach and its presence in remote areas , the Indian postal system is also involved in other services such as small savings , banking and financial services.

LITERATURE REVIEW

RITIKA AGGARWAL (2012) find out that India Post Office Savings Bank is widely known and traditional formal institution offering saving products. Its outreach has been ceaselessly increasing both in terms of number of accounts as well as number of branches, especially in small regions of the country. Globalization has brought
Outsized revolution in the financial sector of the country, which proves to be challenging for POSBs.
Liberalization has substantially increased better and innovative investment possibilities to the investor.

BIS (2012) explored that the Post Office network of around 11,500 branches plays a unique and valued role in communities up and down the country. Post Offices are vitally important for the future of communities, both rural and urban. The Government is committed to the long term future of the Post Office. We have carried out a fundamental rethink of Government policy towards the Post Office, designed to break the cycle of decline into which the network has been allowed to fall

COMMITTEE ON HARNESSING THE INDIA POST NETWORK FOR FINANCIAL INCLUSION (2010) has given recommendations for population wide banking, payments and emergency credit access are in line with both the Government's focus on financial inclusion and the India Post capacity and role in delivery of essential financial services to everyday Indians

WORLD BANK (2006) concluded that in India the Post Office will be reaching out to new customers and winning back those who have drifted away, refurbishing its branches, extending its opening hours, reducing queues, and developing its presence online. This will mean a major modernization to address the underlying economics of the network.

OBJECTIVES OF THE STUDY

The Post Office is unique. It is part of the fabric of the country, as well as being the country's largest retail network. The main theme of this research paper is to explore out the major services provided by post offices in India as well as benefits availed by customers in recent times .

RESEARCH METHODOLOGY

This research paper is based on secondary data and by reviewing various authentic research papers from online databases of peer reviewed, official websites of mutual funds and investment management, in-depth studies conducted by specialized agencies as well as their views.

FINDING OF THE STUDY

Some of the major postal services provided by post offices in India are as follows :-

(1) Speed post_speed Post, the market leader in the domestic express industry, was started by Department of Posts in August 1986 for providing time-bound and express delivery of letters ' documents and parcels across the nation and around the world. In the past 20 years, it continues to be the market leader in the express industry with monthly volumes exceeding more than 1.5 cr . The high speed Postal Service Speed Post links more than 1200 towns in India, with 290 Speed Post Centres in the national network and around 1000 Speed Post Centres in the state network. For regular users, Speed Post provides delivery 'anywhere in India' under contractual service. Speed Post offers money-back guarantee, under which Speed Post fee will be refunded if the consignment is not delivered within the published delivery norms.

(2) E-payment services_E-Payment is a smart option for businesses and organizations to collect their bills or other payments through Post Office network. When businesses require collection of bills and other payments from customers across the country, Post Office offers them a simple and convenient solution in the form of e-Payment's-Payment is a many-to-one solution which allows collection of money (telephone bills, electricity bills, examination fee, taxes, university fee, school fee etc.) on behalf of any organization. The collection is consolidated electronically using web based software and payment is made centrally through cheque from a specified Post Office of biller's choice. The information and MIS regarding the payment can be had by the biller online. The MIS will contain the five fields of biller's choice like name, telephone number, application number etc. The service is currently available through more than 14,000 Post Offices across the country. There is no agency in the market today with a large reach and established trust as the Post Office where the public can comfortably deposit all their bills in their neighbourhood.

(3) Logistics Post - B2B Express Distribution _ If you are a corporate customer looking for logistics solutions, Logistics Post services will provide you cost-effective and efficient distribution across the country. Logistics Post manages the entire distribution side of the logistics infrastructure from collection to distribution, from storage to carriage, from order preparation to order fulfilment at the lowest possible price. Some of the important elements are as follows :-

(a) Distribution solutions: With a high growth Indian economy in India, transport and logistics take on a new dimension in any business. Logistics Post can cater to any demand for moving goods, parcels and consignments in terms of delivery deadline and quality of service. Further, it offers the possibility of monitoring the delivery progress at all times. Whether you want to distribute your computers across the nation or to send your auto parts to the distributors, Logistics Post provides you a tailor-made solution.

(b) FTL and LTS services: Under this service, customers can send their consignments either in full truck load (FTL) or Less than a Truck Load (LTL) , one parcel or multi-parcels, based on their requirements. It is flexible and convenient. Logistics Post uses a special network for carrying and delivering packages and consignments across the nation. It moves the shipments by road, rail and air and ensures safe and timely delivery.

(c) Logistics Post Centres: We have established Logistics Post Centres across the country to take your consignments. Just get in touch with any of the Logistics Post Centres.

(d) Distance and weight-based tariff: The tariff is based on weight, volume and distance. The weight slab is 50 kg. For each consignment, a docket fee of INR100 is payable in addition to other charges based on weight, volume and distance.

(e) Multi-modal transport: Based on the specific requirements of the customers, the consignments are sent by road, rail or air. India Post has a fleet of exclusive aircraft to carry Logistics Post air consignments. Further, we have a fleet of vehicles to transport the consignments by road.

(f) Warehousing services: To make logistics operations cost effective and efficient, Logistics Post provides warehousing options (storage of goods before dispatch/ delivery) to the customers, on payment of warehousing charges. This enables you to bring your products closer to your customers. Let us know your requirements and we shall provide you the warehousing solutions.

(g) Order processing & fulfilment services: Along with warehousing services, we provide you an order processing and order management solution that takes a "whole of business" approach. Logistics Post will make the entire Logistics operations smooth by providing 'pick and pack' facilities based on specific requirements of the customers. Each consignment will be packed with the specific goods, as desired by the customer.

(h) Return Logistics: Businesses requiring 'Return services' will find Logistics Post the ideal solution. Just sign a business agreement with us for 'Reverse logistics' and we shall make the required arrangements.

(4) E post services In the recent past, Internet and e-mail have revolutionized the world of communications. At the same time, accessibility to email continuous to be a major problem for many people, especially in the rural areas. In its endeavour to make the benefits of e-mail available to everyone and to bridge the digital divide, Department of Posts has introduced E- POST service. Through E- POST, customers can send their messages to any address in India with a combination of electronic transmission and physical delivery through a network of more than 1,55,000 Post Offices. E- POST sends messages as a soft copy through internet and at the destination it will be delivered to the addressee in the form of hard copy. E- POST costs just Rs. 10 per page of A4 size. E- POST can also be availed by the corporate customers, by having a business agreement with India Post. Corporate customers will get special E- POST rates and other value additions.

(5) Business post services Business Post - Mailing solutions for businesses If you are a corporate customer looking for mailing solutions, Business Post services will make your task easy and convenient. Business Post demonstrates our responsiveness to market demands in providing value additions to mail services, with the best possible delivery at the lowest possible price. Our customers are the reason for our existence. Their satisfaction in our products and services is of paramount importance to us. Realising this, we are improving our services at all levels and we focus on continual improvement.

(a) Business mail processing made early: Business Post handles all business mail processing to make the task easy and convenient for the customer. Outsourcing the business mail processing needs to India Post means that the company can redirect precious resources to its core business activities. It makes sound business sense.

(b) Business Post Centres: Business Post services are available in 'Business Post Centres' which have been established in major towns. Business Post Centres are available at major post offices. Business Post Centres deal with the processing of the Business Post consignments. Business Post centres can also be set up at the premises of the customers, specially at Bank Head quarters or company Headquarters where the business volumes are very large. Under Business Post, the amount payable for Business Post services is received in advance.

(6) Media post services India Post offers an unique media concept to help the Indian corporate and the Government organizations reach potential customers through Media Post. Creative, cost-effective and personalized, it is over packed . Absolutely no other media can match the sheer expanse of India Post in terms of volume and reach. Media Post - an innovative & effective vehicle for Brand and Marketing managers to communicate their corporate messages across the nation.

(7) Direct post Direct Post is the un-addressed component of Direct Mail, and would comprise of un-addressed postal articles like letters, cards, brochures, questionnaires, pamphlets, samples, promotional items like CDs/floppies and Cassettes etc., coupons, posters, mailers or any other form of printed communication that is not prohibited by the Indian Post Office Act 1898 or Indian Post Office Rules 1933.

(8) Parcel services Anything may be sent in a parcel excepting articles the transmission of which is prohibited. A parcel may contain a single written communication of the nature of a letter or having the character of a personal communication, addressed to the addressee of the parcel. Save as provided in sub-clause (a) No written communication must be enclosed in a parcel. If a parcel is suspected to contain any written communication other than that permitted by sub-clause (1) It will be forwarded to its destination marked " For open delivery". If on being opened in the office of delivery in the presence of the addressee or his authorized agent it is found to contain any written communication other than the one permitted by sub-clause (1), each such written communication shall be charged on delivery with double the letter postage. Any postage paid on the parcel shall not be taken into account in assessing this charge. If the addressee fails attend as required or refuse to pay the charge in full the parcel shall be returned to the sender from whom the charge will not be recovered.

(9)Greeting post services some of the main greeting post services are as follows :-

(a) Innovative Product: Welcome to the world of Greeting Post ,a new range of delightful greeting cards, brought to you by India Post. These cards come ready with pre-paid postage envelopes thereby eliminating the need to affix stamps: a unique concept for the first time in India. What's more fascinating, the postage stamps are an exact replica of the cards inside.

(b) Advantage Greeting Post: And it's not only convenience that these cards offer, but a lot more. Through Greeting Post you can express yourself perfectly on every occasion, festival

or event. Few would miss the warmth reflected in their beautiful designs and pleasing colours Which undoubtedly makes them an absolute joy to receive.

(c) Where you can Get: The cards are being sold through the private distributors of the Greeting Cards and the stationary shops. The Cards and the envelopes with the embossed stamp will be sold together. Greeting cards are available at all major Post Offices.

(d) Features: Greeting Post is yet another innovative product of India Post comprises of a card with envelop with pre-printed postage stamp upon the envelope. The envelope contains multi coloured embossed stamp (which is a miniature replica of the design that appears upon the card) of 5 cm x 4 cm x 3 cm of the denomination of INR 5/- written on the stamp. Thus you need not affix postage stamps on the envelope thus saving your time of going to post offices and standing in the queue. The Greeting Card also has in built around stamp in gray blue on the back of the card precisely on the flap. All the rules and regulations for the postage dues will be applicable to the Greeting Post. As per the current rules, INR 5/- postage entitles the sender to send the article to any part of the country up to 20 grams. The same rule will be applicable for the Greeting Post also.

REFERENCES

(1) Kumar, K.S.; Banu, C.V.; Nayagam, V.L.G. (2008), "Financial product preferences of Tiruchirapalli investors using analytical hierarchy process and fuzzy multi criteria decision making",

(2) Investment Management and Financial Innovations, Volume 5, Issue 1.

(3) Mahamuni, P.N.; Apte, S.K.; Jumle, A.G. (2011), "A Study on Personal Financial Planning for IT Sector Investor in Pune", International Journal of Management, IT & Engineering, Volume 1, Issue 5, October.

(4) Das, S.K. (2011), "An Empirical Analysis on Preferred Investment Avenues among Rural and Semi-Urban Households". Journal of Frontline Research in Arts and Science Vol. 01, pp. 26-36.

(5) G, H.S.; Jacob, P. (2009), "Post Office savings and its relevance in rural areas- A study on the impetus for Rural Investment with reference to Kumbalangi in Cochin", VIDWAT, The Indian Journal of Management, Dhruva College of Management, Hyderabad Vol. 2, ISS 1, Jan-June 2009, pp.26.

(6) India Post (2012), Post Offfice Saving Schemes, http://www.indiapost.gov.in, accessed on 2nd September 2012.

(7) Issahaku, H. (2011), "Determinants of Saving and Investment in Deprived District Capitals in Ghana -A Case Study of Nadowli in the Upper West Region of Ghana", Continental J. Social Sciences, 4 (1), pp. 1 - 12.

(8) Merikas, A.A.; Merikas, A.G.; Vozikis, G.S.; Prasad, D. (2011), "Economic Factors and Individual Investor Behaviour: The Case of the Greek Stock Exchange", Journal of Applied Business Research, Volume 20, Number 4.

(9) The World Bank new flagship report (2012), "Turkey Country Economic Memorandum (CEM) on Sustaining High Growth: the Role of Domestic Savings", conference in Ankara, organized jointly with the under secretariat of the Treasury and the Ministry of Development, March 14.

(10) Thilakam, C.; Ganesan (2012), "Financial Literacy Among Rural Masses In India", International Conference on Excellence in Business, Sharjah, United Arab Emirates, University of Sharjah, 9-10 May.

ACCOUNTING DIVERSITY AND DEVELOPMENT IN GLOBAL ARENA

Sidhartha Sharma
Assistant Professor of Commerce in R.S.D College,
Ferozepur city, Punjab
Contact detail: sid_rocks333@yahoo.com, Cell no. 9464463537

ABSTRACT

Before 1970's a reasonable answer for accounting was a statement which depicts financial position of the business enterprise. Now days if we are of the same opinion that accounting are just a process of recording and reporting of financial information, it will be a wrong notion. With the drastic reforms in international markets , emergence of large number of MNC's , expansion of Accounting bodies and various other environmental factors . Most accountants and financial executives at international level are realizing the diversity and complexities in accounting policies, practices and procedures. This paper broadly examines the impact of various environmental factors on accounting as well as various new accounting concepts and methods which has been originated due to complex interaction of environmental variables

KEYWORDS: Accounting, Diversity, Environmental Factors, Concepts, Methods.

INTRODUCTION

Accounting is influenced by various environmental variables, but at the same time, it is one of the factors affecting on this same environment. This is a fact that points to the interdependency of accounting and its environment. A nation's accounting policies , practices and procedures is affected by a variety of economic, socio – cultural, political , legal and many other environmental factors, so it is highly unlikely for the influential factors of any two countries to be exactly the same. Nation's accounting principles and practices are the product of complex interaction of above environmental factors etc. It is unlikely that mix is identical in any two countries or more and therefore diversity is to be expected at global level.

REVIEW OF LITERATURE

FREDERICK D.S CHOI (1991) concluded that investors and participants in the international capital market perceive accounting diversity as a major problem that affects the capital market decisions .The paper concluded the two main factors .Firstly; differences in the accounting practices may affect the pricing of securities and the composition of international portfolios. Secondly, this paper described as effective ways of coping with accounting diversity and its impact on international capital markets.

PETER JOOD & MARK LANG (1994) investigated the diversity in the accounting practices of France, Germany and United Kingdom. This paper concluded the various factors. Firstly, the paper has explored the significant differences between accounting ratios and stock market valuation. Secondly, it also provides preliminary evidence on the effects of the (EU) European Union directives on accounting measurement differences.

SUSANA & JOSE A LAINEZ (2000) explored out that existence of diversity in accounting principles and accounting system has significant consequences for the interpretation of financial reporting in global arena and, therefore, for the decisions which may be taken on the basis of the interpretation drawn from an analysis of such accounting information. The paper concluded the two main factors .Firstly, accounting diversity can be considered as a prime obstacle for the international comparability of financial reporting. Secondly, the paper have found the important differences in the situation of companies i.e. liquidity, solvency, indebtedness and profitability under different accounting principles

HASSAN R. HASSABELNABY, RUTH W. EPPS AND AMAL A. SAID (2003) found the impact of environmental variables on the development of accounting. Four

environmental variables are used to explain the variation observed over time in accounting development. These factors were the economic environment, the political environment, the development of the stock market, and privatization of state owned corporations. The paper concluded the two main factors. Firstly, the impact of the environmental variables on accounting development changes over time reflecting the different stages of democracy and economic reform. Secondly, it provides international investors and researchers with a in depth understanding of the dominating environmental variables that affect accounting in global arena.

LOANA MARIA DRAGU (2010) found that the global accounting conceptual framework and standards still continue to represent a mission for international accounting bodies like international accounting bodies like (IASB) international accounting standard board and (FASB) financial accounting standard board, being far from the stage of practical implementation. Both accounting bodies are witnessing the diversity and complexities with regard to accounting system in global arena. Thus, harmonizing both national and international accounting regulations is necessary so that it would be in accordance with companies' interest.

ADELA DEACONU & ANUTA BUIGA (2011) witnessed the diversity between accounting systems of Continental-European type and Anglo-Saxon type respectively. The paper concluded the two main factors. Firstly, the paper examines the relevance of the criterion in the historic context. Secondly, it studies the whole framework comprising economical, social, legal and political variables and their impact on accounting diversity.

JOEL BRANSON & MUIZ JAMIL (2011) observed the main factors for diversity in accounting practices, policies and procedures and to better understand how accounting differences have a huge impact on accounting harmonization .The paper concluded the two main factors. Firstly, it strengthens the awareness of the existence of and the causes for accounting diversity. It is important to understand the current complexities and difficulties of the drive towards international accounting harmonization. Secondly, the in-depth analysis of the environmental variables that are considered most influential in causing accounting diversity.

OBJECTIVES OF THE STUDY

The present paper is concerned with fulfilling the following objectives:-

(1) To study the impact of environmental variables on accounting practices, policies and procedures.

(2) To explore the new accounting concepts and methods this has been originated due to the complex interaction of environmental variables.

RESEARCH METHODOLOGY

This paper is totally based upon empirical studies and data. The data used in the study is primary as well as secondary. Primary data has been collected on the basis of personal interactions with experts, academicians and the learned persons. On the contrary, secondary data is collected by reviewing various authentic research papers from online databases of peer reviewed, journals, official websites, books, professional magazines and newspapers.

FINDINGS OF THE STUDY

Research literature reveals the following factors that impact accounting diversity at national level as well as which are likely to shape accounting diversity in global arena.

- **Accounting and economic environment**

The level of economic development of the country is likely to influence the type of business entities or groups exist in a country. Research literature reveals the fact that Developed countries like US and UK are more featured by large and complex organizations in comparison to developing countries like India, Pakistan and Sri Lanka. Financial recording and reporting practices will be more sound and complex in developed countries due to the presence of hefty number of multinational corporations.

- **Accounting and political environment**

The political environment and system prevailing in a particular country will have a greater impact on the accounting principles and practices. The way a country is politically governed can have considerable influence on accounting system. The relevance of political system can also see in many countries that are effectively run by dictators. Research literature found that Countries like France and Netherlands still follow accounting system given by their colonial rulers. Likewise countries like India, NZ, Australia and Hong Kong has adopted the accounting system of Britishers.

- **Accounting and socio-cultural environment**

A major source of influence on accounting practices and procedures is socio-culture factor. Research literature reveals

the fact that socio-cultural factor like secrecy v/s transparency, optimism v/s pessimism and uniformity v/s flexibility etc have a huge impact on the measurement of financial items as well as financial disclosure practices. Research literature found that Developed countries like US and UK are more transparent, optimistic and flexible than Japan, Germany, India and China etc when it comes to disclosure of financial records.

- **Accounting and legal environment**

Legal environment is one of the most dominating factor for diversity in accounting practices in global arena. Different countries have their own legal structure and systems. Research literature reveals out the fact that some countries are nationalistic and other are rationalistic. In other words, some countries possess strict legal system and other countries possess adaptive legal system. Countries like France and Germany follows code law which is more legalistic, detailed, prescriptive, procedural and nationalistic. On the contrary, countries like US, UK and NZ and Australia follows common law which is more flexible, adaptive and innovative in comparison to code law.

- **Accounting and Internationalization of capital market**

Research literature reveals the fact that various elements of capital market have an impact on accounting practices and procedures. Difference in financial system, emergence of new and innovative financial securities and impact of GAAR etc factors leads to diversity in accounting practices and procedures. Research literature explore out the fact that in debt oriented countries like Germany , Japan and Switzerland , financial reporting tends to be more Spartan against equity oriented countries like US , UK and Canada . The level of globalization of capital market or listing of securities at international level impacts financial recording and reporting practices to huge extent.

- **Accounting and Emergence of multinational corporations**

Developed countries tend to have capitalistic economy as well as possess large and complex organizations, where accounting problems are far more complex and detrimental than those of small organizations in developing and underdeveloped countries. Research literature explore out the fact that US and UK, organizations are relatively large, complex and owned by large number of employees against developing countries like India, Pakistan and Sri Lanka. The extent of accounting principles and practices is likely to be maximum and complex in developed countries.

- **Accounting and inflation**

An economy's level of inflation can also be perceived as a influencing factor in the context of diversity in accounting practices, policies and procedures, because it has a direct impact on the asset valuation method and because, in conditions of high inflation, it is essential to have an accounting system in line with the inflationary conditions of a particular country. Research literature reveals that Countries like US and UK are familiar with historical cost model when it comes to their accounting practices. On the contrary, countries like Bolivia and Mexico do not have luxury of persisting with the practice of historical cost model. They use inflation adjusted models of financial reporting to provide more decision relevant information in context to their economies.

- **Accounting and professional bodies**

Number of accounting professional bodies has a direct link with the quality of accounting practices, policies and procedures that prevails in a particular country. Research literature reveals the fact that the designing and standard of accounting system in a country is primarily depends upon the quality of professional bodies. Independent accounting professional bodies like (AASB) Australian accounting standard board, (AARF) Australian accounting research foundation, (ICAA) Institute of chartered accountants in Australia etc has a huge impact on Australian accounting principles and practices. At global level, (IASB) international accounting standard board and (FASB) financial accounting standard board are providing conceptual framework to satisfy the needs and nature of diverse groups of accounting users at global level which facilitate the harmonization and universality of information at global level.

- **Accounting and conceptual framework**

Conceptual framework provides a logical and consistent guide to accounting standards that prevails in a particular country. While a conceptual framework does not have a compulsory status in every country, still it provides a reference point for developing and adopting accounting standards. Research literature reveals the fact that counties like US, UK, Canada and Australia etc have invented their own version of conceptual framework in accordance with their own

environmental variables. On the contrary, developing countries like India, Pakistan, Sri Lanka have a habit to follow conceptual framework of other countries.

- **Accounting and level of enforcement**

There is a vast difference between the accounting rules, regulations and provisions and actual accounting policies, practices and procedures that prevails in a particular country. The difference between accounting regulations and principles often depends upon the level of enforcement. Research literature reveals the fact that in case of developing countries like India and China, scarcity of resources and lack of professionalism can impact the level of enforcement.

- **Accounting and report regime**

Type of report regime can also have a huge impact on the system of accounting as well as the financial reporting that prevails in a particular country. Research literature reveals the fact that countries like Austria and Germany who follow single set of rules i.e. same rules for financial as well as tax reporting looks rich in their report regime to potential investors but poor to tax authorities against countries like US , UK and India who use to follow double set of rules while reporting .

- **Accounting and e-business**

The concept of e-business which has emerged in developed countries like US, UK and Japan has now entered in developing as well as under developed countries at a very rapid rate. Companies are catching global customers but at many levels e-business has posed number of international problems. At global level, various accountants and financial executives are inventing new methods and techniques in order to tide over such problems

- **Accounting and cross border terrorism**

Cross border terrorism is not a new phenomenon particularly for Asian countries. However terrorist attack on 11 September, 2001 in US has made cross border terrorism an international issue. Research literature reveals the fact that developed countries like US in particular is not only providing financial assistance to developing and under developed countries to fight against terrorism but also business and their own accounting system to carry out transactions in an efficient manner.

- **Accounting and new concepts**

Various accounting approaches and concepts have been emerged due to the recognition of business enterprise with complex interaction of various environmental variables like economic, social, political, legal and technological etc. Research literature reveals the fact that concepts like social accounting, human resource accounting, strategic accounting, inflation accounting, international transfer pricing, consolidation and foreign currency translation etc are the precious gift of environment.

SUGGESTIONS

It is next to impossible to bring perfection in accounting system and practices all over the world due to different environmental factors prevailing in different countries but accounting differences at global level can be reduced by establishing effective accounting standards, formats, methods and procedure which are acceptable at global level. It is the duty of international accounting bodies and institutions to come together and establish such a global accounting conceptual framework which reduces the element of subjectivity and facilitate harmonization and universality of accounting at global level but still the universal accepted accounting conceptual framework continue to represent a mission for international accounting bodies and institutions.

CONCLUSION

In nutshell, accounting principles and practices are the product of environment. Different countries are indifferent to international dimensions of accounting and financial reporting due to complex interaction of environmental variables. The cumulative impact of the changed character of international capital market , predominance of MNC's , new accounting bodies , emergence of e-business, economic , legal , political , social and various other environmental variables has created the element of subjectivity and harmonization looks next to impossible . On the other side, accounting diversity in global arena has also enhanced the nature and scope of accounting at global level. Today financial experts are witnessing sound conceptual framework given by different accounting bodies as well as innovative concepts and methods to tide over the complexities related with the accounting diversity at global level.

REFERENCES

(1) Loana maria dragu (2010) , Diversity of national and international accounting practices , Annals of the University of Oradea : Economic Science 01/2010

(2) Hassan R. hassabelnaby , Ruth W. epps , Amal A. said (2003) , The Impact of Environmental Factors on Accounting Development: An Egyptian Longitudinal Study , critical perspective on accounting , volume 14 , issue 3 , pages 273 - 292

(3) Jose a lainez , susana callao (2000) The effect of accounting diversity on international financial analysis: empirical evidence , the international journal of accounting , volume 35 ,issue 1 , march 2000 , pages 65-83

(4) Joel branson , muiz jamil (2007) , The Effect of Environmental Factors on Accounting Diversity – A Literature Review ,SSRN

(5) Frederick D.S Choi (1991) , international accounting diversity: does it impact market participants? , NBER working paper no. 3590 (also reprinted no. r1679)

(6) Radebaugh, L.H., Gray, S.J., Black, E.L., (2006), International Accounting and Multinational Enterprises, (Hoboken: John Wiley & Sons, Inc).

(7) Nobes, C., (1998), «Towards a General Model of the Reasons for International Differences in Financial Reporting», ABACUS, 34 (2): 162 – 187.

(8) Salter, S.B., Niswander F., (1995), «Cultural Influence on the Development of Accounting Systems Internationally: A Test of Gray)´s (1988) Theory», Journal of International Business Studies, 26, (2): 379 – 397.

(9) Baldarelli, M.G., Demartini, P., Mošnja – Škare, L., (2007), International Accounting Standards for SMEs: Empirical Evidences from SMEs in a Country in Transition and a Developed Country Facing New Challenges, (Pula:Juraj Dobrila University of Pula, Department of economics and tourism «Dr. Mijo Mirković»)

(10) Mueller, G.G., Gernon, H., Meek, G., (1987), Accounting: An International Perspective, (Illinois: IRWIN, Homewood).

(11) D' Arcy, A., (2001), «Accounting classification and the international harmonisation debate – an empirical investigation», Accounting, Organizations and Society, (26): 327 – 349.

A SURVEY ON DETECTION AND REPLACEMENT OF FAULTY NODES IN WIRELESS SENSOR NETWORKS

Er. Kanwalpreet Kaur
M.Tech Research Scholar
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology, Amritsar
Kanwal.preet0511@gmail.com

Dr. Tanu Preet Singh
Professor & HOD
Department of Electronics & Communication Engineering
Amritsar College of Engineering & Technology, Amritsar
tanupreet.singh@gmail.com

***Abstract*- Wireless Sensor Networks (WSNs) generated interest from industrial and research perspectives of particular interest are applications in remote and hard areas in which human intervention is risky or impractical. In WSNs, it is necessary to maintaining the internodes interaction and stalwartly connected network topology at all time. A breakdown of an actor-node may cause the network to partition into disjoint blocks and changes the routing path. In wireless sensor actor network, a number of schemes have been proposed for restoring the network connectivity. This paper has analyzed the node recovery from a failure in WSNs. In WSNs, node recovery and node restoration is an active area for research. In this paper, failures have been classified into the node recovery process into two broad categories: (i) Recovery by node reposition and (ii) Replace by relay node placement. This paper also analyzes the node recovery with consideration of topology changes. This paper has highlighting the strengths and limitation of each node recovery technique.**

Index terms: **FAILURE, NODE RECOVERY, RESTORATION, TOPOLOGY MANAGEMENT.**

1. INTRODUCTION

Wireless sensor network is an important area in wireless technology. Wireless network have devices which monitors physical or environmental conditions such as temperature, pressure etc at different areas. Such sensor networks are used for vast variety of environments for commercial, civil and military applications. The main drawback of WSN is the storage, power and processing. The main challenge of sensor network is to increase the lifetime of sensor nodes. In the network, each node has battery and it is not feasible to change or recharges there is need to save energy and make it energy efficient as possible. The sensor node have three basic components such as sensing sub system for data acquisition from the physical surrounding environment, a processing subsystem for local data processing and storage[2].

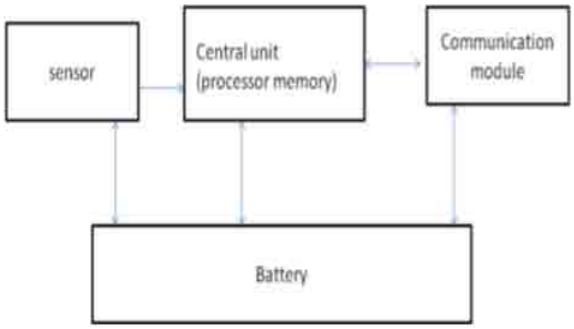


Figure 1: The sensor node architecture [2]

The accuracy of data is the main concern for the whole system's performance. Detecting nodes with faulty readings is the key issue in network management [1].So some applications or methods are designed for fault tolerant to some extent, removing the nodes with faulty reading from the system and replace that node with good ones to improve the whole system's performance [1].

1.1 WIRELESS SENSOR NETWORK

WSN is required to maintain powerfully connected network topology at all times [3].In this performance is increases with inter-actor co-ordination. The several faults lead to failures in WSN. Wireless sensor network node faults are due to following causes-the failure of modules due to fabrication process problems, environmental factors, enemy attack etc [3].The main goal of this paper is to provide the node detection and recovery of that node in WSN, So the several techniques has been designed for node recovery from failure [3].

2. LITRATURE SURVEY

The approach presented in [1] describes that the accuracy of the data is essential for whole system's performance, detecting the nodes with faulty readings is the key issue in network management. Detect the nodes with faulty readings from a system and replace them with good ones so the whole system's performance will increases and lifetime of sensor node is also increases .In WSN the two types of faults that would lead to degradation of performance. First type is functional fault, which is due to the crash of nodes, packet loss, network partition and the other type of fault is data fault detection.

The work in [3] uses the WSN which have nodes and maintains the internodes interaction. A breakdown of the nodes causes the partition of network into different blocks and also changes the routing path. In this paper, the number of schemes designed for restoring the network connection.

The work in [4][5] describes the connectivity factor of the nodes in the wireless sensor network but due to some factors the connectivity between the nodes breaks so the failure of the mission takes place and in this case the reconstruction of the network is essential. In this paper the DRFN (Detection and Replacement of a failing node) used for maintains the connectivity.

The work in [6] describes the increase in implementation and deployment of wireless sensor network for the critical applications in WSN. In this paper, it describes the implementation of sensor nodes and use of the resources available to the sensor node. The different techniques like power, data and communication management are used so the total depletion is realized.

In paper [2], it tells about the wireless sensor network, in which WSN is made up of large number of nodes which forms the network. In WSN network each node has battery which is difficult to recharge. So for the save of energy and increase the lifetime, the adaptive sleep-wake up technique is used.

In paper [7],In case of Wireless Sensor Networks (WSN) the accuracy of data is key feature for the whole system's performance, detects nodes with faulty readings is the main issue in network management. As a complementary solution to detect nodes with functional faults, this paper uses FIND, a novel method to detect nodes with data. After the nodes in a network detect a natural event, FIND ranks the nodes based on their sensing readings.

In paper [8] Wireless sensor networks (WSNs) are an important for monitoring distributed remote environments. As one of the key technologies involved in WSNs, node fault detection is indispensable in most WSN applications. It is well known that the distributed fault detection (DFD) scheme find out the failed nodes by interchange the data and mutually testing among neighbor nodes in this network., but the fault detection accuracy of a DFD scheme would decrease rapidly when the number of neighbor nodes to be diagnosed is small and the node's failure ratio is high. In this paper, an improved DFD scheme is proposed by defining new detection criteria. Simulation results demonstrate that the improved DFD scheme performs well in the above situation and can increase the fault detection accuracy greatly.

3. DRFN (Detection and Replacement technique of a failing node for connectivity maintenance in wireless sensor networks)

If a sensor node Sn fails(due to lack of energy),then one of its neighbors Ni covers or replace it and checks the functions of the failing node Sn (maintains the connectivity with its neighbors).So one of the neighbors of Ni goes to take the place by the node Ni[5].This process will continue until arriving:

1. At a node where its area is completely covered by its neighbors or
2. To reach at a node which does not have any neighbor other than the node subject for the replacement [5].So this node must checks its functions.

The idea is to imply in the replacement a node with high potential energy than a node with low potential energy. The number of neighbors and distance between the sensors is also the important criteria. The several nodes permits to share the energy consumption and so extend the global network lifetime.

In the case, when there are several neighbors of the failure node or the node chooses for substitute, what is the process to follow for elect a substitute? Many solutions are there:

a) Suppose the node which has less neighbors (less charged) to be elected. In this case, if the node is weak in terms of energy, it will be preferable to choose another node with a higher potential energy from the neighbor nodes.

b) Suppose we opt now to the election the node which has a higher potential energy. In this case, if the node has a greater number of neighbors, it means that it is a very significant relay node in case of connectivity. It will be then preferable to support the election of another node with a less number of neighbors.

Scenario Examples

Case 1: Single Failure

If the sensor node sn6 fails so in this case, the set of nodes {sn1, sn2, sn5, sn9} will be disconnected from the network. In the same way, if the node sn7 fails then is the set {sn3, sn4, sn8} which will be disconnected from the network. And if it is the nodes sn10 or sn11 fails then the set {sn13, sn14} or the set {sn12, sn15, sn16}, which will be respectively, disconnected from the network. Suppose now, that all the nodes have an equal potential energy and the distance between the nodes is the same, and that the node sn10 fails [4].

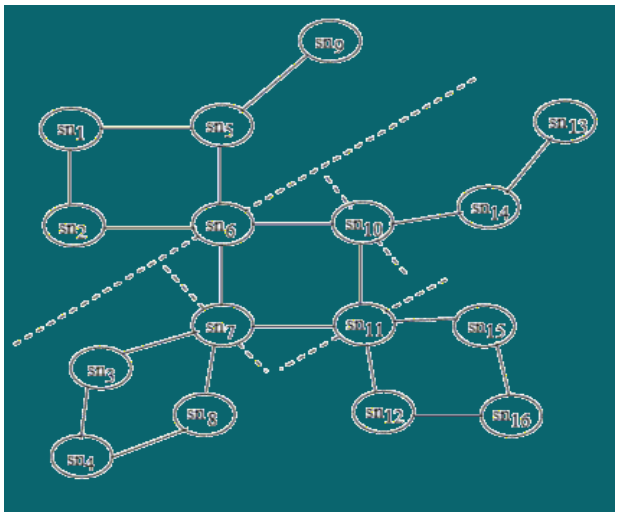


Figure 2: Connected network of mobile sensors nodes [5]

Case 2: Multiple Failures 1

If the sensor nodes sn6 and sn7 fails, then the connection breaks of the sets of nodes {sn1,sn2,sn5,sn9} and {sn3,sn4,sn8} from the network.

• Among its neighbors, the node sn2 have less number of neighbors, thus it will be elected to replace sn6.

• sn 1 is the only neighbor of sn2, it will be choose for replace it.

• The nodes sn3 and sn8 have the same number of neighbors. In this case, the node which has the smaller index (node sn3) will be elected to replace the failed node sn7 [4].

• sn 4 is the only neighbor of sn3, it will be elected to replace it[4].

The same process continues until reaching to the node which its coverage range is completely covered by its neighbors or reaches at an extremity node less significant in terms of connectivity of the global network.

Case 3: Multiple Failures 2

Suppose now the failure of the nodes sn6 and sn8. The problem in this case is: the node sn7 is the neighbor of two failed nodes, it has to participate to elect a substitute for only one of this failed nodes. If this multiple failures detected at different time, the node sn7 participates to elect the first detected failure. But if these multiple failures are detected at the same time, it must participate to elect a substitute for the failed node which is the smaller index [5]. The same process use as described in case 1 and case 2. The failing of some nodes (for example extremity nodes) does not effect the connectivity of network, but have an effect on the coverage range of network. For that, our replacement algorithm must be executed for any failed node [4]. Thus we are able to guarantee the network connectivity and coverage at the same time.

4. Recovery by Node Repositioning

The main aim of this scheme is to reposition the failure node by some healthy nodes for strong network connectivity.

A. Recovery by Inward Moving

In this method, a node failure means partitioned network and it is the most crucial task. The main issue is restoring connectivity [3].The RIM [3] method is used for move the Healthy node towards the failure position and replace t he failure node [3].

1. Failure Detection

In WSN, the failure node detects according to the manner that each node will send any message to its neighbors. After some time the missing acknowledgement message is used for detection of the failure node. After detection the failure node the recovery process is starting.

2 . Node Relocation

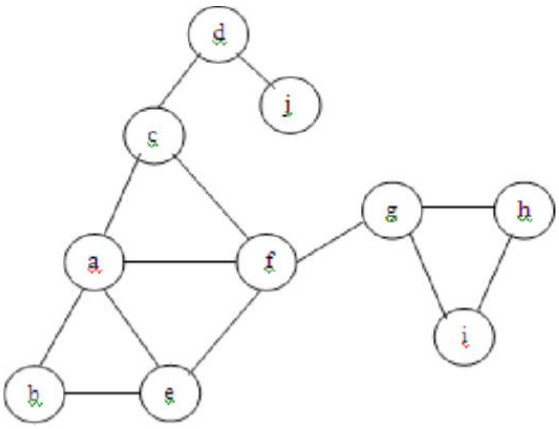


Figure 3: Wireless sensor network [3]

In the figure, it shows the wireless sensor network with the failure node. In figure f node is a failure node and its neighbor's node 'g' and 'e' sends notification message to its 1-hop neighbor's when the failure of node takes place. After the detection of node the recovery process starts.

In the figure below shows the node recovery process. Node 'f' is the failure node; node 'g' and 'e' is the neighbor for failure node 'f'. The failure node then replaces by the best candidate (BC)

node. The selection of the BC node is based on the healthy condition and distance from the failure node [3].The neighbor's node move near to the failure node. So the nodes 'g' and 'e' sends the notification message to children nodes and tells the children nodes about their movements. The children nodes (node 'i' and 'h' for node 'g') will move according to their parent nodes. If two nodes selected for best node, use node id in this case to select the BC node.

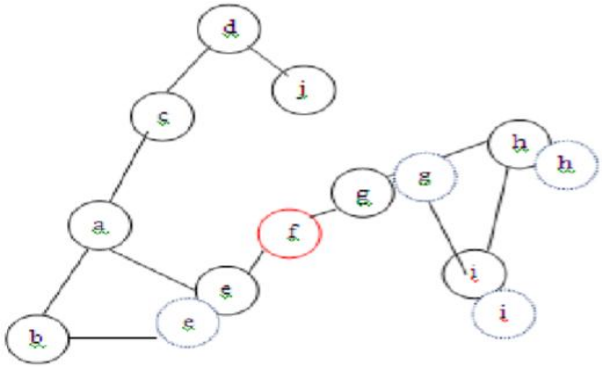


Figure 4: Node Repositioning by RIM [3]

The main features of RIM are that it is simple and effective technique.RIM uses the simple procedure to recover from serious and non serious breaks in network connectivity.
Recovery from inward motion has some limitations. Firstly, the network life time depends on many factors like mobility, traffic generation frequency and application level coordination [3].Secondly, this technique recovers only single node failure only and does not focus on the multiple node failure.

B. LeDiR

The above technique mentions only how to recover a node from failure but does not discuss how to handle the topology during recovery from failure of the node. This approach discuss the recovery from node failure with minimal topology changes [3].this approach is same as RIM but in this the movement of block takes place rather than single node movement. In LeDiR , every node is aware about the network topology so can build the shortest-path routing(SRT) table for every node[3].The detection of failure is same as RIM[3].In the figure below ,it have 19 nodes. Node 1 is a failure node and which has red circle. If the failure is detected once then the effect of failure determines. If the failure node is leaf node i.e. 17 then its effect is not very huge but if the failure node is cut vertex [3] i.e. 1, 11 and 12 then it will breaks the network connectivity.

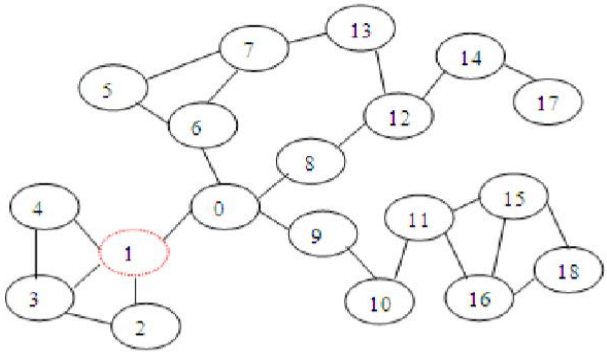


Figure 5: Wireless sensor network with faulty node[3]

1. Recovery Process

In LeDiR technique .it uses the block movement rather than the individual node movement. It starts the recovery process from the smallest block .Node 1 is the failure node and 2,3 and 4 nodes are the children nodes. So the 2,3 and 4 nodes cannot communicate with other nodes when the network breaks due to the failure node.

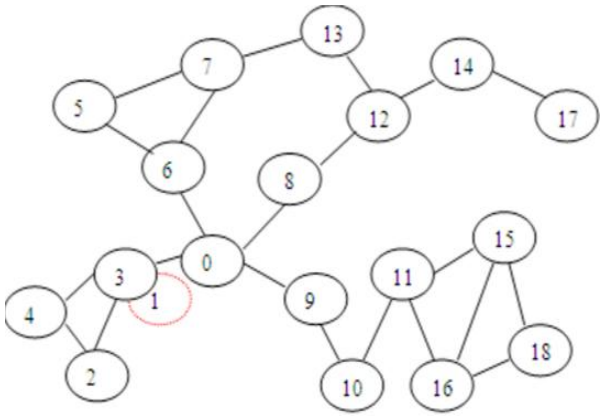


Figure 6: Replacing Failure node by LeDiR[3]

In the above figure ,if 3 and 0 nodes are the neighbors of the failure node 1.Node 3 is the gateway in the smallest block so node 3 assumed as the parent node[3].We choose the smallest block for movement because it has less number of nodes so it is easy to move in case of recovery.So the node 3 moves to replace the failure node, there is possibility that the children nodes also moves towards the parent node[3].So this approach discuss the block movement rather than the individual node movement and there is also the chance of change the topology.
The main limitation of this approach is that it cannot discuss the occurring of multiple node failure.

C. Relay Node Placement

A number of research papers have focused on the deployment of relay nodes in wireless sensor networks [3]. The main purpose of such deployment is as follows:
• Extend the lifetime of sensor networks [3] • Energy-efficient data gathering in sensor networks [3] • Balanced data gathering in sensor networks[3] • Placement of relay node during the recovering from failure. In this survey we focused on placement of relay nodes while recovering a failure node in WSNs [3]. Relay node replacement is another technique for restore the network connectivity when failure detects. The deployment of relay nodes (RNs) to restore connectivity over the disjoint partitions of a damaged WSN. There are many approaches has been discussed based on relay node placement. The idea of deploying relay nodes in sensor networks was first introduced in [8] [3], which were based on flat architectures. They have introduced relay nodes within the network to provide connectivity so that transmission powers of each sensor node can be kept low [3]. The parameters that are used for the optimization are the total-per-node minimum power needed to maintain connectivity.

5. Evaluation: Simulation Setting

C^3R			DRFN		
Displacement	Displacement time	Stay time	Displacement	Displacement time	Stay time
$sn_{10} \rightarrow sn_6$ $sn_{10} \rightarrow sn_{10}$	10 10	10	$\boldsymbol{sn_{10} \rightarrow sn_6}$	**10**	**10** **10**
10 seconds wait			$\boldsymbol{sn_{11} \rightarrow sn_{10}}$		
$sn_5 \rightarrow sn_6$ $sn_5 \rightarrow sn_5$	10 10	10		**10**	**10** **10**
10 seconds wait					
$sn_2 \rightarrow sn_6$ $sn_2 \rightarrow sn_2$	**10** **10**	**10**	$\boldsymbol{sn_{12} \rightarrow sn_{11}}$	**10**	**10** **10**
10 seconds wait			$\boldsymbol{sn_{16} \rightarrow sn_{12}}$	**10**	**10** **10**
$\boldsymbol{sn_7 \rightarrow sn_6}$ $\boldsymbol{sn_7 \rightarrow sn_7}$	**10** **10**	**10**	$\boldsymbol{sn_{15} \rightarrow sn_{16}}$	**10**	**10** **10**

Figure 7: Comparison between C^3R and DRFN

Where Sni → Snj means the displacement of the node Sni from its place towards the place of the node Snj, and Sni → Sni means return of Sni towards its initial place. We take, for the analysis, a period of time of 150 seconds[5]. During this period, the number of displacements, rep- resented in figure, carried out with the C^3R [5]approach is 8, which results that the total travelled distance is of 8d (d is the distance between the neighbors nodes)[5], compared to 5 displacements (5d) with DRFN approach. The number of nodes implied in the replacement is 5 for DRFN approach, to 4 nodes for the C3R approach (it is exactly the number of direct neighbors of the failing node)[4][5].

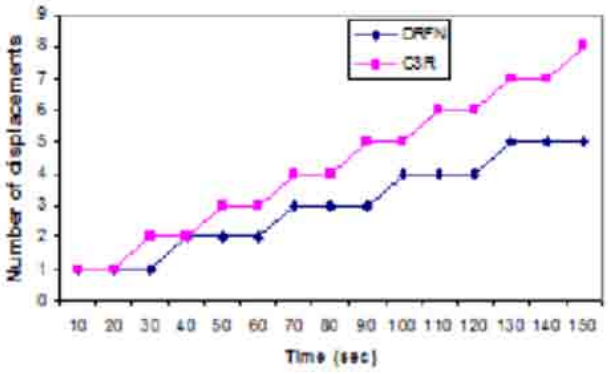


Figure 8: Displacements number of sensors per time unit [5]

the difference of the displacements number between DRFN and C3R per time unit[5]. We assume that the difference between the displacement number between DRFN and C3R extends with time.

6. Conclusion

WSNs have started to receive growing attention due to their potential in real-time applications. As mentioned earlier, in WSNs the node restoration and recovery from a failure is an active area for research. This paper has shown that there is some common problems in all the above mentioned approaches. It has been shown that the only single node failure has been considered in the most of existing research and does not focus on multiple node failure. All the schemes do not have any idea about simultaneous node recovery. Another major thing is many of the approaches could not consider the topology management while recovering a node from a failure in WSNs.

This paper has not considered the mobility of the base station so in near future the effect of mobile base station will also be considered.

7. REFERENCES

[1]Sahoo, Srikanta Kumar. "Faulty Node Detection in Wireless Sensor Networks Using Cluster"International journal of scientific & Engineering research,Volume 4,Issue 4,April-2013.

[2]Suresh,C.B.Vinutha,Dr.M.Z Kurian."Implementation of an Adaptive MAC Protocol in WSN using Network Simulator-2"International journal of science,Engineering and technology Research(IJSETR),volume 2,Issue 12,December 2013.

[3] Sathish, I. S., Lawrance Ramesh, and Sarath Kumar. "A Survey on Node Recovery from a Failure in Wireless Sensor Networks." International journal of Advanced Research in Computer Science & technology(IJARCST),vol.2,Issue 1,Jan-March 2014.

[4][5] Boudries, Abdelmalek, Makhlouf Aliouat, and Patrick Siarry. "Detection and replacement of a failing node in the wireless sensors networks." *Computers & Electrical Engineering* 40.2 (2014): 421-432.

[6] Nair, Nithya G., Philip J. Morrow, and Gerard P. Parr. "Reducing resource consumption in WSN in the event of a node failure." *Communications (NCC), 2014 Twentieth National Conference on*. IEEE, 2014.

[7] Guo, Shuo, Ziguo Zhong, and Tian He. "Find: faulty node detection for wireless sensor networks." *Proceedings of the 7th ACM conference on embedded networked sensor systems*. ACM, 2009.

[8] Jiang, Peng. "A new method for node fault detection in wireless sensor networks." *Sensors* 9.2 (2009): 1282-1294.

[9] Aliouat, Makhlouf, Zibouda Aliouat, and Miloud Naidja. "Adaptative nodes diagnosis and recovery for Wireless Sensor Networks." *Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on*. IEEE, 2012.

[10] Kamei, Sayaka, Takashi Nagai, and Satoshi Fujita. "Fast and reliable route maintenance protocols for WSN with crash and intermittent failures." *Networking and Computing (ICNC), 2011 Second International Conference on*. IEEE, 2011.

[11] Di Martino, Catello. "Software at Scale for Building Resilient Wireless Sensor Networks." *Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on*. IEEE, 2012.

[12] Bellalouna, Monia, and Afef Ghabri. "A priori methods for fault tolerance in wireless sensor networks." *Computer and Information Technology (WCCIT), 2013 World Congress on*. IEEE, 2013.

Animatronics: A New Dawn In Animation

Guneet Kaur
Assistant Professor, E.C.E. Department, A.C.E.T., Amritsar
erguneetkaur@gmail.com

Harminder Singh
Research Scholar, E.C.E. Department, A.C.E.T. Amritsar
harmindersingh.ece@gmail.com

***Abstract*- Robotics is a field which depicts robots to perform some particular functions of the biological real human beings, that functions may be of pattern recognization or may be related to the concept of long and short term memory function recalling. The basic and primary step behind the formation of artificial robot is the study of original human, and this study starts with the literature of neurons. Where neuron is the smallest and basic building element in the biological body, by studing the functionality, characteristics and parameters of this element the researchers are able to form any robotic application. In this paper the main stress is on Animatronics, how animation is done through electronics elements now a days across the globe and how the traditional animation has changed from copy-pen to animatronics.**

Keywords- Animatronic Design, PKD, SSU-1, Animation with AI, Characteristics of Animatronics.

I. INTRODUCTION

Animatronics is the combination of animation with electronics, where animation is the phenomenon of using frequent images to produce motion or making something happen in illusion world that resembles with the motion and appearance of the real world, or in other words animatronics is the collaboration of 2D and 3D, the need arrises to attract the attraction of viewers and make them feel that the animation they are seeing is natural and resembles like them, by doing so the viewer can interact with the screen with more concentration and feels that the animation is the part of his own life and has seen that as a neighbor. People can remember and relate the seen animations with their relatives and friends so they cannot forget the seen much frequently. Under animatronics the robots are made to look like humans and then they are animated on the screen to perform desired task with the help of electronic equipments. In past there was a Myth that the robots could not look like humans, this myth originates from the non-availability of gadgets and vast technology, but this vanishes out with the gradual increase in technology, advancement and requirement of applications to be provided to the world. This technology provides highly expressive mirror images of humans in illusion, with the designing, simulating and fabricating the artificial synthetic skin for mimics.

II. LITERATURE REVIEW

i. "Animatronic shader lamps avatars" by Peter Lincoln, Greg Welch, Andrew Nashel, Andrei State, Adrian Ilie, Henry Fuchs in Virtual Reality DOI 10.1007/s10055-010-0175-5 Springer-Verlag London Limited 2010. In this publication the authors has discussed about the applications of animatronics: telepresence and shader lamps avatar along with the animatronics system, design and methods.

ii. "Animatronics and Emotional Face Displays of Robots" by Asad Yousuf, William Lehman, Phuoc Nguyen and Hao Tang in International Journal of Modern Engineering Volume 7, Number 1. Under this the physical overview along with the hardware - software design is enclosed. Also, hardware interfacing architecture, future directions and challenges is published.

iii. "Physical Face Cloning" by Bernd Bickel, Peter Kaufmann, M´elina Skouras, Bernhard Thomaszewski, Derek Bradley, Thabo Beeler, Phil Jackson, Steve Marschner, Wojciech Matusik and Markus Gross. In this the authors has undergone a detailed research of face capturing with simulation, shape optimization, fabrication-design, measurements and acquisition (face scanning, fitting parameters), physical simulation of synthetic skin with material model, numerical optimization, generic optimization, thickness optimization, actuation parameter optimization, multiple pose optimization and validation optimization.

iv. "Upending the Uncanny Valley" by David Hanson, Andrew Olney, Ismar A. Pereira and Marge Zielke, Hanson Robotics Inc, Fedex Insitute of Technology, the University of Texas at Arlington Automation and Robotics Research Institute, and the University of Texas at Dallas, Institute for Interactive Arts and Engineering. In this the background and basic roots of the human interface with robots is discussed along with the humanoid intelligence architecture, animation systems and challenges in making robots function like humans.

III. ANIMATRONIC DESIGN

The main body part in animation or in animatronics is the face, as it is the first part that is seen. The first step is to take a photograph of human then convert to 3D, then follow the various optimization techniques to create a perfect animatronic figure.

Figure 1. First picture shows original photograph, second one is the scanned 3D geometry. Third-Fourth are the optimized pictures and the last one is the fabricated model after obtaining animatronic figure.

A. Face Capturing

Capturing facial expressions is the challenging task due to the versatility and motion of human face, it is the important topic of research in computer graphic field. As a human can make various emotions on the face so the main task is to fabricate the maximum of these in the animatronic figure after optimization of the photographs. There exist multiple methods of face capturing like structured light system [1] [2], passive markerless approaches [3] [4], marker based motion capture [5] etc.

B. Simulation

It is an vital part in graphic community, there boi-mechanical models of different parts of the body like face [5], hand [6], leg and various organs [7] of the body. Basically simulation is an output-oriented approach i.e. the moments of the original human body is observed and after that with the help of simulation the desired motion or output for the animatronic can be produced.

C. Material Parameters

Finding parameters that exactly or approximately matches with the human body is a time consuming but interested part. Measuring the parameters of the real world the animatronic can be provided with best suitable material parameters. It includes formation response, surface roughnes, visuals and contact sounds. A matching to the graphical parameters and the the fabricated material is necessary, several ways are there to fit measured data to computational models that are linear elastic materials [8], non-linear viscoelastic soft tissue [9], non-linear heterogeneous materials [10].

D. Fabricated Design

After finding out the material parameters the fabrication characteristics for design are worked out to implement the output on animatronic. There are various methods, one of them is to design an flexible material for fixed geometry and other one includes the constant material properties with synthetic skins, the shape can be optimized at any point with the help of simulation and material used.

E. Shape Optimization

It is a necessity for the shape of the animatronic to be optimal with the given conditions/parameters. The best

example is the aerodynamic situation in which the given problem is solved with finite elements. The shape of the synthetic skin is optimized by lowering the elastic energy with the state positions, this help in shape adaption [11] in case of varying various parameters of the fabrication. Modifying the shape sometimes become a tedious task in case of hard synthetic skin so an optimization is necessary at the initial stages to avoid last time rush. In place of considering an approximation in the implementation of the fabrication that has an advantage of stretching and contrasting the fabrication at the physical part, a dedicated proper parameterized approach is used that allows the modification in the thickness parameter only.

IV. PKD – HUMANOID INTELLIGENCE ARCHITECTURE

PKD stands for Philip K Dick, this joins the uncanny valley of humans with the robots. As there was a myth in the past that the research on humanlike robots will be unhealthy field as it can be used in an destructive way if the technique goes in wrong hands but besides this myth the innovation goes on.

In order to make a complete humanlike robot that is mirror of humans and can perform as many functions of the humans the first step is to simulate the whole social ethics to the robot in order to make sure the the output formation is not harmfull. This requires proper face and speech recognization, natural language processing, speech synthesis, motion control system and an ID. There must be a control function that can act upon to compare between good and false.

In proper working condition of the system the robot will in turn make a greeting towards a person who is smiling. The speech recognization system should listen to words carefull and then convert them to the facial expressions as well as in the moment of various body parts as an output function. The language system should have a data base of the words inbuilt to recognize the input words to act upon them in time.

Under this the robot can be made to recognize the faces of the humans by the installed camera, all this happens due to Intel Open CV application.

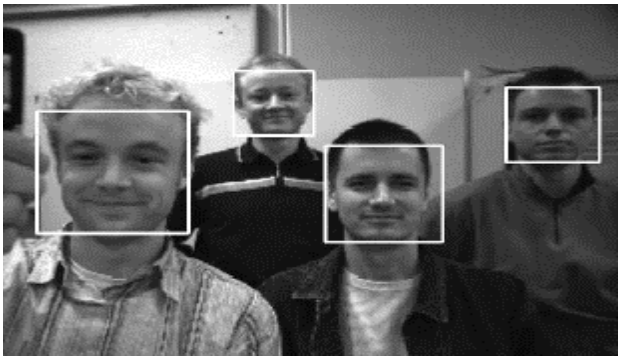


Figure 2. Facial Detection.

V. SSU-1

It is the animatronic puppet that is animated with the help of electromechanical devices, its basic is the frame. Frame is necessary for the formation of eyes, eyebrows, lips, forehead and other facial gestures like smile etc. Actuators like solenoids, servo meters, stepper motors and other mechanical mechanics are used. These actuators are responsible for the facial moments. These are behind the synthetic skin or fabrication mask of the animatronic face and are not visible as these are hidden and provide the moments silently. Sounds and puppet motions are produced by electronics and software synchronization. Springs along with DC motors are used to create up, down, left, right motions of the eyes. To increase the facial gesture speed class 2 levers with the actuators are used [12].

Two major parts in facial mechanics are:-
i. Generation and Control of facial gesture.
ii. Machines to enhance the speed.

Styrofoam head made for storing wigs was then hollowed out to fit the mechanical controls, electrical actuators and electronic components. Additional holes was done for eyes to place the mechanical eyes. Action Vectors can also be used that help in framing.
Preprogrammed embedded microcontroller is the controlling element of SSU-1 that creates original motions.

Figure 3. Possible expression with ping pong balls in place of eyes.

Figure 4. The hardware to control eyes moment and other facial expressions are installed.

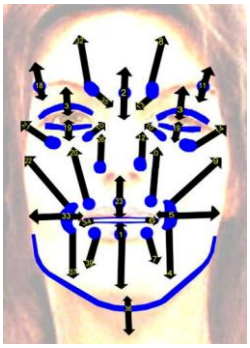


Figure. 5. Action Vectors.

The communication protocol used is DMX 512, where DMX 512 and MIDI protocols are the major standards of music industry and theme parks.
MIDI is used to play music files whereas DMX 512 has been traditionally used to control theatre lighting and has been upgraded in animatronic displays.

VI. ANIMATION WITH AI

The combination of animation with Artificial Intelligence has produced many challenges and the need of further research and innovation in the field of animatronics and computer graphics. This happens because the need arrises to join robots with the conversion, environment, perceptions,

motives and moreover decisions of the humans. Robots need to make direct eye contact with humans, to achieve this the traditional tools must be redefined and upgraded.To gain this collaboration, a larger database is required.

Following steps can be followed for a PKD based robot using AI:-
i. There must be an animation interface architecture.
ii. Motion control layer driven by AI.
iii. Managing the 3D view for enhancing the AI.
iv. Visualization/Debugging tool in case physical hardware is not present.

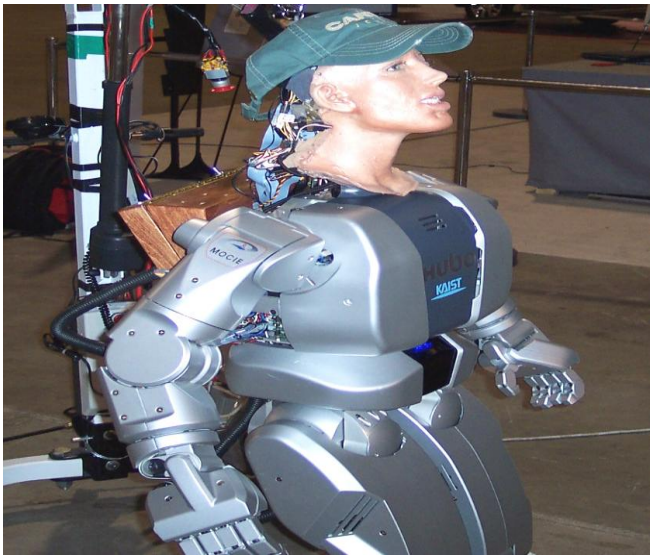


Figure 6.AI Robot.

VII. CHARACTERISTICS OF ANIMATRONICS

Following are the characteristics/parameters related with animatronics:-

A. Difference
There must be a difference between the animatronic robot and the real human.

B. Time
Time should be managed in making the realistic output of the system.

C. Numbers
Multiple characters hold attention of audience as compared to single character.

D. Non-Human
Human characters are judged on ethics but the non-human lies on appearance.

E. Surprises
Unexpected moments and expressions of the character gains audience appreciation.

F. Singing
It is observed that singing robots are more liked by the audience.

G. Personality
Scripting, dressing and moments of animatronics should be up to the mark.

H. Scale
Make difference by doing the normal things in an abnormal way seems to be interesting.

VIII. CONCLUSION

Realistic robots are believed to have an impact on the society which has an integration of moral responsibility and social ethics, this can be achieved by joining the fields of AI, Mechanical, Electronics and Software. In order to achieve the target of making humanlike things it is necessary to have a proper simulation system along with the proper materials and parameters which can be implemented on the silicon based synthetic skin. In SSU-1 the main emphasis was on the collaboration of software with hardware system, software gives commands and hardware follows/fulfills that commands using actuators and other mechanical components, proper programming results in the perfect moments of the artificial face, which can move eyes or can smile according to the input. We conclude that understanding the human behavior and then implement it to achieve an animatronic appearance which has the combination of human and robot is and task of great dedication and is full of responsibility towards the society.

IX. LIMITATIONS AND FUTURE WORK

Motions of animatronic products are still limited because of the physical and hardware constraints that originate due to the the mechanical limitations of the elements used. Currently only a single layered synthetic skin is used which is made up of single soft-tissue material but in future many possible deformations can be developed using multi-layered materials [13] which in turn can increase the moments of the actuators placed beneath the fabricated skin. SLA- Shader Lamps Avatars could be implemented at a large scale in the near future, this is basically a prototype of the original situation. The example of SLA is the scenario in which a patient needs an doctor for emergency or for an normal operation and the doctor is at a far of place, then in that condition an prototype robot, which looks like an human performs all the tasks which the original doctor needs to perform. This happens when there is connectivity of camera from patient to the doctor and the robot follows the instructions being provided by the doctor, this can be reffered to as an prosthetic presence that is otherwise not achievable. SLA enables the people to to visit the remote

places which is not practical in emergency cases or in exceptional cases through an alternate/artificial persona.

X. REFERENCES

[1] WANG, Y., HUANG, X., LEE, C.-S., ZHANG, S., LI, Z., SAMARAS, D., METAXAS, D., ELGAMMAL, A., AND HUANG, P. 2004. High resolution acquisition, learning and transfer of dynamic 3-d facial expressions. In Comp. Graph. Forum, 677–686.

[2] ZHANG, L., SNAVELY, N., CURLESS, B., AND SEITZ, S. M.2004. Spacetime faces: high resolution capture for modeling and animation. ACM Transactions on Graphics 23, 3 (Aug.), 548–558.

[3]BEELER, T., BICKEL, B., BEARDSLEY, P., SUMNER, B., AND GROSS, M. 2010. High-quality single-shot capture of facial geometry. ACM Trans. Graph. 29, 4 (July), 40:1–40:9.

[4] BRADLEY, D., HEIDRICH, W., POPA, T., AND SHEFFER, A. 2010. High resolution passive facial performance capture. ACM Trans. Graph. 29, 4 (July), 41:1–41:10.

[5] TERZOPOULOS, D., AND WATERS, K. 1993. Analysis and synthesis of facial image sequences using physical and anatomical models. IEEE Trans. Pattern Anal. Mach. Intell. 15 (June), 569– 579.

[6] GOURRET, J.-P., THALMANN, N. M., AND THALMANN, D. 1989. Simulation of object and human skin deformations in a grasping task. In Comp. Graph. (Proc. SIGGRAPH), 21–30.

[7] CHENTANEZ, N., ALTEROVITZ, R., RITCHIE, D., CHO, L., HAUSER, K. K., GOLDBERG, K., SHEWCHUK, J. R., AND O'BRIEN, J. F. 2009. Interactive simulation of surgical needle insertion and steering. ACM Trans. Graph. 28, 3 (July), 88:1– 88:10.

[8] BECKER, M., AND TESCHNER, M. 2007. Robust and efficient estimation of elasticity parameters using the linear finite element method. In SimVis, 15–28.

[9] KAUER, M., VUSKOVIC, V., DUAL, J., SZEKELY, G., AND BAJKA, M. 2002. Inverse finite element characterization of soft tissues. Medical Image Analysis 6, 3, 257–287.

[10] BICKEL, B., B¨ACHER, M., OTADUY, M. A., MATUSIK, W., PFISTER, H., AND GROSS, M. 2009. Capture and modeling of non-linear heterogeneous soft tissue. ACM Trans. Graph. 28, 3 (July), 89:1–89:9.

[11] THOUTIREDDY, P., AND ORTIZ, M. 2004. A variational r-adaption and shape-optimization method for finite-deformation elasticity. Int. J. Numer. Meth. Engng. 61, 1–21.

[12] CRISMAN, BEKEY. Grand challenges for robotics and automation: The 1996 ICRA panel discussion.

[13] BICKEL, B., B¨ACHER, M., OTADUY, M. A., LEE, H. R., PFISTER, H., GROSS, M., AND MATUSIK, W. 2010. Design and fabrication of materials with desired deformation behavior. ACM Trans. Graph. 29, 4 (July), 63:1–63:10.

A REVIEW OF THE IMAGE DEGRADED DOCUMENT USING BINARIZATION

Er.Anita Rana[1], Dr.V.K.Banga[2]
M-Tech Scholar, Department of Electronics & Communication Engg

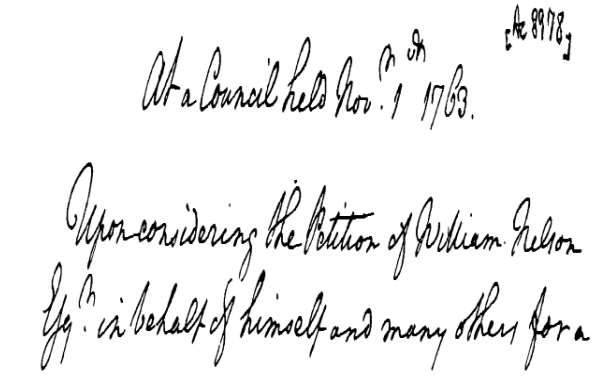
Amritsar collage of Engineering &Technology, Amritsar

Principle, Amritsar collage of Engineering &Technology, Amritsar

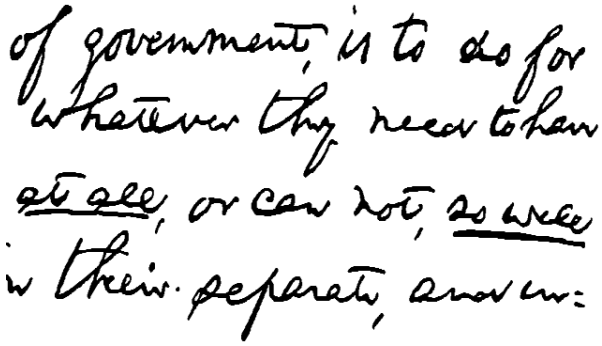
ABSTRACT: - Document binarization is very active research area for many years. Segmentation of the text from badly degraded document image like Google images, foggy images, and blur images is a very challenging task due to the high inters variation between the document background and the foreground text. The three public datasets that were used in the recent Document Image Binarization Contest (DIBCO) 2009 & 2011 and Handwritten Document Image Binarization Contest (H-DIBCO) 2010 and achieves different accuracies. Experiments on the Bickley diary dataset that consists of several challenging bad quality document images also show the superior performance in image binarization technique which is compared with different techniques.

Index Terms:-Image Processing, Pixel Classification, Degraded Document, Image Binarization, filtering.

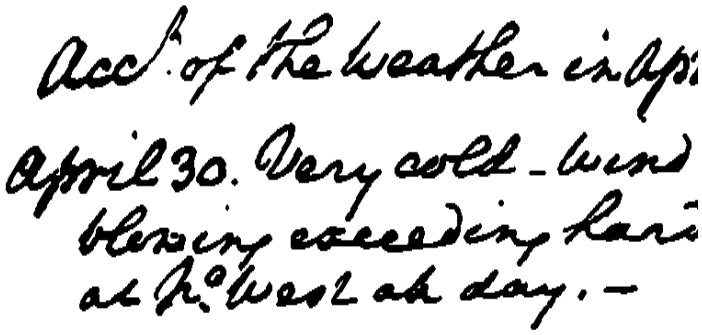
1. INTRODUCTION: - Document image binarization is an important step in the document image analysis. Its aims to segment the foreground text from the document background. A fast and accurate document image binarization technique is important for the ensuing document image processing tasks such as optical character recognition (OCR). As illustrated in Figure 1, the handwritten text within the degraded documents often shows a certain amount of variation in terms of the stroke width, stroke brightness, stroke connection, and document background. In addition, historical documents are often degraded by the bleed-through as illustrated in Figure 1(a) and (c) where the ink of the other side seeps through to the front. In addition, historical documents are often degraded by different types of imaging artifacts as illustrated in Figure 1(e). These different types of document degradations tend to induce the document thresholding error and make degraded document image binarization a big challenge to most state-of-the-art techniques. The recent Document Image Binarization Contest (DIBCO) [1], [2] held under the framework of the International Conference on Document Analysis and Recognition (ICDAR) 2009 & 2011 and the Handwritten Document Image Binarization Contest (H-DIBCO) [3] held under the framework of the International Conference on Frontiers in Handwritten Recognition show recent efforts on this issue.



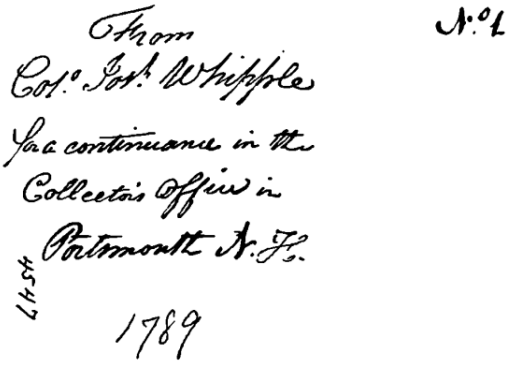
(a)



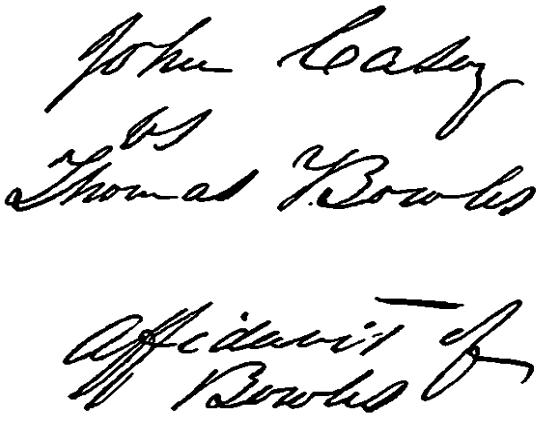
(b)



(c)



(d)



(e)

Fig.1. Five degraded document image examples taken from DIBCO, H-DIBCO and Bickley diary datasets.[1]

II. RELATED WORK: - A number of thresholding techniques [6], [7], [8], [9] have been reported for document image binarization. As many degraded documents do not have a clear bimodal pattern, global thresholding [10], [11], [12], [13] is usually not a suitable approach for the degraded document binarization. Adaptive thresholding [14], [15], [16], [17], [18], [19],[20], which estimates a local threshold for each document image pixel, is often a better approach to deal with different variations within degraded document images. For example, the early window-based adaptive thresholding techniques [18], [19] estimate the local threshold by using the mean and the standard variation of image pixels within a local neighborhood window. The main drawback of these window-based thresholding techniques is that the thresholding performance depends heavily on the window size and hence the character stroke width. Other approaches have also been reported, including background subtraction [4] texture analysis, recursive method decomposition method and combination of binarization techniques .These methods combine different types of image information and domain knowledge and are often complex.

The local image contrast and the local image gradient are very useful features for segmenting the text from the document background because the document text usually has certain image contrast to the neighboring document background. They are very effective and have been used in many document image binarization techniques [5], [14], [18], [19]. In Bernsen's paper [14], the local contrast is defined as follows:

$$C(i, j) = I_{max}(i, j) - I_{min}(i, j) \ldots\ldots (1)$$

where C(i, j) denotes the contrast of an image pixel (i, j), Imax(i, j) and Imin(i, j) denote the maximum and minimum intensities within a local neighborhood windows of (i, j), respectively. If the local contrast C(i, j) is smaller than a threshold, the pixel is set as background directly. Otherwise it will be classified into text or background by comparing with the mean of Imax (i, j) and Imin(i, j). Bernsen's method is simple, but cannot work properly on degraded document images with a complex document background. In a novel document image binarization method [5] by using the local image contrast that is evaluated as follows:-

$$C(i,j)=[I_{max}(i,j)-I_{min}(i,j)]/[I_{min}(i,j)+I_{min}(i, j)+e] \ldots\ldots\ldots\ldots(2)$$

Where *e* is a positive but infinitely small number that is added in case the local maximum is equal to 0. Compared with Bernsen's contrast in Equation 1, the local image contrast in Equation 2 introduces a normalization factor (the denominator) to compensate the image variation within the document background.

III. METHODS:-The section describes the document image binarization techniques on knowledge based studies. Given a degraded document image, an adaptive contrast map is first constructed and the text stroke edges are then detected through the combination of the binarized adaptive contrast map and the canny edge map. The text is then segmented based on the local threshold that is estimated from the detected text stroke edge pixels.

A. Contrast Image Construction:-The image gradient has been widely used for edge detection [22] and it can be used to detect the text stroke edges of the document images effectively that have a uniform document background. On the other hand, it often detects many non-stroke edges from the background of degraded document that often contains certain image variations due to noise, uneven lighting, bleed-through, etc. To extract only the stroke edges properly, the image gradient needs to be normalized to compensate the image variation within the document background. In our earlier method [5], The local contrast evaluated by the local image maximum and minimum is used to suppress the background variation as described in Equation 2.

B. Text Stroke Edge Pixel Detection:-The purpose of the contrast image construction is to detect the stroke edge pixels of the document text properly. The constructed contrast image has a clear bi-modal pattern [5], where the adaptive image contrast computed at text stroke edges is obviously larger than that computed within the document background. We therefore detect the text stroke edge pixel candidate by using Otsu's global thresholding method. The binary map can be further improved through the combination with the edges by Canny's edge detector, because Canny's edge detector has a good localization property that it can mark the edges close to real edge locations in the detecting image.

C. Local Threshold Estimation:-The text can then be extracted from the document background pixels once the high contrast stroke edge pixels are detected properly. Two characteristics can be observed from different kinds of document images [5]: First, the text pixels are close to the detected text stroke edge pixels. Second, there is a distinct intensity difference between the high contrast stroke edge pixels and the surrounding background pixels.

TABLE I
EVALUATION RESULTS OF THE DATASET OF DIBCO 2009

Methods	F-Measure(%)	PSNR	NRM($\times 10^{-2}$)	MPM($\times 10^{-3}$)	Rank Score
OTSU [12]	78.72	15.34	5.77	13.3	196
SAUV [18]	85.41	16.39	6.94	3.2	177
NIBL [19]	55.82	9.89	16.4	61.5	251
BERN [14]	52.48	8.89	14.29	113.8	313
GATO [21]	85.25	16.5	10	0.7	176
LMM [5]	91.06	18.5	7	0.3	126
BE [4]	91.24	18.6	4.31	0.55	101
Proposed method	93.5	19.65	3.74	0.43	100

Fig: Different methods evaluation measures [12].

IV.EVALUATION MEASURES:-

For the evaluation, the measures used comprise an ensemble of measures that have been widely used for evaluation purposes. These measures consist of

(i) F-Measure;
(ii) PSNR;
(iii) Negative Rate Metric and
(iv) Misclassification Penalty Metric.

Definitions:-

(i) F-Measure-

$$\text{F}-\text{Meeasur} = \frac{(2\times\text{Recall} \times\text{Precision})}{(\text{Recall} + \text{Precision})} \quad (1)$$

Where

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

TP, FP, FN denote the True positive, False positive and False Negative values, respectively.

(ii) PSNR-

PSNR= 10log (C^2/MSE)

Where $\text{MSE} = \frac{\left(\sum_{x=1}^{M}\sum_{y=1}^{N}[\left(I(x,y)-I'(x,y)\right)^2]\right)}{\text{MN}}$ (2)

PSNR is a measure of how close is an image to another. Therefore, the higher the value of PSNR, the higher the similarity of the two images. We consider that the difference between foreground and background equals to *C*.

(iii) Negative Rate Metric (NRM):-

The negative rate metric NRM is based on the pixel wise mismatches between the GT and prediction. It combines the false negative rate NRFN and the false positive rate NRFP. It is denoted as follows:

$$NRM = \frac{NR(FN) + NR(FP)}{2}$$

Where $NR_{FN} = \frac{N(FN)}{N(FN) + N(TP)}$

$$NR_{FP} = \frac{N(FP)}{N(FP) + N(TN)}$$

N_{TP} denotes the number of true positives, N_{FP} denotes the number of false positives, N_{TN} denotes the number of true negatives, N_{FN} denotes the number of false negatives. In contrast to F-Measure and PSNR, the binarization quality is better for lower NRM.

(iv)Misclassification penalty metric (MPM):-

The Misclassification penalty metric MPM evaluates the prediction against the Ground Truth (GT) on an object-by-object basis. Misclassification pixels are penalized by their distance from the ground truth object's border.

$$MPM = \frac{MP(FN) + MP(FP)}{2} \qquad (4)$$

Where $MP_{FN} = \frac{\sum_{i=1}^{N(FN)} d\hat{}i(FN)}{D}$,

$$MP_{FP} = \frac{\sum_{j=1}^{N(FP)} d\hat{}j(FP)}{D}$$

d^i_{FN} and d^j_{FP} denote the distance of the ith false negative and the jth false positive pixel from the contour of the GT segmentation. The normalization factor D is the sum over all the pixel to-contour distances of the GT object. A low MPM score denotes that the algorithm is good at identifying an object's boundary.

4. Conclusions:-

In this paper, the performance of proposed wiener filter algorithm is compared with various de-blurring techniques. The proposed algorithm has to calculate the value of F-Measure, NRM (Negative Rate Metric), PSNR (peak signal to noise ratio) and MPM (Misclassification penalty metric). This paper concludes the different methods that have been tested on various datasets. The increased interest in this competition is a two-fold proof: first, it shows the importance of binarization as a step towards effective document image recognition and second the need for pursuing a benchmark that will lead to a meaningful and objective evaluation..

REFERENCES

[1] N. Otsu, "A threshold selection method from gray level histogram," IEEE Transactions on System, Man, Cybernetics, vol. 19, no. 1, pp. 62–66, January 1978.

[2] J. Kittler and J. Illingworth, "On threshold selection using clustering criteria," IEEE transactions on Systems, Man, and Cybernetics,vol. 15, pp. 652–655, 1985.

[3] J. Bernsen, "Dynamic thresholding of gray-level images," Internation Conference on Pattern Recognition, pp. 1251–1255, October 1986.

[4] A. Brink, "Thresholding of digital images using two-dimensional entropies," Pattern Recognition, vol. 25, no. 8, pp. 803–808, 1992.

[5] N. Papamarkos and B. Gatos, "A new approach for multi threshold selection," Computer Vision Graphics and Image Processing, vol. 56, no. 5, pp. 357–370, 1994.

[6] O. D. Trier and A. K. Jain, "Goal-directed evaluation of binarization methods," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 17, no. 12, pp. 1191–1201, 1995.

[7] O. D. Trier and T. Taxt, "Evaluation of binarization methods for document images," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 17, no. 3, pp. 312–315, 1995.

[8] G. Leedham, C. Yan, K. Takru, J. Hadi, N. Tan, and L. Mian, "Comparison of some thresholding algorithms for text/background segmentation in difficult document images," International Conference on Document Analysis and Recognition, vol. 13, pp. 859–864,2003.

[9] M. Sezgin and B. Sankur, "Survey over image thresholding techniques and quantitative performance evaluation," Journal of Electronic Imaging, vol. 13, no. 1, pp. 146–165, 2004.

[10] B. Gatos, K. Ntirogiannis, and I. Pratikakis, "ICDAR 2009 document image binarization contest(DIBCO 2009)," International Conference on Document Analysis and Recognition, pp. 1375–1382, July 2009.

[11] "H-DIBCO 2010 handwritten document image binarization competition," International Conference on Frontiers in Handwriting Recognition, pp. 727–732, November 2010.

[12] S. Lu, B. Su, and C. L. Tan, "Document image binarization using background estimation and stroke edges," International Journal on Document Analysis and Recognition, vol. 13, pp. 303–314, December 2010.

[13] B. Su, S. Lu, and C. L. Tan, "Binarization of historical handwritten document images using local maximum and minimum filter," International Workshop on Document Analysis Systems, pp. 159–166, June 2010.

[14] I. Pratikakis, B. Gatos, and K. Ntirogiannis, "ICDAR 2011 document image binarization contest (DIBCO 2011)," International Conference on Document Analysis and Recognition, September 2011.

[15] L. Eikvil, T. Taxt, and K. Moen, "A fast adaptive method for binarization of document images,"*International Conference* on Document Analysis and Recognition, pp. 435–443, September 1991.

[16] I.-K. Kim, D.-W. Jung, and R.-H. Park, "Document image binarization based on topographic analysis using a water flow model,"Pattern Recognition, vol. 35, no. 1, pp. 265–277, 2002.

CONCURRENCY CONTROL : DATABASE MINING ANALYSIS

Er.PushpinderKaur
M-Tech Research Scholar
Amritsar College of Engineering and Technology,Amritsar.
pushpinderkaur406@yahoo.com

Rakesh Jaitley
Dean Placements
A.C.E.T. Amritsar

Abstract:A database system that had been optimized for in-memory storage can support much higher transaction rate. Our analysis is a decomposition of concurrency control problem into two major subproblems read –write and write-write synchronization .We describe a series of synchronization techniques for solving subproblem and how to combine these techniques into algorithms for solving concurrency control problem .Such algorithms are called concurrency control methods.We describe the correctness and structure of concurrency control method.

Keywords:DataMining,ConcurrencyControl,Deadlock,Locking,serializability,Time-stamp ordering, Synchronization,2phase locking.

INTRODUCTION

Data Mining is used to extract useful information from data.Data mining is one of computer based information system devoted to scan large amount of data repositinaries,discoverknowlegde .Data mining pursues to find out data pattern,organize information of data relationship.Thereby Data Mining out comes represent valuable support for decision making.This paper investigates concurrency control mechanisms in database mining.

Concurrency Control is the process of coordinating concurrent accesses to a database in multiuser .Concurrency Control permits the user to access the database in a multiprogrammeThe concurrency Control problem is excracted in a distributed database because of two reasons (a) users can also able to access the data stored in many different computers

The goal of concurrency control is to prevent interference among users who aresimultaneously accessing a database. Let us illustrate the problem by presenting two "canonical" examples ofinteruser interference.Both are example of an on-line electronic funds transfer system accessed via remote automated teller machines (ATMs). In response to customer requests ATMs retrieve data from a database, perform computations, and store results back into the database.

Anomaly 1 ; Lost updates. Suppose two customers simultaneously try to deposit money into the same account. In the absence of concurrency control,these two activities could interfere (see Figure 1). The two ATMs handling the two (b) Concurrency control at one computer cannot instantaneously know about the interactions at other computers.

Research on non-distributed concurrency control is focused on improvements to two-phase locking.There are about more than 20 concurrency control algorithmsthat has been proposed for distributed database.

Transaction—Processing Model

In order to understand how a concurrency control algorithm operates, one must understand how the algorithm fits into an overall DDBMS. In this section we present a simple model of a DDBMS, emphasizing how the DDBMS processes user interactions. Later we explain how concurrencycontrol algorithms operate in the context of this model.

Example of concurrency control anomalies

customers could read the account balance approximately the same time, compute two balances in parallel, and then store the new balances back into the database.The net effect is incorrect : although two customers deposistedmoney, the database only reflects one activity; the other deposit is lost by the system.

Anomaly 2 : Inconsistent Retrievals. Suppose

Two customers simultaneously execute the following transactions.

Customer 1 : Move Rs 1,000,000 from Acme corporation's saving account to its checking account.

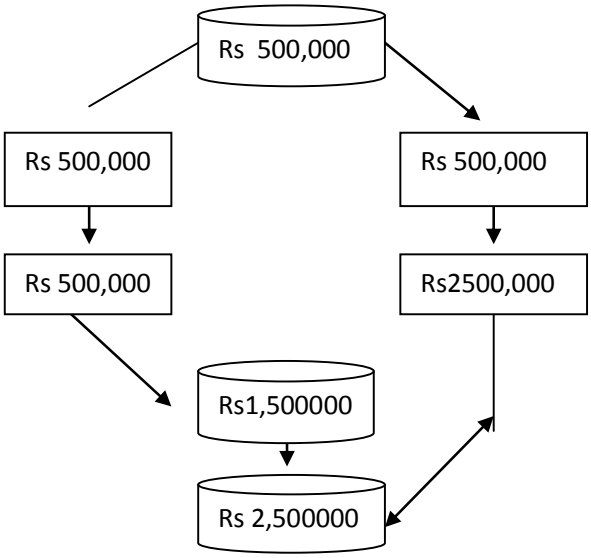


Fig 1 Lost Update Anomaly

1.1 CENTRALIZED TRANSACTION-PROCESSING MODEL

A centralized DBMS consists of one TM and one DM executing at one site. A transaction T accesses the DBMS by issuing BEGIN ,READ ,WRITE and END operations, which are processed as follow.

BEGIN: The TM initializes for T a private workspace that functions as a temporary buffer for values read from and written into the database.

READ (X): The TM looks for a copy of X in T's private workspace. If the copy exists, its value is returned to T. Otherwise the TM issues dm-read (x) to the DM to retrieve a copy of X from the database,gives the retrieved value to T, and puts it into T's private workspace.

WRITE (X, new value): The TM again checkthe private workspace for a copy of X. If it finds one, the value is updated to new-value; otherwise a copy of X with the new value is created in the workspace. The new value of X is not stored in the database at this time.

END: The TM issues dm-write (x) for each logical data item X updated by T. Each dm-write (x) requests that the DM update the value of X in the stored database to the value of X in T's local workspace. When all dm-writes are processed, T is finished executing and its private workspace is discarded.

2. CONTROL PROBLEM

In this section we review concurrency control theory with two objectives: to define "correct executions" in precise terms, and to decompose the problem into moresubproblems.

2.1 Serializability

Let E denote an execution of transactionsT1, ….Tn. E is a serial execution if no transactions execute concurrently in E; That is, each transaction is executed to be complete beforethe next one begins. Every serial execution is defined to be correct, because the properrties of transactions (see section 1.1) Imply that a serial execution terminates properly and preserves database consistency. An execution is serializable if it is computationally equivalent to a serial execution, that is, if it produce the same output and has the same effect on the database as some serial execution.

Theorm 1=[Papa77,Papa79,STEA76]
Let T={T1,……,Tm} be a set of transactions and Let E be an execution of these transactions modeled by logs{L1,……..Lm}.E is serializible if there exists a total ordering of T such that for each pair of conflicting operations Oi and Oj from distinct Transactions Ti and Tj,Oi,preceedOj,in any log L1……Lm if and only if T1 and Tj in the total ordering .
The total order hypothesized in Theorm 1 is called a serialization order.If the Transaction had executed serially in the serializableorderthe computations performed by transactions would have been identical to the computation represented by E.
To attain serialiazibility,the DDBMS must gurantee that all executions satisfy the conditions of Theorm 1,namely that Conflicting dm-reads and dm-writes be processed in certain relative orders

2.2 Paradigm for concurrency Control

In Theorm 1,rw and ww conflicts are treated together under the general notion of conflict.We can decompose the concept of serializiabilty by distinguishing two types of conflict.Let E ba an execution modeled by a set of logs.We define several binary relations on transactions in E,for each pair of transaction,T1 and Tj

(1) Ti- rwTj,if some log of E,Tt reads some data item into which tj subsequently writes;
(2) Tt-wrjTj,if in some log of E,Tt ,writes into some data item that Tj subsequently reads:
(3) Ti-wwTj,if in some log of E,Ti writes into some data item which Tj subsequently writes;
(4) Ti-rwrTj if Ti-rwTj or Ti-wrTj;
(5) Ti-Tj if Tj-rwtTj or Tt-wwTj;

3. SYNCHRONIZATION TECHNIQUES BASED ON TWO-PHASE LOCKING

Two-phase locking (2PL) synchronizes reads and writes by explicitly detecting and preventing conflicts between concurrent operations.
Before reading data item x,Transaction must own a readlock on x.
Before writing data item on x,it must own a writelock on x.
Conflicting Locks depends on the type of synchronization being performed ,thus forrw synchronization two locks conflict if (a) both are locks on same data item.
(b) one is readlock and other is writelock.
and for ww synchronization two locks conflict if (a) both are locks on the same data item
(b) both are writelocks.
Two-Phase Locking is an synchronization technique,which means that 2PL attains an acyclic relation Order.

3.2DEADLOCK : The implementations of 2PL force the transaction to wait ,if the waiting is not controlled then deadlock arise.(fig)

TRANSACTIONS

T1 BEGIN;
READ(X);WRITE(Y);END

T2 BEGIN
READ(Y):WRITE(Z);END

T3 BEGIN
READ(Z);WRITE(X),END

1 .Suppose transactions execute concurrently , each transaction isseues its READ,before each transactions issues its END.
2. This partial execution could be represented by following logs
DM A:[X1]
DM B:[Y2]
DM C;[Z3]

3. At this point T1 has readlock on x1
T2 has readlock on y2
T3 has readlock on z3

4. Before Processing, all transaction must obtain Writelocks.
T1 requires writelock on y2 until t2 releases readlock
T2 requires writelocks on Z2 and Z3
T3 requires writelocks on x1

5. But

when used for rwsynchronization.The Serialization order attained by 2PL is determined by order in which transactions obtain locks.

3.1 Basic 2PL Implemantation

An Implementation of 2PL amounts to building 2PL scheduler.
The Way to implement 2PL in distributed database is to distribute schedulers along with the database.In this readlock may be implictly requested by dm-reads and writelocks may be implictly requested by prewriter.The operation will have to be places on waiting queque for desired data otem , if requested lock cannot be granted.Special locks are required in order to release readlock.These lock releases may be transmitted in parallel with dm writes, since the dm-writes signal starts of shrinking phase.Finally when lock is release operations on the waiting queue is processe first in first

T1 cannot get writelock on y2 until t2 releases readlock
T2 cannot get writelock on z3 until T3 releases readlock
T3 cannot get writelock on x1 until T1 releases
Readlock

This is a deadlock

Figure 2 Deadlock

3.2.1DEADLOCK PREVENTION

Deadlock prevention is a scheme in which a transaction is restarted when the system is afraid that deadlock can occur.
In order to implement deadlock prevention,2PLschedulers are modified.When lock request is denied, the scheduler test the requesting transaction and another transaction that currently owns the lock.If Ti and Tj pass the test ti is permiited to wait for Tj,otherwise one of two is aborted.If Ti is again restarted,then the deadlock prevention algorith is called nonpreemtive.The Test applied by scheduler must gurantee that if Ti waits for Tj ,then deadlock cannot result.Another approach is never tolet Ti wait for Tj.This prevents deadlock.

3.2.2 DEADLOCK DETECTION

In Detection Process ,Transaction that wait for each other only aborted if deadlock actually occurs.Deadlock are detected by explictly constructing the waits for graph and search it for cycle.The major difficulty in implementing deadlock detection is constructing wait for graphs. Each 2PL scheduler can easily construct the wait for graph based on waits for relationship.However these local waits all not enough to characterize all deadlock.

One of the major cost of deadlock is the restarting of partially executed transactions.

T1 must wait for T2 to release read lock on Y2

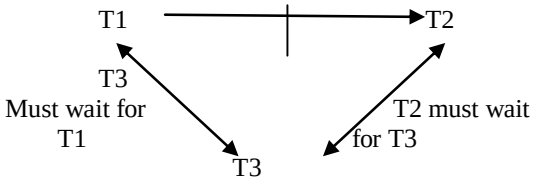


Figure 3Waits for graph

4. SYNCHRONIZATION TECHNIQUES BASED ON TIMESTAMP ORDERING

Timestamp is a technique that when a serializable technique is selected ,transaction is forced to obey that orderEach transaction is assigned a unique timestamp by its TM .TM attaches timestamp to all dm-reads and dm –writes issued on the behalf of the transaction .In order to process conflicting operations in timestamp order DM's are required.Thus the conflicting operation depends on the type of synchronization being performed.Forrw synchronization two conflict operations arises
(a) both operate on same data item
(b)one is dm-write and other is dm-read.
It is also easy to prove that T/O attains an acyclic relation when used for rwsynchronization.Inaddition ,the timestamp order is a valid serialization order.

4.1 THOMAS WRITE RULE

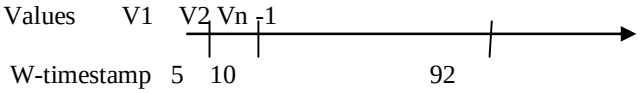
For ww synchronization the basic T/O scheduler can be optimized using an observation of THOM 79.Let W be a dm-write(x) and suppose ts(W)< W-ts(x).We can simply ignore W instead of rejecting it. This is called Thomas Write Rule.
If we use TWR then there is no need to incorprate two phase commit into the ww synchronization algorithm; the ww always accept prewrites and never buffer dm-writes.

4.2 MULTIVERSION T/O

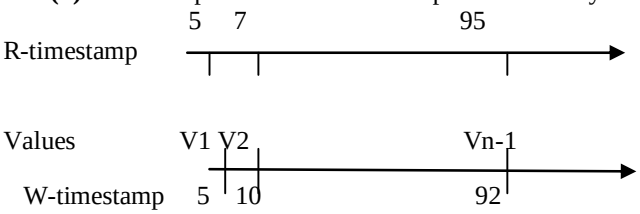
For rw synchronization the basic T/O scheduler can be improved using multiversion data items.
For each data item x there is a set of R-t's and set of (w-ts value) pairs called versions.
MultiversionT/O accomplishes rw synchronization as follows.
Let r be a dm-read(x).R is processed by reading the version of x with largest timestamp less than ts(r) and adding ts(r) to x set of R-ts's.

Let w be a dm-write(x) and let interval(w) be interval from ts(w) to smallest W-ts(x).
If we want to improve correctness of multiversion T/O,we must know that every execution is equivalent to serial execution in time stamp order.

(a) Let us represent versions of dataitem x on "timeline"

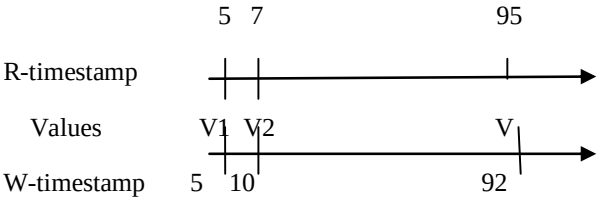


(b) Let us represent the R timestamps of x similarly:



Let W be dm-write(x) with timestamp 93.Interval W=(93,100)

To process w we create new version of x with that timestamp



However this version "invalidates" the dm-read of port(a),because if the dm-read had arrived after the dm-write, it would have read value v instead of Vn-1.Therefore we must reject the dm-write.

Fig 4:Multiversion reading and writing

CONCLUSION

Here we presented a framework for design and analysis for distributed database concurrency control algorithms. .Thus ,the framework has two main components.

(a) System model that provide common terminology for describing variety of concurrency control algorithms
(b) A problem decomposition that decomposes concurrency control algorithms into read-read and write-write synchronization algorithms.

The focus of this paper had primarily
Been the structure and correctness of synchronization techniques and concurrency control algorithms
The maim performance metrics for concurrency control algorithms are system throughput and transaction response time
The impact on each cost factor on system throughput and response time varies form system to system, application to application.
We hope and recommended that future work on distributed concurrency control will concentrate on the performance of algorithms. There are many methods, question is to arises which is the best.

REFERENCES :

[1]MENASCE, D. A., AND MUNTZ,R.R . "locking and deadlock detection in distributed database". IEEE Transaction softw. Eng.SE-5,3(May 1979),195-202.

[2] CASANOVA,M.A. " the concurrency control problem for database systems." Ph.D. Dissertation.HarwardUni.,Tech.rep. TR 17-79, Centre for research in Computing Technology, 1979.

[3] MINOURA,T "A newconcurrency control algorithm for distributed database system", in proc 4thBarkeley workshop Distributed Data Management and Computer network. Aug 1979.

[4] GARCIA –MOLINA, H. " A concurrency control mechanism for distributed database which use centralized locking controllers." In proc. 4th Barkley Workshop Distributed database and Computer Network , Aug. 1979.

[5] KAWAZU, S, MINAMI, ITOH, S, And TERANAKA, K. " Two-phase deadlock detection algorithim in distributed databases," in proc. 1979 int.Conf. very large databases (IEEE),New York.

[6] PAPDIMITRIOU, C.H.,Bernstein,P.A.AndRothnie,J.B. "Some computational problems related to database concurrency control." In proc. Conf. Theoretical computer science. Waterloo, Ont, Canada Aug. 1977.

[7]RAHIMI,S.K., and FRANTS W.R.,"A posted update approachto concurrency control in distributed database systems." In proc. 1stInt.Conf Distributed systems (IEEE), New York,Oct 1979, pp. 632-641.

[8] REIS,D " The effect of concurrency controlon database management systemPerformance."Ph.D.dissertation, Computer sciencedepartment., university. California, Barkeley, April 1979.

[9] GARDARIN, G. , And LEBAUX, P. "Scheduling algorithims for avoiding inconsistency in large databases," in proc. 1977 Int. Conf. very large data bases (IEEE), New York, pp.501-516.

[10]STEARNS,R.E.LEWIS,P.M. II

AndROSENKRANTZ,D.J ."Concurrency control for database systems," in proc. 17thSymp.Foundations Computer science (IEEE),1976,pp. 19-32.

IMAGE ENHANCEMENT TECHNIQUES – *A REVIEW*

Gurleen Kaur
M.Tech Scholar
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
gillgurleen91@gmail.com

Navneet Bawa
Associate Professor
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
bawa.navneet@gmail.com

Abstract
Image enhancement is one of the most popular algorithms used in vision applications for improving the visibility of the digital images. Recently much work is done in the different fields like medical, remote sensing, military applications etc. to improve the visibility of digital images. This paper reviews different image enhancement techniques. It has been found that the most of the existing researchers have neglected many issues. The existing methods have neglected the use of illuminate normalization to reduce the problem of poor brightness which will be presented in the image due to poor weather conditions. It is also found that the color artifacts which will be presented in the output image due to the transform domain methods got neglected most of the time.

Keywords: Image enhancement, Histogram equalization, Discrete Wavelet Transform, illuminate normalization, color artifacts.

1. INTRODUCTION

The methods for improving the quality of digital images are known as image enhancement techniques [1]. It is relatively simple, for example to make an image light or dark or to enlarge or reduce contrast. Sophisticated image enhancement software also supports several filters for changing images in a variety of ways. The main purpose of image enhancement is to process a given image so that the outcome is more appropriate than the original image for a definite use.

It sharpens image features such as edges, boundaries, or contrast to build a graphic display more useful for display and analysis [2]. The enhancement doesn't raise the inbuilt information content of the data, but it increases the active range of the selected features so that they can be detected simply [3]. Image enhancement methods can be based on either spatial or frequency domain techniques [4].

In the spatial domain method, the pixel composing of image facts are measured and the different procedures are directly applied on these pixels [4]. The image processing functions in the spatial domain may be expressed as

$$G(x.y) = T[f(x,y)] \quad (1)$$

Where $f(x, y)$ is the input image, $G(x, y)$ is the processed output image and T represents an operation on 'f' defined over some neighborhood of (x, y). Sometimes T can also be used to operate on a set of input images.

I. Image Enhancement by Grey level transformation :

The value of pixel before and after processing will be denoted by r and s. these values related by an expression s=T(r) where T is the transformation that maps a pixel value r into pixel value s. some basic intensity transformation functions are image negatives , log transformation , contrast stretching .

Image negatives: the negative of an image with grey levels in range [0,L-1] is obtained by negative transformation as shown in fig.1 which is given by the expression

$$s = L-1-r \quad (2)$$

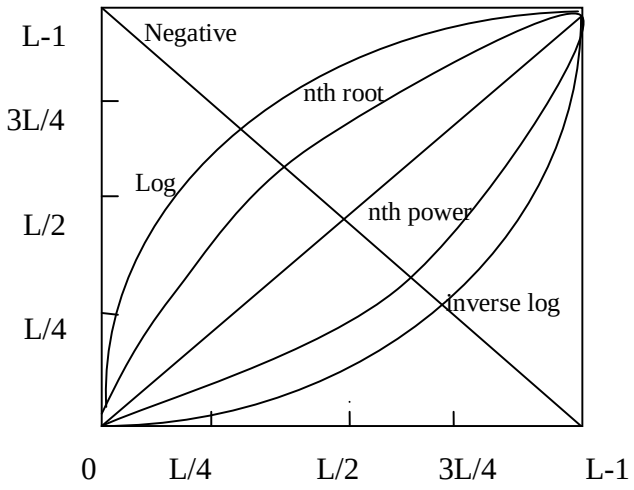


Fig 1 : Image Negatives

Log Transformation : the general form of log transformation is s=c log(1+r). we use transformation of this type to expand the values of dark pixels in an image while compressing the higher level values.

Contrast stretching: it is a process that expand the range of intensity level in an image so that it spans the full intensity range of recording medium.

Fig 2: Image (a) before (b) after enhancement

A. HISTOGRAM EQUALIZATION (HE):

It is a great point processing enhancement method that seeks to optimize the contrast of an image at all points [5]. It advances image contrast by destruction or equalizing the histogram of an image. A histogram is a table that basically counts the number of times a value appears in some data set. For an 8-bit image, there will be 256 promising samples in the image and the histogram will only count the number of times that each sample value really occurs in the image. The general shape of a histogram does not express much valuable information. The extension of the histogram relates straight to image contrast -narrow histogram distributions are representative of low contrast images; wide histogram distributions are representative of higher contrast images.

Histogram of an underexposed image will have a comparatively narrow distribution with a peak that is considerably shifted to the left and of an overexposed image will have a narrow distribution with a peak that is significantly shifted to the right [5].

Fig 3 (a) Original Image (b) Result of HE.

Histogram is a means of improving the local contrast of an image without changing the global contrast to a considerable amount [6]. This process is particularly helpful in images having large regions of related tone such as an image with a very light backdrop and dark forefront. Histogram equalization can depict hidden details in an image by stretching out the contrast of local regions and hence making the differences in the regions more observable. Histogram equalization uses Cumulative Distribution Function (CDF) as the research table. For example, for an N-bit image, histogram h, normalized CDF is given by:

$$\hat{C}j = \sum_{i=0}^{j} \hat{h}i, \quad j \in \{0,1, \ldots\ldots 255\} \qquad (3)$$

CDF gives that what proportion of samples in an image are equal to or less than value j. Normalized CDF must be rescaled to [0,255] and is then used as the research table. It increases the monotonicity. Slope of CDF is vertical where there is a group of information in the source and is horizontal where there is little information in the source. CDF of completely equalized image is straight line with slope 1.

A good quality histogram is which covers all the probable values in the gray scale used [6]. This histogram suggests that the image has fine contrast and details in the image may be observed effortlessly. Histogram equalization is the straight forward method used to accomplish enhanced quality images in black and white color scale in different application areas such as medical image processing that includes X-ray ,MRIs and CT scans ,object tracking ,speech recognition etc. The chief benefit is that it is easy and efficient. The main two disadvantages are: the destruction property; not often utilized in purchaser electronics products such as TV because it may extensively change the original brightness and cause adverse artifacts.

B. BI-HISTOGRAM EQUALIZATION (BHE)

The purpose of the bi-histogram equalization is to conserve the mean brightness of a certain image [7]. The input image is decomposed into two sub-images based on their means and the resulting equalized sub-images are enclosed by each other about the input mean. In hardware implementation, this method requires additional complex hardware than the typical Histogram Equalization (HE). For effective use of this technique, an attempt to decrease the difficulty should be ended. Many applications can be made achievable by utilizing this technique in the field of consumer electronics such as TV, VTR (Video Tape Recorder), Camcorder.

C. ADAPTIVE HISTOGRAM EQUALIZATION

Histogram equalization emphasize only on local contrast instead of overall contrast [13]. Adaptive histogram equalization overcomes from this problem, this technique applicable for overall techniques. Histogram equalization uses similar transformation resultant from the image histogram to transform all pixels. This works well when the distribution of pixel values is similar throughout the image [3].

Fig 4: a) Original image b) Output AHE

Fig4. shows the results of adaptive histogram equalization (a) original image (b) output results of adaptive histogram equalization

However when the image contains regions that are extensively lighter and darker, the contrast in those regions will not be adequately enhanced. Adaptive histogram equalization equation computed as

If (x,y) is a pixel of intensity i from the image, then we note with $m_{+,-}$ the mapping of right upper $x_{+,-}$,$m_{+,+}$ the mapping of right lower$x_{+,+}$, $m_{-,+}$the mapping of left lower $x_{-,+}$ and $m_{-,-}$ the mapping of the left lower $x_{-,-}$ then

$$m(i) = a[bm_{-,-}(i) + (1-b)m_{+,-}(\text{i})] + [1-a][bm_{-,+}(i) + (1-b)m_{+,+}(i)] \quad (4)$$

Where

$$a = \frac{y - y_-}{y_+ - y_-}, b = \frac{x - x_-}{x_+ - x_-}$$

On this by transforming each pixel with a conversion function obtained from a neighborhood region adaptive histogram equalization improves.

D. CONTRAST LIMITED ADAPTIVE HISTOGRAM EQUALIZATION

The methods that prevent the limiting the amplification called contrast limited adaptive histogram equalization. This technique is differing from above in its contrast liming. The contrast limiting procedure has to be applied for each neighborhood from which a transformation function is derived in contrast limiting adaptive histogram equalization [13].

Fig 5 : a) Original image b) Output CLAHE

Fig5. The results of contrast limited adaptive histogram equalization (a) output image (b) output result of CLAHE

The contrast amplification in the neighborhood of a given pixels value is given by the slope of the transformation function. This is proportional to the slope of the

neighborhood cumulative distribution function and therefore to the value of the histogram at the pixel value. The general equation for contrast limited adaptive histogram equalization is

$$N_{aver} = \frac{N_{CR-Xp} \times N_{CR-Yp}}{N_{gray}} \quad (5)$$

Where N_{aver} is average number of pixels, N_{gray} is number of gray level in the contextual region, $N_{CR\text{-}Xp}$is the number of pixel in the X-dimension in the contextual region, $N_{CR\text{-}Yp}$ is the number of pixel in Y-dimension in the contextual region.

2. RELATED WORK

Khan Mohd. Farhan et al. (2012) [8] proposed a weighted average multi segment HE method using Gaussian filter for contrast enhancement of natural images while preserving mean brightness. It also reduces noise present in the images. The proposed method smoothens the global histogram and decomposes it into multiple segments via optimal thresholds, and then HE is applied to each segment independently. Simulation results show that this method enhances the contrast while preserving mean brightness.

.**Huang Shih-Chia et al. (2012) [9]** proposed a histogram equalization method which is composed of an automatic histogram separation module and an intensity transformation module. In this the histogram separation module is a combination of a prompt multiple thresholding procedure and an optimum peak signal-to-noise ratio (PSNR) calculation to separate the histogram in small-scale detail. The use of the intensity transformation module can enhance the image with complete brightness preservation for each generated sub-histogram. This method not only retains the shape features of the original histogram but also enhances the contrast effectively.

Ghimire Deepak et al. (2011) [10] proposed a method for enhancing the color images based on nonlinear transfer function and pixel neighborhood by preserving details. In this method, the image enhancement is applied only on the V (luminance value) component of the HSV color image and H and S component are kept unchanged to prevent the degradation of color balance between HSV components. The V channel is enhanced in two steps. First the V component image is divided into smaller overlapping blocks and for each pixel inside the block the luminance enhancement is carried out using nonlinear transfer function. In the second step, each pixel is further enhanced for the adjustment of the image contrast depending upon the centre pixel value and its neighborhood pixel values and then original H and S component image and enhanced V component image are converted back to RGB image. The results show that this enhancement method yields better results without changing image original color in comparison with the conventional methods.

Zeng Ming et al. (2011) [11] proposed a new form of histogram for image contrast enhancement. The input image is divided into several equal-sized regions according to the intensities of gradients, their corresponding statistical values of grey levels are then modified respectively, and finally the processed histogram for the whole image is obtained by the summation of all the weighted values of regions. The fundamental characteristic of this new histogram is that the amplitudes of its components can independently reflect the contribution of the grey levels to the representation of image information. This new histogram is called grey level information histogram. Testing on x-ray images validates the effectiveness of the new histogram

N. M. Kwok et al. (2010)[12] proposed a strategy of local sector enhancement by histogram equalization. The image is first divided into sectors and they are independently enhanced by histogram equalization. Intermediate images are then generated recursively using this method and a resultant image is obtained by a weighted-sum aggregation on the basis of an intensity gradient measure. Local sectors with higher contrast dominate the others thus achieving overall global contrast enhancement. The results on imperfect illumination images show the effectiveness of this method.

3. CONCLUSION AND FUTURE SCOPE

The survey shows that the most of image enhancement techniques has certain limitations. The main limitations in earlier work include that the most of the existing techniques are based upon the transform domain methods which may introduce the color artifacts and also may reduce the intensity of the input remote sensing image. Due to transform domain methods Gaussian random noise may be present in the output images. Remote sensing and underwater images has been neglected in earlier work.

So in near future dark channel prior as the post processing function can be used to enhance the results further. To overcome the short comings of the available techniques in near future the existing transform domain method can be modified using adaptive gamma correction

to enhance the results further. However, in near future suitable simulation tool can be used.

References

[1] Lee, Eunsung, et al. "Contrast enhancement using dominant brightness level analysis and adaptive intensity transformation for remote sensing images."Geoscience and Remote Sensing Letters, IEEE 10.1 (2013): 62-66.

[2] Imtiaz, Mohammad Shamim, Tareq Hasan Khan, and Khan Wahid. "New color image enhancement method for endoscopic images." Advances in Electrical Engineering (ICAEE), 2013 International Conference on. IEEE, 2013.

[3] Sun, Yaqiu, and Xin Yin. "Optical transfer function-based micro image enhancement algorithm." Communications Workshops (ICC), 2013 IEEE International Conference on. IEEE, 2013.

[4] Teng, Yanwen, Fuyan Liu, and Ruoyu Wu. "The Research of Image Detail Enhancement Algorithm with Laplacian Pyramid." Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE, 2013.

[5] Goel, Savita, AkhileshVerma, and Neeraj Kumar. "Gray level enhancement to emphasize less dynamic region within image using genetic algorithm." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[6] Tianhe, Yu, et al. "Enhancement of infrared image using multi-fractal based on human visual system." Measurement, Information and Control (MIC), 2012 International Conference on. Vol. 2. IEEE, 2012.

[7] Chen, Shaohua, and Azeddine Beghdadi. "Natural rendering of color image based on retinex." Image Processing (ICIP), 2009 16th IEEE International Conference on. IEEE, 2009.

[8] Huang S.C , C.-H. Yeh "Image contrast enhancement for preserving mean brightness without losing image features" Engineering Applications of Artificial Intelligence 26 (2013) 1487–1492

[9] Khan Mohd. Farhan, Ekram Khan, and Z.A. Abbasi "Multi Segment Histogram Equalization for Brightness Preserving Contrast Enhancement" D.C. Wyld et al. (Eds.): Advances in Computer Science, Eng. & Appl., AISC 166, pp. 193–202. 2012

[10] Ghimire D. and J. Lee "Nonlinear Transfer Function-Based Local Approach for Color Image Enhancement" IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011

[11] Zeng Ming et al. "Improving histogram-based image contrast enhancement using gray-level information histogram with application to X-ray images" Optik 123 (2012) 511– 520

[12] Kwok N.M. , Q.P. Ha, G. Fang, A.B. Rad and D. Wang" Color Image Contrast Enhancement using a Local Equalization and Weighted Sum Approach" 6th annual IEEE Conference on Automation Science and Engineering,2010.

[13] Raju, Aedla, G. S. Dwarakish, and D. Venkat Reddy. "Modified self—Adaptive Plateau Histogram Equalization with mean threshold for brightness preserving and contrast enhancement." Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE, 2013.

[14] Gonzalez C.Rafael "Digital Image Processing" third edition Pearson.

Evaluation of Underwater Image Enhancement Techniques

Kanika Sharma[1], Er. Navneet kaur[2], Er. Ajay Sharma[3]
[1]Research scholor, [2,3]Associate Professor
Dept. of Comp. Sci. & Engg.
A.C.E.T, Amritsar

ABSTRACT

Image enhancement is a process of improving the quality of image by getting better its feature. In this paper an inclusive analysis of various enhancement techniques for such underwater images is presented. The underwater image suffers from low contrast and resolution due to deprived visibility conditions, hence an object identification become typical task. The processing of underwater image captured is necessary because the quality of underwater images distress and these images leads some serious problems when compared to images from a clearer environment. A lot of noise occurs due to low contrast, deprived visibility conditions, absorption of natural light, non consistent lighting and little color variations, and blur effect in the underwater images, because of all these reasons number of methods are there to heal these underwater images, different filtering techniques are also available in the literature for processing and enhancement of underwater images.

Keywords- RGB HSV Color model, color enhancement Light Correction Method, filters

1.INTRODUCTION

Deprived imaging condition, bad influence of light absorption and dispersal by water molecule, underwater images usually have lower contrast and stronger noise, this is a major problem for many applications of computer vision in underwater images. Underwater image enhancement techniques provided a object detection of the object which is before not exactly visible to reorganization. underwater environment(deep seas and oceans) images get blurred due to deprived visibility conditions and effects "absorption of light", "reflection of light", "bending of light, "denser medium of water", and "scattering of light" etc. These are the important factor which causes the deprived visible condition of underwater images.

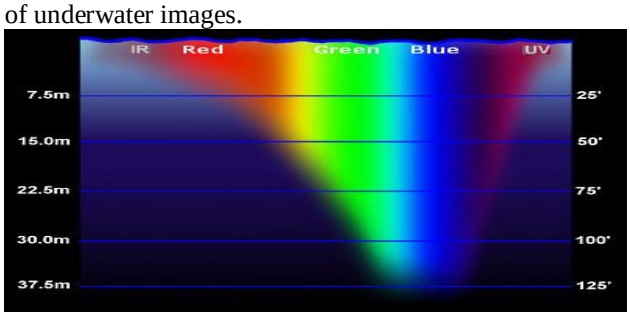


Figure 1: How deep is the sea[10]

Other reason for deprivation of underwater images is light. When ray light go through from air to denser medium water which is 800 times denser the air , its intensity partly reflect back in the air and partly enters in the water . So the partly light which enter the water slowly get start dropping at different distance under the water. E.g. at the beginning the red color starts depart at the depth of 3 m , after that orange color going to be disappear and in this way the rest of all color will gradually going to be depart at particular depth of the water.

2. IMAGE ENHANCEMENT TECHNIQUES

2.1 Contrast Limited Adaptive Histogram Equalization (Clahe)

CLAHE was initially developed for medical imaging and has which can be successful for enhancement of low contrast images such as for instance portal films. The CLAHE algorithm [11] partitions the images into tiles and applies the histogram equalization to each one. This evens out the distribution of used grey values and thus makes unseen top features of the image more noticeable. The total grey spectrum is engaged to state the image. Contrast Limited Adaptive Histogram Equalization, (CLAHE) is a better version of AHE, or Adaptive Histogram Equalization. Both overcome the precincts of standard histogram equalization. A number of adaptive contrast limited histogram equalization techniques (CLAHE) are provided. Sharp field edges could be maintained by selective enhancement technique within the field boundaries. Selective enhancement technique is accomplished by first detect the field edge in a portal image and then only processing those parts of the image that lie in the field edge. Noise could be reduced while maintaining the high spatial frequency content of the image through the use of a variety of CLAHE, median filtration and edge sharpening. An alternative of the contrast limited technique called adaptive histogram clip (AHC) can be applied. AHC automatically adjusts clipping level and moderates over enhancement of background parts of portal images. CLAHE On RGB Colour Model: The RGB colour model is definitely an additive colour model. Here red, green and blue light are added together in a variety of ways to duplicate a wide variety of colours. The worth of R, G, and B components could be the amount of the respective sensitivity functions and the incoming light. In RGB color space, CLAHE is applied on most of the three components individually and the consequence of full-color RGB may be

obtained by combining them. CLAHE on HSV colour model: HSV is really a cylindrical-coordinate representation of points within an RGB color model. In color space it describes colors when it comes to the Hue (H), Saturation (S), and Value (V). Regardless of the worth staying at either min or max intensity level, hue and saturation levels won't differ. CLAHE can just only be applied on V and S components.

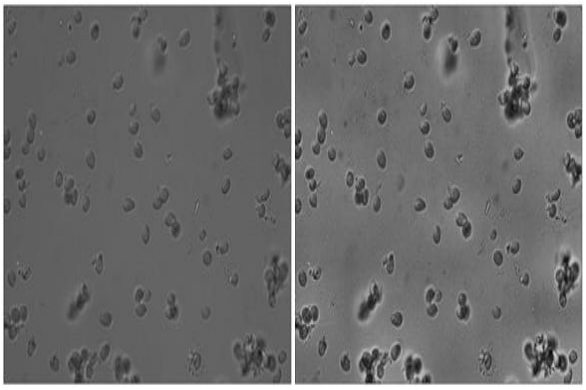


Figure.2. (a) original image (b) CLAHE image

2.2 MIX-CLAHE

When applying a mix algorithm the main element to acquire good visibility of the ultimate result is represented by the well tailored inputs and weights [3]. Unique of all the existing fusion methods (however, do not require designed to cope with underwater scenes), this fusion technique processes just a single deprived image. The overall notion of image fusion is that the processed result, combines several input images by preserving only probably the most significant top features of them. Thus, results obtained by way of a fusion-based approach fulfil the depiction hope when each area of the result presents a suitable appearance in one or more of the input images. Inside single-based image approach two inputs of the fusion process are based on the first degraded image. Enhancing solution doesn't search to derive the inputs on the basis of the physical style of the scene, since the present models are very complex to be tackled. Instead, we strive for a quick and simple technique that works generally. The very first derived input is represented by the color corrected version of the image while the second reason is computed as a contrast enhanced version of the underwater image after having a noise reduction operation is performed. This strategy was tested for sure underwater videos and images obtained from different available amateur photographer collections. Consequently, images and videos have now been captured using various cameras and setups. However, an essential observation is that individual's process only 8-bit data format although many professional cameras have the choice to shoot in the RAW mode that typically stores the unprocessed data of the camera's sensor in 12-bit format. This technique is computationally effective taking approximately 2 seconds in mat lab code for a 800×600 frame but we believe that the optimized implementation could run real-time on common hardware. By way of a general visual inspection it may be observed this technique has the capacity to yield accurate results with enhanced global contrast, color and fine details as the temporal coherence of the videos is well preserved.

Figure 3: Comparison on CLAHE methods on R2. Upper left: original underwater image. Upper right: CLAHE-RGB image. Bottom left : CLAHE-HSV image . Bottom right: CLAHE-MIX image[3].

2.3 OPTICAL MODEL

Light is attenuated when disseminating in water, the lucidity of images or videos captured under water is usually degraded to varying degrees [12]. By explore the difference in light attenuation between in atmosphere and in water, for this a new underwater optical model is derived to describe the formation of an underwater image in the true physical process, and then propose an efficient enhancement algorithm with the derived optical model to improve the acuity of underwater images or video frames. In this algorithm, a new underwater dark channel is derived to estimate the scattering rate, and an effective method is also presented to estimate the background light in the underwater optical model. Experimental results show that this algorithm can well handle underwater images, especially for deep-sea images and those images and video which are captured in muddy water. They use underwater dark channel prior to estimate the scattering rate and the transmission of blue and green light. They also employ a novel and effective light attenuation difference based method to estimate the background light of an underwater scene.

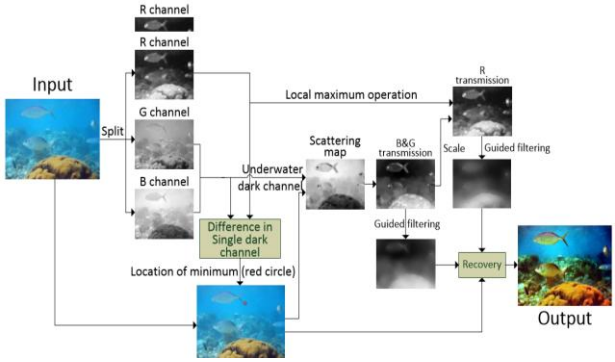


Figure 4: Frame Diagram of our method [12]

3. LITERATURE SURVEY

It represents the related literature concerning underwater images processing techniques and enhancement techniques. In 1990 Wn. R Schneider proposed to use the colored filters in Black and White photography to change the way tones of a scene record on film. Yellow filters are commonly. Because the light coming from clouds is white, it is not affected by the filter like that from the blue sky. Hence a yellow filter causes clouds to stand out more than usual. It affects the quality of the image. This kind of work was especially for the images which are presence in the air, but there were require some other technique to explore the underwater images which are captured in the deep seas and the oceans.

Pooja et al. (2014) [1] has discussed a lot of noise occurs due to low contrast, poor visibility conditions (absorption of natural light), non uniform lighting and little color variations, pepper noise and blur effect in the underwater images because of all these reasons number of methods are existing to cure these underwater images different filtering techniques are also available in this , for processing and enhancement of underwater images one of them is image enhancement using filter named median filter which enhances the image and help to estimate the depth map and improve quality by removing noise particles with the help of different techniques, and the other is RGB Color Level Stretching have used. Forward USM technique can also be used for image enhancement.

Pulung et al. (2013) [2] has proposed Success of scale-invariant feature transform (SIFT) in which image captured is limited when attempted on camera footage taken under water. This is, because of the poor image quality inherent to imaging in underwater environments and or due to turbid water and muddy water. In their research they focused to overcome this issue using a new method of pre-processing of true-color imagery taken under water based on the Contrast Limited Adaptive Histogram image Equalization (CLAHE) algorithm. CLAHE assumes that the distribution function of the pixel intensity values of an underwater-recorded image is dominated by Rayleigh scattering, and so that the noise can be removed as a function hereof. After applying the Results showed that CLAHE image enhancement method registration success of SIFT increased by 41% compared to reference method. With this research it also explained the preprocessing step of underwater image registration using image enhancement framework. This paper proposed a method for image enhancement using adaptive filtering base on CLAHE using Rayleigh Distribution.

Hitam et al. (2013) [3] has been worked on improving the quality of an underwater image has received urgent attention due to the cause of visibility of the image which is caused by physical properties of the water. Here they presented a new technique called Mix. Contrast Limited Adaptive Histogram Equalization (CLAHE) color spaces that specifically developed for underwater image improvement. This technique perform work CLAHE on RGB and HSV color spaces and both results are joint together using Euclidean rule. Tentative results show that the future approach considerably improves the visual quality of underwater images by enhancing contrast, as well as dropping noise and artifacts.

Tiejun et al. (2013) [13] has discussed when light is attenuated it disseminating in water, the lucidity of images or videos captured under water is usually degraded to varying degrees . By explore the difference in light attenuation between in atmosphere and in water, for this a new underwater optical model is derived to describe the formation of an underwater image in the true physical process, and then propose an efficient enhancement algorithm with the derived optical model to improve the acuity of underwater images or video frames. In this algorithm, a new underwater dark channel is derived to estimate the scattering rate, and an effective method is also presented to estimate the background light in the underwater optical model. Experimental results show that this algorithm can well handle underwater images, especially for deep-sea images and those images and video which are captured in muddy water. They use underwater dark channel prior to estimate the scattering rate and the transmission of blue and green light. They also employ a novel and effective light attenuation difference based method to estimate the background light of an underwater scene

Shamsuddin et al. (2013) [4] has researched on a technique "Significance level of image enhancement techniques for underwater images,". Underwater imaging is a most demanding in the area of photography specially for low contrast and low resolution images and which are captured by normal digital camera. There are many issues arise in underwater images such as low range of visibility, low contrast, non uniform lighting, blurring, intense artifacts, color degradation and noise issues . This research paper concentrated on color degradation. Major application of typical computer vision techniques to marine imaging is essential in dealing with the thought problems. Both automatic and manual level methods are used to record the mean values of the stretched histogram.

Hung et al. (2011) [6] has worked on blurred underwater images. These images is always an irritating problem in the deep-sea engineering. It proposed a competent and low complexity underwater image enhancement technique based on dark channel prior. This technique employs the median filter in its place of the soft matting method to estimate the depth map of image. Furthermore, a color improvement method is adopted to improve the color contrast for underwater image. The tentative results show that the proposed approach can well improve the underwater image and decrease the implementation time. Moreover, this technique requires fewer computing reserve and is well

appropriate for implementing on the supervision and underwater navigation in real time.

Iqbal et. al (2010) [8] has worked on the affected underwater images reduced contrast and non-uniform color cast because of the absorption and scattering of light rays in the marine environment. For that they proposed an Unsupervised Colour Correction Method (UCM) for underwater image quality enhancement. UCM is based on color matching, contrast improvement of RGB color model and contrast improvement of HSI color model. Firstly, the color cast is concentrated by equalizing the color values. Secondly, an improvement to a contrast alteration method is useful to increase the Red color by stretching red color histogram towards the utmost , similarly the Blue color is concentrated by stretching the blue histogram to the minimum. Thirdly, the Saturation and Intensity parts of the HSI color model have been useful for contrast correction to enlarge the true color using Saturation and to address the illumination problem through Intensity.

4. Underwater Image Enhancement

Image enhancement is a method of convalescing the quality of image by improving its feature and its RGB values. The underwater image processing area has received considerable attention within the last decades, showing important achievements. This paper has an inclusive survey on some of the most recent methods that have been exclusively developed for the underwater scenarios. These methods are capable of extend the range of underwater image processing, improving image contrast level and resolution superiority.

A major obscurity to process underwater images comes from light attenuation; it limits the visibility distance, at about twenty meters in clear water and five meters or less in muddy water. The light dropping process is caused by the absorption (which removes light energy) and spreading (which changes the direction of light wave path). Absorption of light and its scattering effects are because of the water itself and to other components such as dissolved organic matter or small observable floating particles. Due to this difficulty, underwater imaging suffers too many problems [1][4]: first the quick attenuation of light requires attaching a light source to the vehicle providing the essential lighting. unfortunately, synthetic lights tend to enlighten the scene in a non uniform fashion producing a bright spot in the centre of the image and poorly illuminated area surrounding. Then the distance between the camera and the scene usually induced important blue or green color (the wavelength corresponding to the red color disappears in only few meters). Then, the floating particles highly variable in kind and application, boost absorption and dispersion effects: they blur image features , transform colors and turn out glow artifacts known as “marine snow”. Lastly the non solidity of the sunken vehicle affects once again image contrast. From the pre-processing filter has been assessed on natural underwater images with and without additional synthetic underwater degradations as proposed in [1]. Underwater perturbations we added are typical perturbations observed and it have been tested with varying degrees of severity. We simulate blur and unequal illumination using Jaffe and McGlamery’s model gaussian and particles noise as additive contributions to the images and finally reduced color range by histogram operation.

5. Noise Removal

For removal of noise in the underwater image enhancement filtering is a process of removing the noisy elements which are horizontal to a variety of noise.

Noise is basically the result of errors in the process of image acquisition which result in pixel values that do not reflect the true intensities of the real view. There are several ways that remove the noise which introduced in an image, depending on how the image is created. Such as blur effect, pepper noise etc.

There are various ways in terms of filters to remove these noise two of them are:

(a) Removal of noise using Linear filter:

The linear filtering can be used to remove certain noise types. Some filters, for instance averaging or Gaussian filters, are suitable for this reason, e.g., an averaging filter is helpful for removing grain noise from a snap. As each pixel gets situate to the common of the pixels in its surrounding area, local changes caused by particle are compact.

(b) Removal of noise using median filter:

Underwater image enhancement is also done with the help of one median filter it is an efficient and low complexity underwater image enhancement method which contains two method one is the Median filter which is used to approximation the transmission of input image. The atmospheric light A is obtained by using dark channel prior. Further upgrading a color correction quality is employed to enhance the color contrast of the object in underwater. Median filtering is similar to using an averaging filter, in that every output pixel is put to an average of the pixel values in the neighborhood of the corresponding input pixel. Though, by median filtering, the value of an output pixel is determined by the median of the region pixels, somewhat than the mean. The median is greatly less responsive than the mean to great values. Median filtering is consequently well able to eliminate these outliers without declining the unevenness of the image.

(c) Photographic Unsharp Masking:

This process is used for increasing the acutance, or apparent resolution, of photographic images. For the

Photographic process a lagre format glass plate negative is contact copied on to a low contrast film or plate to create a positive image. Though, the positive copy is prepared with the copy stuff in contact with the reverse of the unique, rather than mixture-to mixture, so it is distorted. After processing this blurred positive is replaced in contact with the back of

the original negative. After light is passed throughout equally negative and in-record positive , the positive somewhat cancels a few of the information in the negative.Because the positive has been blurred intentionally, only the low frequency (blurred) information is cancelled. As well, the mask efficiently reduces the vibrant range of the original negative. Therefore, if the ensuing increased size image is recorded on contrasts pictorial paper, the fractional deletion emphasizes the high occurrence information in the original, exclusive of loss of emphasize or shadow aspect.

The consequential print appears more sensitive than one made lacking the unsharp mask: its acutance is enlarged .In the pictorial procedure, the quantity of blurring can be restricted by altering the "softness" or "hardness of the light source used for the first unsharp mask revelation, while the strength of the effect can be controlled by changing the contrast and density (i.e., exposure and development) of the unsharp mask. For traditional photography, unsharp masking is usually used on monochrome materials; special panchromatic soft-working black and white films have been available for masking photographic color transparencies. It is particularly useful to manage the density range of a transparency intended for photomechanical reproduction.

USM can increase either sharpness or (local) contrast because these are both forms of increasing differences between values, increasing slope – sharpness referring to very small-scale (high frequency) differences, and contrast referring to

larger scale (low frequency) differences. Extra dominant methods for improving tone are referred as tone mapping

6. Problem Statement

This Inclusive survey paper covers the image enhancement techniques and the image quality enhancement using filers, the atmospheric light is the major difficulty to process under water images come from the deprived visibility conditions under the water , scattering of light and light attenuation due to all the reasons underwater images suffers a lot and affect their visibility and the contrast which they contain actually. Light attenuation limits the visible distance , at about 20 meters in clear water and 5 meters or less in less muddy or turbid water.

Use Dehazing which has proposed Image enhancement by wavelength compensation and dehazing which is used to estimate the transmission of input image the atmospheric light is obtained by using dark channel prior and used to remove the noise like pepper noise, with this method the noise can be removed and the image which has less amount of noise and more improved image can be achieved but the actual color contrast and less sharp image is less accurate than the original image therefore in future there is a need of some method in addition to improve the quality of these kind of underwater images.

7. Conclusion

In this review paper, we focused on an inclusive survey on different techniques of underwater image enhancement to enhance the quality of underwater images and different techniques used Color Stretching, USM filter, dark channel, Contrast enhancement to improve underwater images. The approached used i.e. median filter , linear filter and optical model which is used to estimate the transmission of input image. The atmospheric light is obtained by using dark channel prior. Future improvement is on color correction quality is employed to enhance the color contrast of the entity in underwater and remove different noise particles and artifacts .

References

[1] Pooja sahu,neelesh gupta,"*a survey on underwater image enhancement techniques*" 2014, (IJCA) vol. 87, no.13, pp. 0975-8887.

[2] Pulung nurtantio, *"Underwater image enhancement using adaptive filtering for enhanced sift-based image matching"*,2013.

[3] Hitam, M.S.; Yussof, W.N.J.H.W.; Awalludin, E.A.; Bachok, Z., *"Mixture contrast limited adaptive histogram equalization for underwater image enhancement," Computer Applications Technology*"(ICCAT), 2013 International Conference on , vol., no., pp.1,5, 20-22 Jan. 2013.

[4] bt. Shamsuddin, N.; bt. Wan Ahmad, W.F.; Baharudin, B.B.; Kushairi, M.; Rajuddin, M.; bt. Mohd, F., *"Significance level of image enhancement techniques for underwater images*," Computer & Information Science (ICCIS), 2012 International Conference on , vol.1, no., pp.490,494, 12-14 June 2012.

[5] Chiang, J.Y.; Ying-Ching Chen, "*Underwater Image Enhancement by Wavelength Compensation and Dehazing*," Image Processing, IEEE Transactions on , vol.21, no.4, pp.1756,1769, April 2012.

[6] Hung-Yu Yang; Pei-Yin Chen; Chien-Chuan Huang; Ya-Zhu Zhuang; Yeu-Horng Shiau, "*Low Complexity Underwater Image Enhancement Based on Dark Channel Prior*," Innovations in Bio-inspired Computing and Applications (IBICA), 2011 Second International Conference on , vol., no., pp.17,20, 16-18 Dec. 2011.

[7] Balvant singh , ravi shankar mishra , puran gour, "*analysis of contrast enhancement techniques for underwater image*",2011.

[8] Iqbal, K.; Odetayo, M.; James, A.; Salam, R.A.; Talib, A.Z.H., *"Enhancing the low quality images using Unsupervised Colour Correction Method,"* Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on , vol., no., pp.1703,1709, 10-13 Oct. 2010 .

[9] Dr.g.padmavathi, dr.p.subashini, mr.m.muthu kumar and suresh kumar thakur. "*comparison of filters used for underwater image pre-processing*",2010.

[10] Bathymetric mapping- How deep is the sea?, sep 2014 (available online) www.seos-project.ev

[11] Mary Kim, Min Gyo Chung, *"Recursively Separated and Weighted Histogram Equalization for Brightness Preservation and Contrast Enhancement"*, Volume:54 , August 2008.

[12] Haocheng Wen and Tiejun Huang *"Single Underwater Image Enhancement with a New Optical Model",* IEEE , 2013.

An Efficient Content Based Image retrieval using fusion of various visual features.

Er. Sumit Chopra. [1], Dr. V. K . Banga [2]

[1] Student, Ph.D Punjab Technical University

[2]Prinicipal, Amritsar College of Engineering , Amritsar

***Abstract*— As the use of the searching digital images has increased a lot in the recent years, so a system is required which searches images from the large database on the basis of the query image and return result in the form of images which are matched with the query image. An efficient content based image retrieval system is developed in this paper by fusion of the various visual features and neural network is used for the retrieval process. The content based image retrieval is more efficient as compared to other methods as many visual features are fused together. The efficiency of the content based image retrieval is measured by drawing the recall precision graphs.**

Keywords: Content based image retrieval, neural network, fusion, recall and precision.

I. INTRODUCTION

The rapid growth in the number of large scale repositories in many domains such as medical image management, multimedia libraries, document archives, art collections and journalism have brought about the need for efficient content based image retrieval mechanisms. With the development of the Internet, and the availability of image capturing devices such as digital cameras, image scanners, the size of digital image collection is increasing rapidly. Users in many professional fields are exploiting the opportunities offered by the ability to access and manipulate remotely-stored images in all kinds of new and exciting ways. However, the process of locating a desired image in a large and varied collection can be a cumbersome process.

CBIR refers to image content that is retrieved directly, by which images with certain features or containing certain content will be searched in an image database. The main idea of CBIR is to analyse image information by low level features of an image [1] which will include color, texture, shape and spatial relationship of objects etc., and to set up feature vectors of an image as its index. Retrieval methods focus on similar retrieval and are mainly carried out according to the multi-dimensional features of an image.

Features are basis for CBIR, which are certain visual properties of an image. The features are either global for entire image or local for small group of pixels. According to the methods used for CBIR, features can be classified into low level features and high level features. The low level features are used to eliminate the sensory gap between the object in the world and information in the description derived from a recording of that scene. The high level features are used to eliminate the semantic gap between the information that one can extract from the visual data and the interpretation that the same data has for a user in given situation.

II. TEXT BASED VS CONTENT BASED – THE SEMANTIC GAP

The fundamental difference between content based and text based systems is that the human interaction is an indispensable part of the latter system. Humans tend to use high level features (concepts), such as keywords, text descriptors, to interpret images and measure their similarity. while the features automatically extracted using computer vision techniques are mostly low level features (color, texture, shape, spatial layout etc.) . In general, there is no direct link between the high level concepts and low level features.[2]

Though many sophisticated algorithms have been designed to describe colour, shape and texture features, these algorithms cannot adequately model image semantics and have many limitations when dealing with broad content image databases [3]. Many experiments on CBIR show that the low level concepts often fail to describe the high level concepts in user's minds [4].There are three types of queries in Content Based Image Retrieval systems. Level 1: Retrieval by primitive features such as color, texture, shape or spatial location of image elements. Typical query is query by example "find picture like this".

Level 2: Retrieval of objects of given type identified by derived features, with some degree of logical inference. For example, 'find picture of a flower'.

Level 3: Retrieval by abstract attributes, involving a significant amount of high level reasoning about the purpose of the objects or scene depicted. This includes retrieval of named events, of pictures with emotional or regional significance etc. For example "find the picture of a joyful crowd".

The discrepancy between the limited descriptive power of low level image features and richness of user semantics is referred to as semantic gap. Users in level 1 retrieval are usually required to submit an example image or sketch as query. But what if the user doesn't have the example image at hand? Semantic image retrieval is most convenient for users as it supports query by keywords or by texture. Therefore, to support query by high level concepts. CBIR

system should provide full support in bridging the 'semantic gap' between numerical image features and the richness of human semantic.

III. COLOR FEATURE EXTRACTION

Colour is one of the low level visual feature which is mostly used in the applications of image processing. It has the characteristic of easy calculation and invariant in image scaling, rotation and translation. Colour features of an image can be represented by a set of k bins for each channel. Many proposed methods perform the similarity matching employing this kind of matching.[10][11]

The MPEG standard includes various well defined descriptors for colour low level features. Its applications have good results in image retrieval. The DCD represents the main colours, such as red, green and blue, for several set of image contents and describes an image by using these colours which have been quantified. The SCD is defined in the HSV colour space with fixed colour quantization and employs Haar transform encoding [5]

The HSV colour space is developed to obtain an intuitive representation of colour and to nearly achieve the way in which human perceive and process colours. It is uniformly quantized into 256 bins and respectively include 16 levels in H, four levels in S and four levels in V. The Haar transform encoding is convenient for a scalable representation of descriptors as well as the complexity scalability for feature extraction and matching process. The CLD is the compact colour descriptor which employs representative colours in a 8 X 8 grid followed by a Discrete Cosine Transform (DCT) and YCrCb colour space is exploited.

IV. TEXTURE FEATURE EXTRACTION

Texture is another kind of important low level visual features. It can express the relationship between the innate surface properties of an object and surrounding environment. [6] The method of Sim exploits the discrete Fourier Transform and the modified Zernike moments for invariant texture retrieval.

Texture provides properties such as smoothness, coarseness and regularity. The three principal approaches used in image processing to describe the texture of a region are statistical, structural and spectral. Statistical approaches yield characterization of texture as smooth, coarse, grainy and so on. Structural techniques deal with the arrangement of image primitives, such as the description of texture based on properties of the Fourier spectrum and are used primarily to detect global periodicity in an image by identifying high energy, narrow peaks in the spectrum. One of the simplest approaches for describing texture is to use statistical moments of the intensity histogram of an image or region.

In [8] a texture spectrum using 3 X 3 windows. The grey level of the central pixel is compared with the other eight pixels in the window. Each pixel is assigned a value of 0 if the value is less than , 1 if its value is equal to , and 2 if its value is greater than that of the central pixel. The centre pixel is not assigned any value. Using such scheme, the number of grey levels is reduced to 3. After the reduction, the number of all combinations within the 3 X 3 window is 38 = 6851. A simple scheme was proposed to assign a number between 0 and 6560 automatically to each possible pattern of 0s, 1s and 2s in a window.

V. PROPOSED WORK

In the proposed work an efficient content based image retrieval system is developed by fusion of various visual features and selecting the best combination of visual features. The various steps of the proposed work is shown graphically in Fig. 1

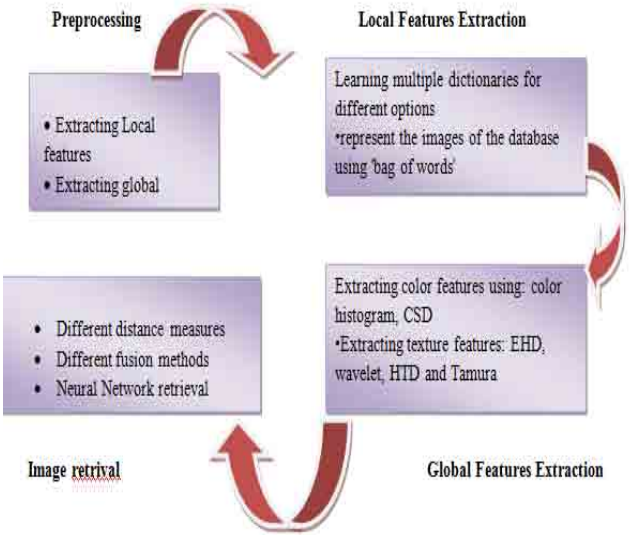


Fig. 1 The flow chart of the proposed work.

The algorithm is composed of following steps

1) Select the input query image.
2) Select the image dataset from which the query image is to be matched.
3) Select whether the extraction is to be applied locally or globally.
4) Extract the colour feature i.e. either select the colour histogram feature or colour structure descriptor
5) Apply the different distance metrics i.e. Euclidean, Quadric, KS, ch2 and KL
6) Extract the texture feature i.e edge histogram descriptor, Wavelet, Homogeneous Texture, Tamura feature
7) Select the colour sketch and extract scale invariant feature transform.
8) Apply the colour sketch
9) Then apply the fusion level.
10) Neural network are used for training and content based retrieval of images
11) Analysis is done using recall and precision values.
12) Repeat the steps 1 to 11 for multiple images.

In the proposed method the first step consists of selecting an

input query. Then the image dataset is selected from where the query image is to be retrieved. The next step consists of feature extraction. The various visual features used are colour and texture. Three schemes of colour are used for colour feature extraction namely colour histogram and colour structure descriptor. Four schemes of feature extraction are used namely edge histogram descriptor, Wavelet, Homogeneous texture and Tamura. The edge histogram descriptor resembles the color layout descriptor (CLD) in its principle of capturing the spatial distribution of edges which is useful in image matching even if the texture itself is not homogeneous. An image is partitioned into 4×4 = 16 sub-images, and 5-bin local edge histograms are computed for these sub-images, each histogram representing five broad categories of vertical, horizontal, 45^{o}-diagonal, 135^{o}-diagonal, and isotropic (non-orientation specific) edges. The resulting scale-invariant descriptor is of size 240 bits, i.e. 16×5 = 80 bins and supports both rotation-sensitive and rotation-invariant matching.

The wavelets involve filtering and subsampling. A compact representation needs to be derived in the transform domain for classification and retrieval. The mean and variance of the energy distribution of the transform coefficients for each subband at each decomposition level are used to construct the feature vector. [9]

Textures can also be classified into homogeneous, weakly homogeneous and inhomogeneous patterns. Specifically, homogeneous texture contains ideal repetitive structures, and such uniformity produces ideal repetitive structures and such uniformity produces idealised patterns. Weak homogeneity involves local spatial variation in texture elements or their spatial arrangement, which leads to more or less violates the precise repetitiveness. An inhomogeneous texture mostly refers to an image where repetition and spatial self-similarity are absent. Tamura feature represents the statistical properties of the texture. It represents the coarseness, contrast and directionality.

The various distances used for similarity measurement are Euclidean, Quadric, KS, Ch2 and KL. If we have two patterns X and Y , then the Euclidean distance will be

$$d_2(X,Y) = \sqrt{\sum_{k=1}^{d}(x_k - y_k)^2}$$

The Kullback- Leibler Distance is a non-metric distance as it does not obey the law of symmetry and triangular inequality. If

$$a = \{a_1, a_2, \ldots\ldots a_n\} \quad and \quad t = \{t_1, t_2, \ldots t_n\}$$

then KL distance will be given by

$$d(a,t) = \sum_i a_i \log_2 \frac{a_i}{t_i}$$

Artificial neural network are then used for training and retrieval of images. During training, network is trained to associate output with input patterns. When the network is used it identifies the input pattern and output the associated output pattern. The weights and threshold value used in the neural network makes neural network a powerful tool. Classification accuracy is calculated by determining the percentage of cases in which the test sets are
correctly classified. A good classification test always results from high values of accuracy. The accuracy value can be calculated as follows

$$Accuracy = \frac{True\ positive + True\ negative}{Total\ Number\ of\ images}\ .$$

Where true positive is the number of correct predictions when an instance is positive; true negative is the number of correct predictions when an instance is negative.

VI. Result and Discussion

In the proposed work a database containing 2600 images are taken. The fusion of the features is done and the results were taken for the various combination of the features. Fig. 2 demonstrate the various retrieval methods performed by using fusion of features on the Arabian horse database. Figure 3 demonstrate the plot between feature number and the precision percentage using techniques specified for retrieval of images in Fig. 2. Retrieval methods were performed for the flower database using distance level fusion.

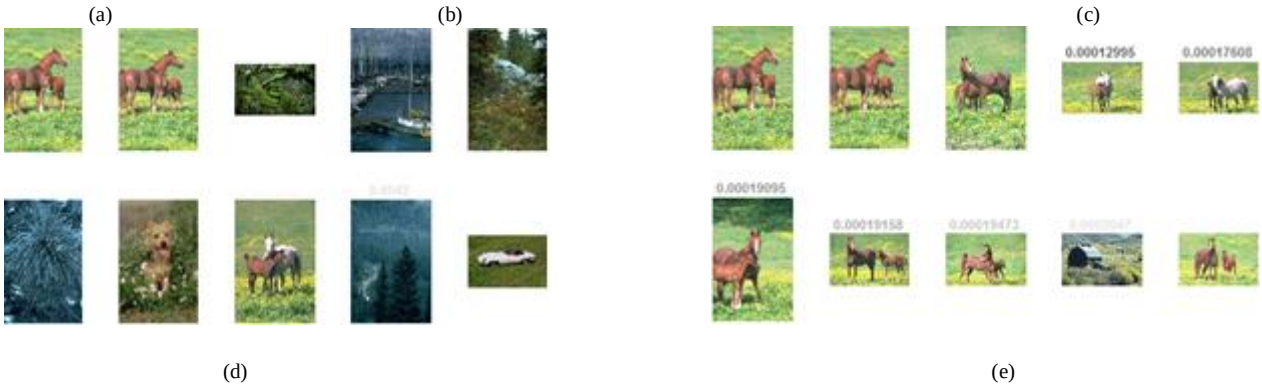
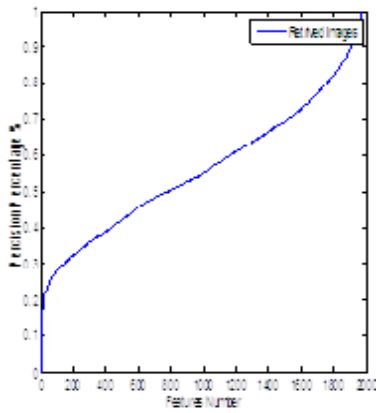
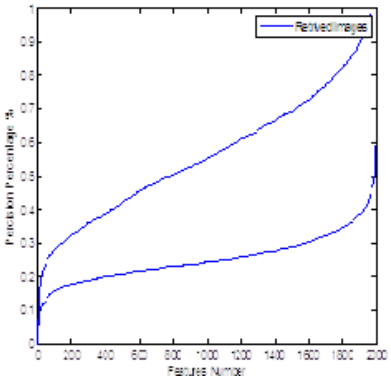


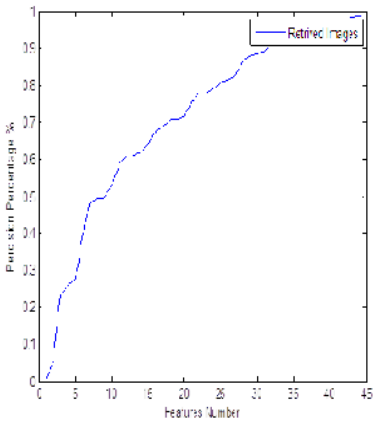
Fig.2 Image Retrieval results using fusion of features using different texture features on Corel image database (a) Query Image (b) Result of using fusion of features Colour Histogram using RGB, Wavelet, SIFT (c) Result of using fusion of features Color Histogram using RGB model, Homogeneous Texture, SIFT (d)Result of using fusion of features Color Histogram using RGB model, Tamura feature, SIFT (e) Result of using fusion of features Color Histogram using RGB model, EHD, SIFT



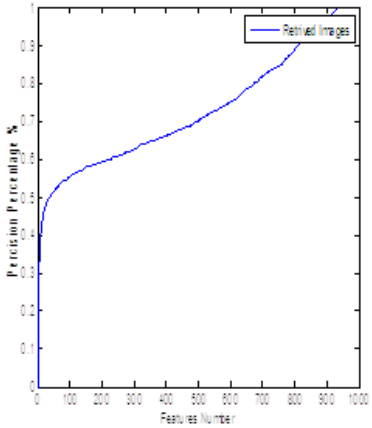
(a)



(b)



(c)



(d)

Fig . 3 Plot between feature number and precision Image for (a) Fusion of features Colour Histogram using RGB, Wavelet, SIFT (b) Fusion of features Colour Histogram using RGB model, Homogeneous Texture, SIFT (c) Fusion of features Colour Histogram using RGB model, Tamura feature, SIFT (d) Fusion of features Colour Histogram using RGB model, EHD, SIFT

Fig. 4 Image retrieval results using distance level fusion (a) Query image (b) Fusion of CSD, EHD, SIFT (c) Fusion of CSD, Wavelet, SIFT

(d) Fusion of CSD , Homogeneous texture , SIFT (e) Fusion of CSD , Tamura , SIFT

VII. CONCLUSION

We have presented a system for searching and retrieving images in this work. Regarding the "huge" size of the database our system has shown promising results over the reported results using existing techniques. Using more performance measures we can fine tune more features and possibly provide the users with the best options of retrieval as default parameters, much like Google search engine. As future work we are planning to measure the performance of more options and offer 3D visualization of the search result.

VIII. REFERENCES

[1] Datta R . , Joshi D. , Li J. , Wang J. Z. " Image retrieval ideas, influences and trends of the new age , *ACM Computing Surveys*, Vol. 40, No. 2, pp. 1-60, New York , USA, April 2008.

[2] Sethi I. K. , Coman I. L. "Mining association rules" between low level image features and high level concepts", *Proc. SPIE Data Mining and Knowledge Discovery* , Vol. 3, pp. 279-290, Orlando FL, April 16, 2001

[3] Chang S. K. , Liu. S. H. ," Picture indexing and abstraction techniques for pictorial databases", *IEEE Trans. on Pattern Anal. Mach. Intelligence*, Vol. 6, No. 4, pp. 475-483, Washington DC , USA, April 1984.

[4] Zhou X.S. , Huang T.S. "CBIR: from low-level features to high level semantics *" , SPIE , Image and Video Communication and Processing*, Vol. 3974, pp. 426-431,San Jose , CA, January 2000.

[5] Manjunath R . , Vasudevan V.V., Yamada, A. " Color and texture descriptors", *Proc. IEEE Trans. on Circuit and System for Video Technology*, Vol. 11, No.6, pp. 703-715, June 2001

[6] Wang X.Y. , Yu Y. J .,Yang H.Y., "An effective image retrieval scheme using color, texture and shape features V ", *Proc. Computer Standard and Interfaces* , Vol. 33,No. 1, pp. 59-68, January 2011

[7] Sim D. G. , Kim H. K. , Park R. H. , "Invariant texture retrieval using modified Zernike moments*", Image and Vision Computing* , Vol. 22, No. 4, pp. 331- 342, April 2004.

[8] He, D.C. and Wang Li "Texture filters based on texture spectrum, *Elsevier Pattern recognition* , Vol. 24 No. 12, pp. 1187-1195, 1991.

[9] Huang, Y., Zhao, S. Xu, L., " Vehicle Licence plate location Technique based on texture feature and color

matching", *Proc. International Conf. on Wavelet Analysis and Pattern recognition* , Vol. 28, No. 9, pp. 123-126, China, 2011.

[10] Chang B. M. "Using visual features to design a content – based image retrieval method optimized by particle swarm optimization algorithm", *Elsevier Engineering Applications of Artificial Intelligence*", Vol. 26, pp. 2372- 2382, 2013

[11] ElAlami M. E. "A new matching strategy for content based image retrieval system" *Elsevier Applied Soft Computing*, Vol. 14, pp. 407- 418, 2014.

Study of Recently Developed Image Segmentation Algorithms

Seema Panwar
Department of Electronics and communication
PEC University of technology
Chandigarh, India
seema.panwar3@gmail.com

Bipan Kaushal
Department of Electronics and communication
PEC University of technology
Chandigarh, India
bipan_pec@yahoo.com

Abstract— ***Image segmentation is one of the most essential step in image processing. It has also emerged out as one of the fine area where research is going on. There are basically two approaches of image segmentation i.e. discontinuity based and region based. In discontinuity based approach partition of image is done based on some abrupt changes in the intensity level. So in discontinuity based approach our interest is only on finding the isolated points, lines or edges. But a different approach is followed for region based approach. Here the pixel which are similar in some sense are grouped together. There are further three kind of segmentation under similarity based approach and these are thresholding, region growing and region splitting and merging. In this paper a brief review of some of the new image segmentation algorithms is carried out and results their of are discussed.***

Keywords— Image segmentation, sobel operator, normalized cut, graph partitioning, JSEG algorithm, ant weight lifting algorithm

I. INTRODUCTION

An important technique in the analysis of digital images is the division of an image in meaningful and distinct structures. It facilitates visualization, representation, analysis and many other tasks related to digital processing of images.

Image segmentation basically is a process of subdividing an image into its constituent parts so as to further analyze each of its constituent parts in detail. The extent to which segmentation is carried out depends on the problem under consideration. Therefore segmentation should stop when the object or the region of interest is detected. This subdivision is basically application dependent. More precisely it is the process of allocating certain label to each pixel so that each pixel shares a common characteristic.

A large variety of algorithms for segmentation of images have been presented during the last decade. Although it is not possible to carry out disjunctive categorization, since even two verily different approaches of segmentation could share properties which defy distinctive categorization.

Image segmentation finds application in several fields like industries, medical image processing, remote sensing, real time visual tracking and so on. Each field needs an optimum segmentation approach. In the whole image analysis process, proper image segmentation determines the whole success or the failure of the image analysis. Image segmentation is very important task, so we should try to find some robust image segmentation algorithm.

II. COMPARATIVE VIEW OF SEGMENTATION ALGORITHMS

Comparative study of some of the recently developed algorithms for image segmentation is carried out here.

A. Image Segmentation Based on Sobel Operator and Maximum Entropy

The earlier methods like threshold method, regional growth method, edge method were successful in many fields, but these methods can't be applied in all applications. The traditional sobel based image segmentation suffer from many disadvantages like low accuracy, ambiguity of image segmentation, low contrast etc. So in order to overcome all these flaws an improved sobel operator based on 2-d maximum entropy was put forward [1]

Here, in this method initially, an early image segmentation is carried out, then using the sobel operator real edges are detected, and then the threshold value obtained from the sobel edge detection is applied to 2-d maximum entropy image segmentation method.

In order to tell the superiority of the algorithm the author here has compared the PSNR and the time spent of the six image segmentation algorithm. The information is illustrated in table 1.

TABLE 1. IMAGE QUALITY ASSESMENT STANDARDS

Algorithm	PSNR/dB	Time
Algorithm of threshold segmentation	20.723	0.578
Wavelet image segmentation algorithm	21.861	0.641
Segmentation of sobel operator	25.782	0.391
The maximum entropy segmentation	25.782	0.906
Image of canny operator	21.384	2.531
Algorithm of this paper	29.433	1.226

From table 1 we can see that the proposed method has many advantages like it is robust; highly accurate i.e. it retains the important information of the image and gives high PSNR value.

B. Normalised Cut and Clustering Algorithm (NC)

When we are dealing with object recognition, the basic segmentation method fails to give efficient result. So, there arises a need for more reliable segmentation technique. Color information is a domain which can be used for image segmentation.

Image segmentation method can be categorized as- global knowledge based segmentation, edge-based segmentation and region based segmentation [2, 3].These segmentation methods were having few drawbacks. Like, in global knowledge based segmentation method it was difficult to obtain an optimum threshold. Similarly edge based segmentation do not guarantee forming closed boundaries in order to recognize the distinguishable segments. Graph based algorithm suffered from algorithm complexity [4], when applied to real time system.

In order to overcome all of the drawbacks a new algorithm called the normalized cut and clustering algorithm was introduced [5].

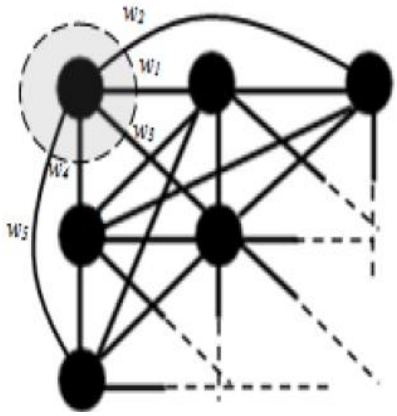


Fig. 1 Weight assigning for paired pixel

Fig. 1 illustrates the example of assigning weight [3]. In this method a graph is constructed with the collection of vertices (V) and edges (E).

The vertices are represented by pixels. Since the pixel hold the color information so by grouping these pixels according to their similarities and dissimilarities can lead to segmentation. The edge is assigned with a weight w (i,j). Each weight is a measurement of similarity between the pixel i and pixel j. Fig. 1 illustrates the example of assigning weight [3].

Then graph partitioning is done by cutting out edges with low value of weight. This is called the minimum cut method. The method suffers from isolated pixels problem which is further removed by using normalized cuts. Then k-means clustering of Eigen vectors is done.

An image that has a size of m x n pixels will require NC to have a **W** matrix with a size of (m x n) x (m x n). This will result in a large amount of computation. So in order to reduce the large memory usage a 2-stage image segmentation is performed.

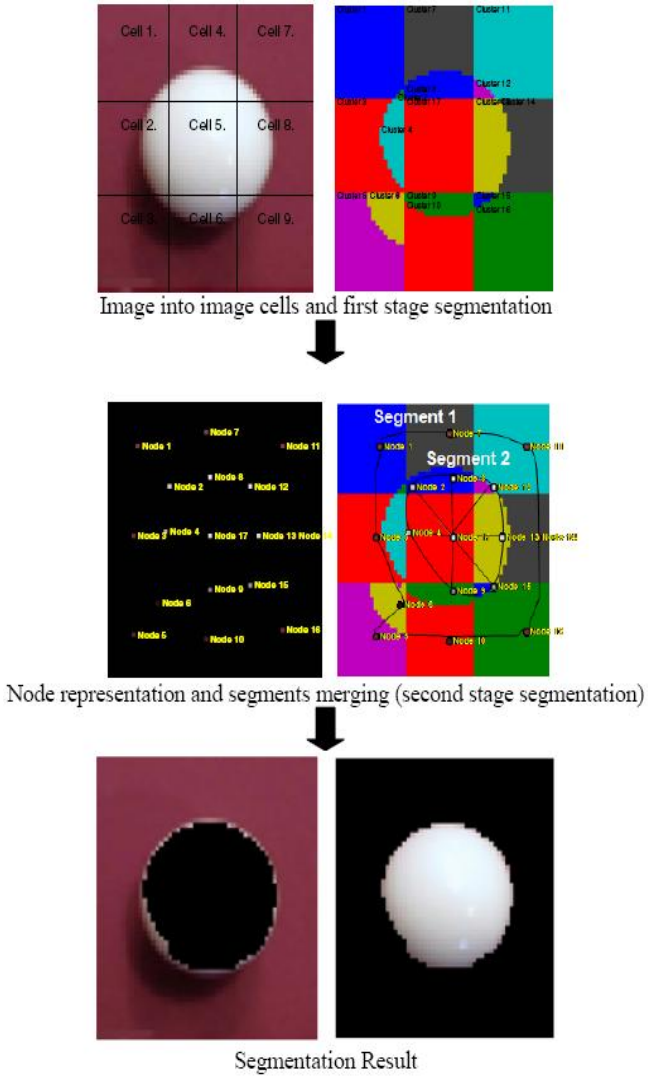


Fig. 2 Summary of two stage image segmentation

Fig. 2 illustrates the two stage image segmentation. In the first stage a high resolution image is divided into small sub-images and in the second stage segment merging is done.

The two stage image segmentation helps to reduce the unnecessary image segmentation thus reducing the computation time.

C. *Image Segmentation Based on JSEG and Normalised CUTS*

There are several segmentation technologies based on region growing, edge detection, wavelet transform but there is no algorithm which can be fit into different type of images. Among the various methods the JSEG algorithm is based on unsupervised color texture and regional growth. The two shortcomings it suffers from are -the need for large J value computation which results in high algorithm complexity and the other is poor merging.So, a new segmentation algorithm which combined the graph theory and JSEG algorithm, namely J-Cut algorithm was proposed [6].

TABLE 2. TIME COMPARISON TABLE

Pictures label	JSEG/s	J-cut/s	Absolute reduction time/s	Relative reduction time/ %
1	5.016	3.359	1.657	33.03
2	4.359	3.628	0.731	16.77
3	4.655	3.513	1.152	24.69
4	6.011	4.567	1.444	24.02
5	4.738	3.866	0.872	18.40
Average	**4.958**	**3.787**	**1.170**	**23.39**

Table 2 illustrates the comparison of the performance of J-cut and JSEG algorithm based on the simulation results obtained from the MATLAB. The table shows that the J-CUT method reduces the computation time by 20%. So it can be deduced that the J-CUT method is better than the earlier JSEG method.

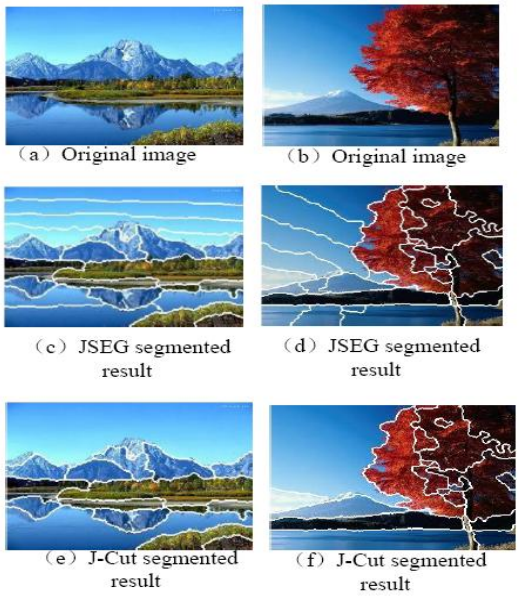


Fig. 3 The segmentation result of J-CUT and JSEG algorithm

As can be observed from fig 3 (c) and (d) that the JSEG algorithm suffers from the over segmentation problem. In picture (c) we can see that the sky is divided into many parts but according to human perception it should be considered as the single class. But contrary to this in picture (e) the whole sky is segmented as a single area. So this method is simple, effective and easy to understand. It reduces the complexity involved with JSEG algorithm and makes region merging accurate.

D. *Image Segmentation Based on K Means Clustering and Watershed Technique*

Watershed algorithm belongs to the region based segmentation. The idea basically comes from geography where watershed is depicted as an area of land that feeds all the water running under it and draining off of it into a body of water. Any grayscale image can be thought of as a topographic surface where high intensity denotes peak and low intensity denotes valleys. Every valley is filled with different colored water [7]. As the water rises, depending on the gradients nearby, water from different valleys, with different colors will start to merge. To avoid this, barriers are built at the locations where water merges. This work of filling water and building barriers is continued until all the peaks are under water. Then the barriers created give the segmentation result. Watershed technology changes the image into another image whose catchment basins are the objects to be identified. K-means clustering is one of the most widely used clustering method which divides the objects into clusters such that objects in the cluster are similar in properties to each other than to the objects in another cluster [8].

Discrete entropy and root mean square error is used to evaluate effects of K-means clustering and watershed segmentation algorithm. Watershed algorithm find wide application in the medical image processing because of many advantages like its simplicity, speed, border closure, high accuracy and its usefulness even if the contrast is poor.

E. *Image Segmentation By Ant Weight Lifting Algorithm (AWL)*

Several image segmentation techniques like k-means clustering, watershed technique, N-cut method are discussed above [9]. K-means clustering is threshold based image segmentation technique which has the disadvantage that the number of k becomes difficult to determine. Similarly watershed technique suffered from over segmentation. Region based and region growing segmentation always involves some kind of pre-processing or post processing which leads to over segmentation or under segmentation. Therefore there arises a need to develop an algorithm which segments the image in an optimum and convenient way. AWL algorithm provides a solution to the above issues [10].

In this algorithm, each of the input image is considered as a food source where each pixel representing the calorific value.

Each ant is assigned a particular range of the calorific value. Each ant starts moving randomly in order to find the pixel value lying in its range. Having finished the search, the entire quantum is replaced by the mean of the pixel collected by each ant thus creating the segments. Correlation between the real and the segmented image is used to find the degree of accuracy in the segmentation process. This algorithm was applied to several test cases.

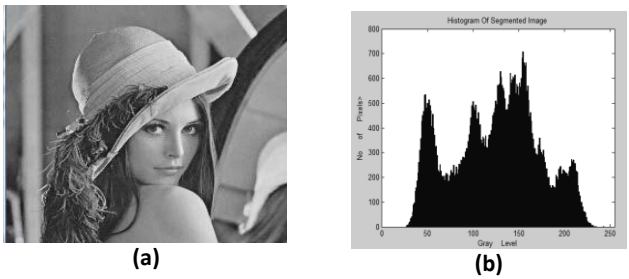
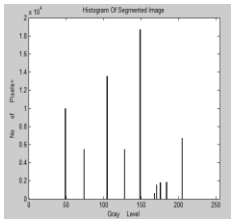
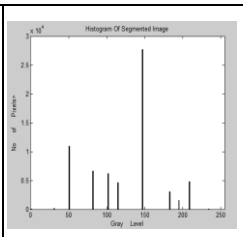
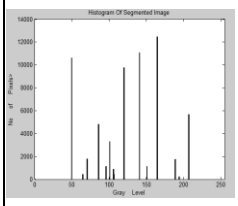


Fig. 4 (a) original image , (b) histogram of the original image

Fig. 4 represents the original image and it was found that it generates the optimum result. A stopping criteria of CC (coefficient of correlation)> 0.99 was taken i.e. testing was stopped on getting CC>0.99.

This algorithm shows exceptional results when compared with the earlier technique. It shows an increased accuracy level over the previous segmentation techniques as it doesn't suffers from drawbacks like over segmentation and under segmentation. The efficiency of the segmentation increases with the increase in the number of ants.

TABLE 3 AN ANALYSIS OF RESULT

Segmented image using AWL	**Histogram**	**Segmentation details**
		Number of ants=8 Mean of standard deviation=5.1913 Stopping criteria=CC>0.98 Elapsed time=6.74 sec
		Number of ants=10 Mean of standard deviation=5.3896 Stopping criteria=CC>0.97 Elapsed time=0.056 sec
		Number of ants=15 Mean of standard deviation=3.46 Stopping criteria=CC>0.99 Elapsed time=6.54 sec

As depicted by table 3, that as the number of ants increases the mean deviation between the original image and the segmented image decreases. And stopping criteria of CC>0.99 was obtained when number of ant chosen is 15.

III. DISCUSSION

In this paper of various image segmentation techniques we have discussed some algorithms for image segmentation. Each algorithm is having its own advantages and disadvantages. The algorithm which is based on sobel operator and maximum entropy is highly applicable where the segmentation demands high PSNR. In case if object recognition is required then we go for normalized cut and clustering algorithm as it reduces the complexity. Similarly the J-CUT algorithm also reduces the complexity and gives accurate region merging but is less robust and gives incomplete region merging. Watershed algorithm find application in medical image processing as it is simple and fast algorithm and can be applied even if contrast is poor. The ant weight lifting algorithm shows exceptional result as it doesn't suffer from over segmentation and under segmentation problem and further its efficiency increases with the increase in the number of ants.

IV. CONCLUSION

The study reviews the various segmentation methodologies and the various segmentation issues related to them. Image segmentation being the important step in any image processing, has become the focus of today's contemporary research. Since segmentation is affected by various factors such as the type of image, intensity, color, segmentation algorithm, therefore there is no single algorithm which can be

applied to all the images. Due to all these factors image segmentation still remains a big hurdle in proper image processing.

REFERENCES

[1] Hui Zhang, Quanyin Zhu, Xiang-feng Guan, "Probe into image segmentation based on sobel operator and maximum entropy algorithm," 2012 International conference on computer science and service system.

[2] Digital image processing by Rafael C. Gonzalez and Richard E. Woods 3rd edition.

[3] A. A. Farag, "Edge Based Image Segmentation", 19 Oct 2009,

[4] J. Liu, "Image Segmentation Algorithm Based on Graph Theory," Harbin: Harbin Institute of Technology, 2006.

[5] Mei Yeen Choong, Wei Yeang Kow, Yit Kwong Chin, Lorita Angelina, Kenneth Tze Kin Teo, " Image segmentation via Normalised Cuts and Clustering Algorithm," 2012 IEEE International conference on control system, computing and Engineering

[6] Yongzheng Geng , Jian Chen , Li Wang, " A novel color image segmentation algorithm based on JSEG and Normalised Cuts" , 2013 6th international congress on image and signal processing.

[7] Watershed:docs.opencv.org/trunk/doc/py_tutorials/py_imgproc/py_
watershed/py_watershed.html

[8] Sugandhi Vij, Dr. Sandeep Sharma, Chetan Marwaha , "performance evaluation of color image segmentation using k-means clustering and watershed technique," IEEE – 31661.

[9] R. M. Haralick, L. G. Shapiro, "Image segmentation techniques", *Elsevier*, 2006, 29(1)

[10] Sourav Samanta, Suvojit Acharjee, Aniruddha Mukherjee , Debarati Das, Nilanjan Dey, "Ant weight lifting algorithm for image segmentation," 2013 IEEE International Conference on Computational Intelligence and Computing Research.

A Review of Image Edge Detection

Gurpreet kaur[1], Vijay kumar Banga[2]
Dept. of Electronics and Communication Engineering
Amritsar College of Engineering and Technology
Amritsar, Punjab, India.
[1]gurpreetkaurchohan@gmail.com , [2]vijaykumar.banga@gmail.com

***Abstract:* - . This paper is concerned with the study of various edge detection techniques like Prewitt, Robert, Sobel, LoG, Canny operators and improved canny operators. It has been shown that the Improved Canny's edge detection algorithm performs much better than every one of these operators under virtually all scenarios and then merits and demerits of some available algorithms within this category are discussed.**

Keywords—*Prewitt operator, Roberts operator, Sobel, LoG, Canny operators and improved canny operators.*

I. INTRODUCTION

Edge detection is a fundamental tool utilized in image processing. The function of edge detection is feature detection and extraction. Which make an effort to identify points in a image where brightness of digital image change sharply and find discontinuities. The goal of image edge detection is significantly reduce the total amount of data in a image data and preserves the structural properties for image processing. Edge detection is complicated to utilize in noisy images, since the noise and edges contain high frequency content. Attempts to cut back the noise from image end up in vague and distorted edges. Operators applied to noisy images are usually much bigger in scope, to allow them to enough data to discount localized noisy image pixels. Therefore, the objective would be to compare various edge detection techniques and analyze the performance when it comes to examples.

II. EDGE DETECTION METHODS:

In image processing there are many different types of methods to perform edge detection. In that it contains mainly two categories.

*2.1 First Order Derivative based Edge Detection (Based on Gradient method):*It's on the basis of the usage of an initial order derivative or gradient based. The magnitude of gradient computed gives edge strength and the gradient direction that's always perpendicular to the direction of gradient computed gives edge strength and the gradient direction that's always perpendicular to the direction of image edge. If I (i , j) function as input image, then image gradient is calculated by following formula;

$$\Delta I(i,j) = i\frac{\partial I(i,j)}{\partial i} + j\frac{\partial I(i,j)}{\partial j}$$

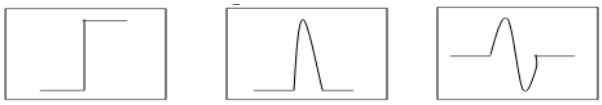
Where: $\frac{\partial I(i,j)}{\partial i}$ is the gradient in i direction.

$\frac{\partial I(i,j)}{\partial j}$ is the gradient in j direction.

The gradient magnitude may be calculated by the formula:

$$|G| = \sqrt{Gi^2 + Gj^2}$$

2.2 Second Order Derivative Based Edge Detection (Laplacian based Edge Detection): This approach look for zero crossings in the 2nd derivative of the image to learn edges. A graphic edge gets the one-dimensional model of a slam and discover the derivative of the image can highlight its location. This approach is characteristic of the "gradient filter" category of edge detection filters. A pixel location is declared a benefit location, if the worthiness of its gradient exceeds some threshold. As stated earlier, edges have higher pixel intensity values than those are surrounding it. So once a threshold is defined, the gradient value with the threshold value may be compared and an edges may be detected whenever the threshold is exceeded. Furthermore, when the initial derivative are at a maximum peak, the 2nd derivative is zero. Consequently, another option to finding the place of a picture edge is to find zeros in the 2nd derivative of image.



(a) ideal step edge **(b) first order derivation and** **(c) second order derivation**

This process uses zero-crossing operator which acts by locating zeros of the 2nd derivatives of image I(i, j). The differential operator is used in the so-called zero-crossing edge detectors,

$$\nabla^2 I = \frac{\partial^2 I}{\partial i^2} + \frac{\partial^2 J}{\partial j^2}$$

Thresholding allocates a variety of pixel values to object of interest. It is most effective with greyscale images that make use of the whole array of greyscale. For the image I(i,j), the threshold image g(i, j) is defined as,

III. CLASSIFICATION OF EDGE DETECTION TECHNIQUES

The classical gradient operators are Sobel operator, Prewitt Operator, Roberts operator, Laplacian operator.These classical operators which are uses first derivative has very simple calculations to detect edges but its limitations are inaccurate detection and sensitivity to noise. Classical operators and canny operator are beneath the sounding first order derivative based edge detection (Gradient method). Marr-Hildreth edge detector is really a gradient based operator which uses the Laplacian to take the 2nd derivative of an image.

3.1 Roberts Operator: The Roberts operator provide a simple approximation to the gradient magnitude. It computes the amount of the squares of the difference between diagonally neighboring image pixels through distinct discrimination and then calculate approximate gradient of an image. The input image is convolved with default kernels of operator and gradient magnitude and directions are computed. . One kernel is simply the other rotated by 90°. This is very similar to the Sobel operator. This operator consists of a pair of 2×2 convolution kernels as shown below:

$$Di = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } Dj = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

The advantage of this operator is very simple but having small kernel it is highly sensitive to noise. It is not much compatible with today˝s technology.

3.2 Sobal Operator: Sobel operator is also discrete differentiation operator.That is used to calculate an approximation of the gradient of an image intensity function for edge detection.An image at each pixel , it gives either the corresponding gradient vector or normal to the vector. This convolves the input image with kernel and computes the gradient magnitude and direction. The operator consists of a pair of 3 × 3 convolution masks as shown below:

$$Di = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \text{ and } Dj = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}$$

As compared to Roberts operator have slow computation ability but as it has large kernel so it is less sensitive to noise as compared to Roberts operator. As having larger mask, errors due to noise are reduced by local averaging within the neighborhood of the mask.

3.3 Prewitt Operator: Prewitt operator is also discrete differentiation operator, computing an approximation of the gradient of the image intensity function. The purpose of Prewitt edge detector is practically same at the time of sobel operator but have different kernels:

$$Di = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \text{ and } Dj = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

Prewitt edge detection operator gives much better results than Sobel operator and Roberts operator.

3.4 Canny Operator: Canny edge detector is really a advanced algorithm produced from the prior work of Marr and Hildreth. It's a maximum edge detection technique as provide accomplishment in detection, in clear response and in localization. It's widely found in current image processing techniques found in everywhere with further improvements.

STEP I: *Noise reduction by smoothing*

Noise reduce by smoothing noise contained image is smoothed by convolving the input image I (i, j) with Gaussian filter G. Mathematically, the smooth resultant image is written by,

$$F(i,j) = G * I(I,J)$$

Prewitt operator is very simple operator as compared to sobel operator, but it is more sensitive to noise.

STEP II: *Finding gradients*

In this we detect the edges where in fact the change in greyscale intensity is maximum. Required areas are determined with the aid of gradient of an image. Generally, Sobel operator is employed to ascertain the gradient at each pixel of smoothed image. Sobel operators in i and j directions get below,

$$Di = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} \text{ and } Dj = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

These sobel masks are convolved with smoothed image and gives gradients in i and j directions.

$$Gi = Di^{*}F(i,j) \text{ and } Gj = Dj^{*}F(i,j)$$

Therefore edge strength or magnitude of gradient of a pixel is given by,

$$G = \sqrt{Gi^2 + Gj^2}$$

The direction of gradient is given by,

$$\theta = \arctan\left(\frac{\mathrm{Gi}}{\mathrm{Gj}}\right)$$

$Gi\ and\ Gj$ are the gradients in the i and j directions respectively.

STEP III*: Non maximum suppressions:*
Non maximum suppression is carried out to preserves all local maxima in gradient image, and deleting the rest, this results in thin edges. For a pixel M (i, j):

• Firstly across the gradient direction nearly 45°, then compare the gradient magnitude of the pixels in positive and negative gradient directions i.e if gradient direction is east then compare gradient of the pixel with west direction say E (i, j) and W (i, j) respectively.

• If the edge strength of image pixel M (i, j) is bigger than that of E (i, j) and W (i, j), then preserves the worthiness of gradient and mark M (i, j) as edge pixel, or even then suppressed.

STEP IV: *Hysteresis thresholding:*

The output of non-maxima suppression still contains the neighborhood maxima produced by noise in image. Instead picking a single threshold, for avoiding the situation of streaking two thresholds t_{high} and t_{low} are used.

For a pixel M(i, j) having gradient magnitude G following conditions exists to detect pixel as edge:

□ □ If$G < t_{low}$ than discard the edge.
□ □ IfG □ □ thant_{high} keep the edge.
□ □ Ift_{low} □G □ □and t_{high} and any of its neighbors in a 3□ □3 region around it have gradient magnitudes greater than t_{high} keep the edge.
□ □ If none of pixel (x, y)'s neighbors have high gradient magnitudes but at least one falls between $t_{high}$and t_{low} search the 5 × 5 region to see if any of these pixels have a magnitude greater than t_{high} . If so, keep the edge.
□ □ Else, discard the edge.

3.5 Laplacian of Gaussian or Marr Hildrith Operator:

The Marr-Hildreth edge detector was a extremely popular edge operator prior to the Canny proposed his algorithm. It is really a gradient based operator which uses the Laplacian to get the next derivative of an image. It works on zero crossing method. LOG uses both Gaussian and laplacian operator to ensure that Gaussian operator reduces the noise and laplacian operator detects the sharp edges in a image.

The Gaussian function is defined by the formula:

$$G(i,j) = \frac{1}{\sqrt{2\pi\sigma^2}} exp - \left(i^2 + \frac{j^2}{2\sigma^2}\right)$$

Where,

$$LoC = \frac{\partial^2}{\partial i^2} G(i,j) + \frac{\partial^2}{\partial j^2} G(i,j)$$
$$= i^2 + j^2 - \frac{2\sigma^2}{\sigma^4} \exp\left(-i^2 + \frac{j^2}{2\sigma^2}\right)$$

The Marr–Hildreth operator, however, suffers from two main limitations. It gives responses that do not correspond to edges, so-called "false edges", and localization error may be severe at curved edges.

3.6 Improved Canny Operator:

A. The introduction of Bilateral Filtering

The conventional canny algorithm smoothes the image with Gaussian filter, while suppressing the noise, the edge pixels are also smoothed. In 1988, C.Tomasi and R.Manduchi proposed bilateral filtering. The traditional lowpass filter considered the center pixel similar to its neighborhood and unconcerned with the noise. However, the pixels on the edges of the images greatly differ from its bilateral pixels, thus when smoothing, the edge pixels are unavoidable to be smoothed, making the loss of the edge pixels. Fortunately, when processing the neighbor pixels, the bilateral filtering not only has considered the closeness of the space, but also the range of the intensity. By the means of non-linear combination of these two, a new filter is born, which can smooth the image adaptively. For image f(x), after applying low-pass filter, the filtered image can be denoted as h(x), namely:

$$h(x) = k_d^{-1}(x) \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(\xi)\, c(\xi, x) d\, \xi$$

where $c(\xi, x)$ denotes the geometric closeness between the neighborhood center x and a nearby point ζ.Assuming $x = (x1, x2), \xi = (\xi 1, \xi 2)$ as the spatial coordinate, if the low-pass filter preserve the direct currency of the signal, then

$$k_d(x) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} c(\xi, x) d\xi$$

If the filter is shift-invariant, $c(\xi, x)$ is the vector difference $\xi - x$. Range filtering is similar, accordingly, it can be defined as:

$$h(x) = k_r^{-1}(x) \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(\xi) s\big(f(\xi), f(x)\big) d\xi$$

where $s(f(\xi), f(x)$ indicates the photometric similarity between the center pixel x and its neighborhood point□ ξ□ □ □At this moment:

$$k_r(x) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s\big(f(\xi), f(x)\big)d\xi$$

Contrary to what occurs with the geometric closeness, the photometric similarity is determined by the difference $f(\xi) - f(x)$. According to the formula (1) and formula (3), the combined filtering by spatial filtering and range filtering can be described as follows:

$$k(x) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} c(\xi, x)s(f, \xi), f(x))d\xi$$

This combined filtering through the spatial domain and range domain is called bilateral filtering. Its advantages are that it replaces the pixel value at x with an average of similar and nearby pixel values. In smooth regions, pixel values in a small neighborhood are similar to each other, and approximating to a constant. At this moment, the bilateral filtering is degraded into a standard domain filter. In a sharp region, the filter replaces the bright pixel at the center by an average of the bright pixels in its vicinity, and essentially ignores the dark pixels. Conversely, when the filter is centered on a dark pixel, the bright pixels are ignored instead. Thus, the bilateral filtering can not only filter the noise,but also preserve the edge details, which is practical method that can be put into practice to a greet extent.

B. OTSU adaptively determine the thresholds

OTSU is an approach that makes the separability of the resultant classes maximum to automatically determine the thresholds. Its basic ideas are according to the gray characteristics of images, the image is separated into background and foreground, making their variances of interclass maximum, finally obtaining the optimal thresholds. For an $M \times N$ image $I(X,Y)$, the segmented threshold of foreground and background denotes as T, the rate of foreground is $\omega 2$ its average value is $u1$; the rate of the background is $\omega 2$, and the average value is $u2$, the mean of the image is u , the variance of the inter-class is g. Then we can get the following formulas:

$$\omega_1 = \frac{N_1}{M \times N}$$

$$\omega_2 = \frac{N_2}{M \times N}$$

$$N_1 + N_2 = M \times N$$

$$\omega_1 + \omega_2 = 1$$

$$u = u_1 \times \omega_1 + u_2 \times \omega_2$$

$$g = \omega_1 \times (u - u_1)^2 + \omega_2 \times (u - u_2)^2$$

From the above formula the following formula can be obtained:

$$g = \omega_1 \times \omega_2 \times (u_1 - u_2)^2$$

Finally, applying traversed approach to obtain the threshold which makes g maximum, and then T is the optimal threshold. As a sequence, we consider T as the high threshold, and the low threshold can be got as:

$$T_h = K \times T_1$$

Where k is a constant (recommend as 2-3), its default value is 2.

C. Steps of improved algorithm

1) Smooth the image with bilateral filtering

Applying bilateral filtering to smooth the image and remove the noise, when the bilateral filtering smoothed the image, it considers not only the domain relation, but also the range relation, by the non-linear combination of these two, it can adaptively smooth the image and obtain the smoothed image. After this step, not only much noise has been removed, but the edge information has been preserved.

2) Compute the gradient magnitude and direction

After processing from (1), in this step, the gradient, direction and magnitudes are computed. The details can refer to the description of the conventional canny operator.

3) Perform non-maximum suppression

This step is same as the conventional canny operator, and more details can refer to the related contents of the introduction of the conventional canny operator in section 2.

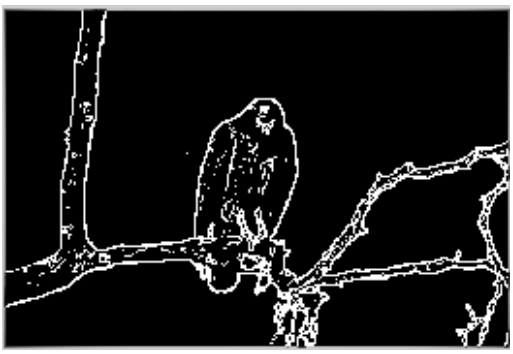
4) Adaptively determine the double thresholds and perform edge detection and connection. Calculating the histogram of gradient magnitudes, and then the OTSU algorithm is applied to determine the double thresholds Th and Tl. After this, it scans the whole image to detect any pixels that are marked as candidate edge points. If the gradient magnitude G (i,j) of Poin t(i, j) is greater than the high threshold Th, then it is absolutely determined as edge point; It is completely not edge point when the gradient magnitude G(i,j) of point(i,j) is less than Tl. For these points whose gradient magnitudes range from Tl to Th, they are considered as the suspected edge points and examine their connectivity. If their adjacent pixels have edge pixels, then they are also considered as edge pixels, otherwise, they are non-edge pixels.

IV. VISUAL COMPARISON OF VARIOUS EDGE DETECTION ALGORITHMS

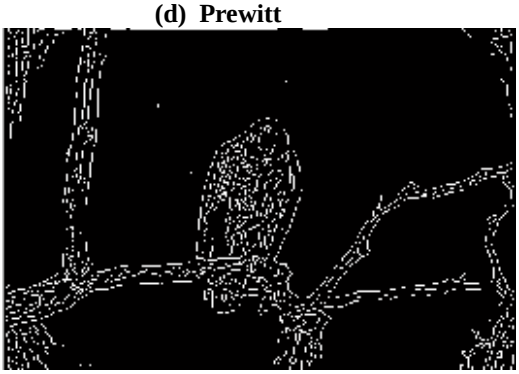
(a) Original

(b) Robert

(c) Sobel



(d) Prewitt



(e) Canny

(f) LoC

Figure-1: Edge images on the original image using different operators

Operator	Merits	Demerits
Classical (Sobel, prewitt, Kirsch,…)	Simplicity, Detection of edges and their orientations	Sensitivity to noise, Inaccurate
Zero Crossing(Laplacian, Second directional derivative)	Detection of edges and their orientations. Having fixed characteristics in	Responding to some of the existing edges, Sensitivity to noise

	all directions	
Laplacian of Gaussian(LoG) (Marr-Hildreth)	Finding the correct places of edges, Testing wider area around the pixel	Malfunctioning at the corners, curves and where the gray level intensity function varies. Not finding the orientation of edge because of using the Laplacian filter
Gaussian(Canny, Shen-Castan)	Using probability for finding error rate, Localization and response. Improving signal to noise ratio, Better detection specially in noise conditions	Complex Computations, False zero crossing, Time consuming
Improved canny operator	improved Canny operator has more continuity, and greater signal to noise ratio.	At the same time, the numbers of few false edges are being reduced

(a) Original **(b) Canny** **(c) Improved Canny**

Figure:-2

(a) Original **(b) Canny** **(c) Improved Canny**

Figure:-3

Figure:-2 and 3 Compared the images of traditional canny with improved canny:

Compared to the traditional Canny operator, the improved Canny method can automatically determine high and low threshold parameters according to the actual feature of the image, to get more integrated information. The continuity of the edge is strong, and positioning is accurate.

IV. CONCLUSION:

In this paper many edge detection methods like Sobel operator technique, Roberts technique ,Prewitt technique, LoC technique,Canny technique, and Improved canny technique are discussed. It has described these techniques in details and analyzed its drawbacks, and proposed the improved adaptive threshold canny algorithm based on the bilateral filtering and the maximum of the separability of the
resultant classes based on the gradient magnitudes. Firstly, this algorithm applies bilateral filtering to smooth the image,
which not only has suppressed the noise of the image, but also has well preserved the edges. Secondly, OTSU is performed to adaptively determine the low and high thresholds. An improved canny show that this improved algorithm can well solve the drawback analyzed above, as

well as, it have the capability of self-adapting the changes of scenes and illumination, and extended its use.

REFERENCES

[1] R. C. Gonzalez and R. E. Woods. "Digital Image Processing". 2nd ed. Prentice Hall,pp. 1-190, 2002.

[2] Raman Maini and Dr. Himanshu Aggarwal, Study and Comparison of different Image Edge Detection Techniques, *International Journal of Image Processing (IJIP), Volume (3) : Issue (1) ,pp 1-11January/February 2009.*

[3] Muthukrishnan.R and M.Radha (2011), Edge detection techniques for image segmentation, *International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, pp 259-267*,Dec 2011.

[4] Huili Zhao, Guofeng Qin and Xingjian Wang (2010), Improvement of Canny Algorithm Based on Pavement Edge Detection, *3rd International Congress on Image and Signal Processing,Vol (9),pp16-18, (CISP2010).*

[5] P. Thakare (2011), A Study of Image Segmentation and Edge Detection Techniques, *International Journal on Computer Science and Engineering, Volume 2, Issue 5, pp 319-323,May 2013.*

[6] V.Shrimalli, R.S.Anand ,R.K.Srivastav,"Medical feature based evaluation of structuring elements for morphological enhancement of ultrasonic images", Journal of Medical Engineering & Technology , Vol. 33,No. 2,February 2009,pp 158-169.

[7] Yuancheng ―Mike‖ Luo and Ramani Duraiswami, ―Canny Edge Detection on NVIDIA CUDA‖, University of Maryland, College Park Volume 2, Issue 3, March 2014.

[8] J. F. Canny, "A computational approach to edge detection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679-698, 1986.

[9] ZHANG Yongliang,LIU Anxi, Improved algorithm for computer digital lmage edge detection based on Prewitt operator,*Journal of PLA University of Science and Technology*,6(1):45-47, 2005.

[10] Otsu N. A threshold selection method from gray-levelhistograms.*IEEE Trans Systems,Man and Cybernetics*,9(1):62-66,1979.

[11] L. G. Roberts. "Machine perception of 3-D solids" ser. Optical and Electro-Optical Information Processing. MIT Press, Vol 4,pp 220-226,feb 2012.

Comparative Analysis of Mammogram With Various Filtering Techniques

Er. Rahul Vohra
Research Scholar
ACET, ECE Deptt.
Amritsar ,Punjab
rvohra57@yahoo.co.in

Er.Sandeep Kaushal
Associate Professor
ACET Deptt Of (ECE)
Amritsar , Punjab
Sandeep.laddi@gmail.com

Er.Jaspinder Singh Sidhu
Assistant Professor
Deptt. Of (ECE),RTI
Amritsar ,Punjab
Jaspinder.12253@gmail.com

***Abstract*— Breast cancer is second most commonly diagnosed cancer worldwide. In order to find the cure it is necessary to quickly diagnose the disease accurately and treat it based on the kind of symptoms appeared. Breast cancer has several classifications, which may help to determine the best treatment. The most important of these classifications are binary classification, either benign or malignant. If the cancer is in benign stage, less invasive and risk of treatments is used than for malignant stage. The main cause of breast cancer is when a single cell or group of cells escapes from the usual controls, that regulate cellular growth and begins to multiply and spread. This activity may result in a mass, tumor or neoplasm. The present paper implies the edge detection techniques for the cancer cell detection purpose. The present paper deals with observation of breast cancer classification through Image Processing using the various filters which are mainly gradient based Roberts and Sobel. Laplacian based edge detector which is Canny edge detector. The various aspects and the implementation of above mentioned filters has been put across in the present paper. The images and data sample have been taken from the Digital Database for Screening Mammography (DDSM) and American cancer society and an effort has been made for the detection of malignant cells responsible for cancer.**

***Keywords*: - Canny, Robert, Sobel.**

I. INTRODUCTION

Recently studies show that one in 10 women will contract breast cancer in their lifetime, and that breast cancer is the leading cause of death of women between the ages of 35 and 54. Every year 27% of the new cancer cases in women are breast cancers. Although X-ray mammogram detection is best way of screening the breast cancer and ultrasound method is more popular because of its non-invasiveness and low cost. Due to high noise, low contrast radiologists cannot detect and classify the tumor or dense in breast cancer. Image enhancement is a best way for the diagnostic reliability by reducing noise effects in mammogram and filtering is a challenging process in ultrasound image processing since the noise is of unknown source with non specific form and trend[2]. Several algorithms have been proposed to enhance the signal-to- noise ratio and to eliminate noise speckles.

Breast cancer takes years to develop. It is commonly classified into four stages according to size of tumors and degree of cancer spread from the breast to other parts of the body. There is one pre-cancerous stage called ductal carcinoma in situ (DCIS) when a pre-cancerous lesion has not developed into a cancer tumor. In the first stage, a 0-2 centimeter tumor forms without spreading outside the breast[17]. If the cancer is detected in this stage the five-year survival rate is 96%. In the second stage, the cancerous cells form new malignant foci in positive lymph nodes or the tumor enlarges to 2-5 centimeter. In this stage, the survival rate drops to 73% . In the third stage, a tumor is larger than 5 centimeters with positive lymph nodes, or a tumor has skin and chest wall involvement. The surgical intervention performed would be quite heavy; it may need partial or total breast removal and lymph nodes dissections. In the fourth stage, obvious metastases to other organs of the body, most often the bones, lungs, liver, or brain occur and the five-year survival rate drops to 20% [2].

Although breast cancer can be fatal, people have the highest chance of survival if cancer could be detected at the early stages. Early diagnosis and treatment play critical roles in increasing the chance of survival. My study involves a literature research on diagnostic techniques used for breast cancer and development of a computer-aided diagnosis tool using Matlab for breast segmentation in mammograms. Image enhancement techniques commonly used are spatial and frequency domain filters; moreover, fractal analysis could serve as a preprocessing stage before segmentation in mammograms[19]. In order to extract boundaries of suspected tumor masses, region growing and morphological edge detection algorithms are implemented.

In this research, I use mammograms from the Digital Database for Screening Mammography (DDSM) .This paper is organized into five sections.

In section II enhancement of the image and characteristics of the image is described.

FIG.1: IMAGE ENHANCEMENT TECHNIQUES

In section III I introduce the methodology that is various kinds of filters are used. In section IV I describe In digital image processing some general image intensification method like Robert, Sobel, Canny filter, the low pass filtering, the edge enhancement and so on mainly aim in the image the stochastic noise, but in the fuzzy image's grain line flaw belongs to the constitutive noise, therefore is not ideal to the image's enhancement effect The essential procedure is to the primitive gradation image after the low- pass filtering, the histogram transformation and so on general image intensification method carries on processing, carries on the binaryzation and refinement processing.

the comparison of various filtering methods contrast. Parameters are determined using experimental methodology.

II. IMAGE ENHANCEMENT

Image enhancement is basically improving the interpretability or perception of information in images for human viewers and providing `better' input for other automated image processing techniques. The principal objective of image enhancement is to modify attributes of an image to make it more suitable for a given task and a specific observer[7]. During this process, one or more attributes of the image are modified. The choice of attributes and the way they are modified are specific to a given task. Moreover, observer-specific factors, such as the human visual system and the observer's experience, will introduce a great deal of subjectivity into the choice of image enhancement methods. There exist many techniques that can enhance a digital image without spoiling it. The enhancement methods can broadly be divided in to the following two categories, Spatial Domain Methods and Frequency Domain Methods, figure 1 shows the techniques of enhancement of image. In spatial domain techniques [9], we directly deal with the image pixels. The pixel values are manipulated to achieve desired enhancement. In frequency domain methods, the image is first transferred in to frequency domain. It means that, the Fourier Transform of the image is computed first. All the enhancement operations are performed on the Fourier transform of the image and then the Inverse Fourier transform is performed to get the resultant image. These enhancement operations are performed in order to modify the image brightness, contrast or the distribution of the grey levels. As a consequence the pixel value (intensities) of the output image will be modified according to the transformation function applied on the input values.

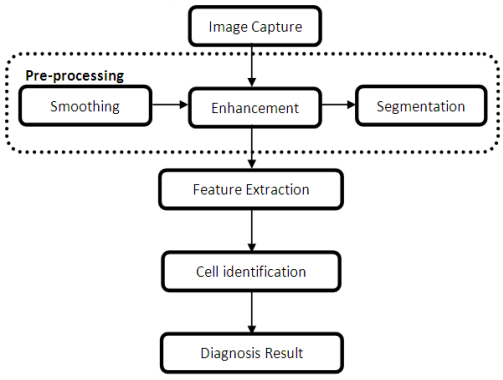


FIG. 2: DIAGNOSIS PROCESS

III. METHODOLOGY

There are many ways to perform the edge detection. However, it may be grouped into two categories, that are gradient and Laplacian. The gradient method detects the edges by looking for the maximum and minimum in the first derivative of the image. The Laplacian method searches for the zero crossings in the second derivative of the image to find edges. The edges of an image detected using the gradient method (Roberts, Sobel) and the Laplacian method (Canny filter). It can compare the feature extraction using the Sobel edge detection with the feature extraction using the Laplacian [3]. It seems that although it is better for some features but it still suffers from mismapping some of the lines. A morphological approach is constructed using individual selected points which will work better.

3.1 Robert Filter

The Roberts cross operator is used in image processing and computer vision for edge detection.. As a differential operator, the idea behind the Roberts cross operator is to approximate the gradient of an image through discrete differentiation which is achieved by computing the sum of the squares of the differences between diagonally adjacent pixels. The Roberts Cross operator performs a simple, quick to compute, 2-D spatial gradient measurement on an image. Pixel values at each point in the output represent the estimated absolute magnitude of the spatial gradient of the input image at that point. The operator consists of a pair of 2×2 convolution kernels. One kernel is simply the other rotated by 90°[4]. This is very similar to the Sobel operator. The Roberts Cross operator performs a simple, quick to compute, 2-D spatial gradient measurement on an image as shown in figure[3.1]. Pixel values at each point in the output represent the estimated absolute magnitude of the spatial gradient of the input image at that point. One kernel is simply the other rotated by 90°. This is very similar to the Sobel operator.

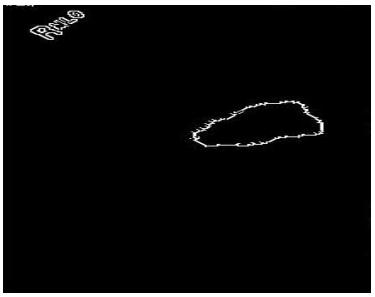


Fig.3.1 Robert Filter

3.2 Sobel Filter

The operator consists of a pair of 3×3 convolution kernels. These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular orientations. Operators can be optimized to look for horizontal, vertical, or diagonal edges. Edge detection is difficult in noisy images, since both the noise and the edges contain high-frequency content. Attempts to reduce the noise result in blurred and distorted edges. Operators used on noisy images are typically larger in scope, so they can average enough data to discount localized noisy pixels. This results in less accurate localization of the detected edges. Not all edges involve a step change in intensity. Effects such as refraction or poor focus can result in objects with boundaries defined by a gradual change in intensity [1]. The operator needs to be chosen to be responsive to such a gradual change in those cases. So, there are problems of false edge detection, missing true edges, edge localization, high computational time and problems due to noise etc.

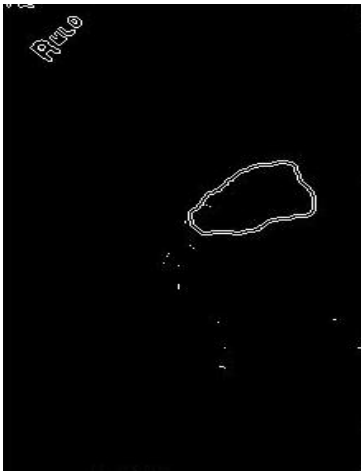


Fig.3.2 Sobel Filter

3.3 Canny Edge Detection Algorithm

The Canny edge detection algorithm is known to many as the optimal edge detector. Canny's intentions were to enhance the many edge detectors. "A Computational Approach to Edge Detection"[11]. In this paper, he followed a list of criteria to improve current methods of edge detection. The first and most obvious is low error rate. It is important that edges occurring in images should not be missed and that there be no responses to non-edges. The second criterion is that the edge points be well localized. In other words, the distance between the edge pixels as found by the detector and the actual edge is to be at a minimum. A third criterion is to

have only one response to a single edge. This was implemented because the first two were not substantial enough to completely eliminate the possibility of multiple responses to an edge. Based on these criteria, the canny edge detector first smoothes the image to eliminate the noise. It then finds the image gradient to highlight regions with high spatial derivatives. The algorithm then tracks along these regions and suppresses any pixel that is not at the maximum (non maximum suppression). The gradient array is now further reduced by hysteresis. Hysteresis is used to track along the remaining pixels that have not been suppressed. Hysteresis uses two thresholds and if the magnitude is below the first threshold, it is set to zero (made a non edge). If the magnitude is above the high threshold, it is made an edge. And if the magnitude is between the 2 thresholds, then it is set to zero unless there is a path from this pixel to a pixel with a gradient.

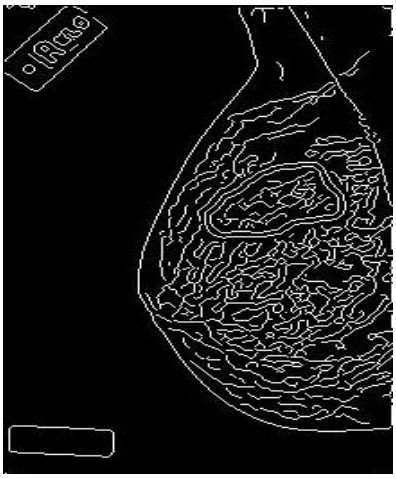


Fig.3.3 Canny Filter

IV. COMPARISON OF VARIOUS FILTERS

Edge detection of three types of filters was performed on Figure [4]. Canny yielded the best results. This was expected as Canny edge detection accounts for regions in an image. Canny yields thin lines for its edges by using non-maximal suppression. Canny also utilizes hysteresis with thresholding. As edge detection is a fundamental step in computer version. it is necessary to point out the true edges to get the best results from the matching process. That is why it is important to choose edge detectors that fit best to the application.

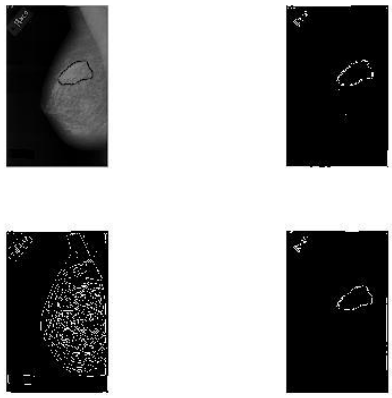


Fig.4 Comparison of all the filters techniques

V. CONCLUSIONS

The edge detection is the primary step in identifying an image of an object, so it is essential to know the advantages and disadvantages of each edge detection filters. In the present paper we have adopted edge detection techniques of Gradient-based and Laplacian based. Edge Detection Techniques are compared with case study of identifying the breast cancer cell. It has been observed that the Gradient-based algorithms have major drawbacks in sensitive to noise. The performance of the Canny algorithm relies mainly on the changing parameters. The size of the Gaussian filter is controlled by the greater value and the larger size. The larger size produces more noise, which is necessary for noisy images, as well as detecting larger edges. Canny's edge detection algorithm is more costly in comparing to Sobel and Robert's operator. Even though, the Canny's edge detection algorithm has a better performance instead of all the others filters. Canny filter is responsible for improving signal to noise ratio as well better detection capability. The evaluation of the images showed that under the noisy conditions, Canny, Sobel, Roberts's are exhibited better performance, respectively. The various methodologies of using edge detection techniques namely the Gradient and Laplacian transformation. It seems that although Laplacian does the better for some features, it still suffers from mismapping some of the lines.

REFERENCES

[1] Canny, J., "A Computational Approach to Edge Detection", *IEEE* Trans. Pattern Analysis and Machine Intelligence, vol. *8: 679-714*, November.

[2] M.J. Bottema, G.N.Lee and S.Lu, "Automatic image feature extraction for diagnosis and prognosis of breast cancer," Artificial intelligence techniques in breast cancer diagnosis and prognosis, Series in machine

perception and artificial intelligence, Vol.39, World Scientific Publishing Co.Pte.Ltd, 2000, pp. 17-54.

[3]G.T.Shrivakshan. Gonzalez and Dr .C.Chandrasekar."A Comparision of various Edge Detection Technique Used in Image Processing", IJCS, Vol 2nd, September 2012.
[4] R. C. Gonzalez and R. E. Woods. "Digital Image Processing". 2nd ed. Prentice Hall, 2002.
[5] N. Senthilkumaran, R. Rajesh, " Edge Detection Techniques for image Segmentation and A Survey of Soft Computing Approaches." International Journal of Recent Trend in Engineering. Vol. 1. No. 2, PP.250-254, May 2009.
[6] T.G. Smith Jr., et.al "Edge Detection in images using Marr-Hildreth Filtering techniques" Journal of Neuroscience Methods, Volume 26, Issue 1,PP.75-81, November 1988.
[7] WenshuoGao, et.al. ;"An improved Sobel Edge detection", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, China, Volume: 5, PP.67-71, 9-11July 2010.
[8] Y. Yakimovsky, "Boundary and object detection in real world images". JACM, vol. 23, no. 4, pp. 598-619, Oct. 1976
[9] J. Canny. "Finding edges and lines in image". Master's thesis, MIT, 1983.
[10] Bergholm. "Edge focusing," in Proc. 8th Int. Conf. Pattern Recognition, Paris, France, pp. 597- 600, 1986.
[11] . Peli and D. Malah. "A Study of Edge Detection Algorithms". Computer Graphics and Image Processing, vol. 20.
[12] M.C. Shin, D. Goldgof, and K.W. Bowyer ."Comparison of Edge Detector Performance through Use in an Object. Recognition Task". Computer Vision and Image Understanding, vol. 84, no. 1, pp. 160-178, Oct. 2001.
[13] A. Yuille and T. A. Poggio . "Scaling theorems for zero crossings". IEEE Trans. Pattern Anal. Machine Intell., vol. PAMI-8, no. 1, pp. 187-163, Jan. 1986.
[14] F.A.Cardillo, A.Starita, D.Caramella, and A.Cilotti, "A neural tool for breast cancer detection and classification in MRI," 2001 Proceedings of the 23rd Annual EMBS International Conference, Oct 25-28, Istanbul, Turkey
[15] Digital Database for Screening Mammography (DDSM), University of South Florida, U.S.A. [Online].Available:http://marathon.csee.usf.edu/Mammogr phy/Database.ht ml
[16]www.sciencephoto.com
[17]Www.Komen.org
[18]Www.Breastcancer.org
[19]Www.Nationalbreastcancer.org
[20] www.imaging.consult.com

SURVEY ON IMAGE FUSION TECHNIQUES

Er. Mandeep kaur
M.Tech Research Scholar
Dept. of Computer science and engineering
ACET, Amritsar
mandeepkaurrandhawa735@gmail.com

Asso.Prof. Navneet Bawa
Dept. of computer science and engineerin
ACET, Amritsar
mtechthesis2014@gmail.com

ABSTRACT:- Image fusion is a system to combine applicable data from a set of images into a solitary image where the resultant fused image is more instructive image. The fused image holds all the vital data as contrast to information images. The fused image acquires all the data from source images. With fast advancement in technology, it is currently conceivable to get data from multi-source images to make an excellent fused image. The result of image fusion is to interchange image that has remaining parts the most attractive information and qualities of input image. The main objective of image fusion is to combine information from multiple images of the same scene in order to deliver only the useful information. The typical objective of this paper has been to explore the different methods for efficiently fusing digital images. It has been found that many the prevailing researchers have neglected many issues; i.e. no technique is accurate for different kind of circumstances

KEYWORDS :- IMAGE FUSION, PCA, DCT

1.INTRODUCTION

Image fusion is a system to combining applicable data from a pair of images in a solitary image in which the resultant fused image is more instructive image. The fused image holds all of the vital data as contrast to information images. The fused image will acquire all the data from source images. With fast advancement in technology, it is conceivable to get data from multi-source images in making a superb fused image. The fused image caused by image fusion is the interchange image that remaining parts essentially the most attractive information and qualities of input Image. Image fusion is a beneficial process for combining the sensor and multi-sensor images to reinforce the data. The motivation behind image fusion is always to join data from group of images paying attention to the aim in making a picture that communicates just the accommodating information. Image fusion is a task wherein images are extracted from distinctive sensors by a particular algorithm so the resultant image is more consistent, clear, and reasonable. Image fusion method like discrete cosine transform is appropriate and efficient in continuous framework. An excellent way of fusion of multi focus images is focused around variance calculated in DCT domain. The primary objective of image fusion is to generate a fused image that gives the complete and consistent data. Image fusion perform at three separate levels i.e. pixel, feature and decision, expects to accomplish the more correct, complete and consistent image description of the same scene.

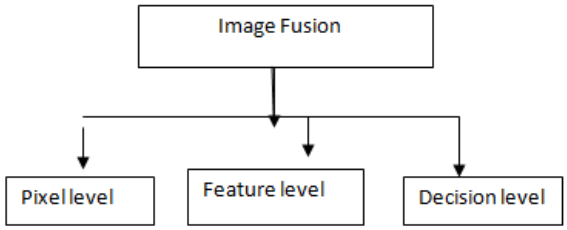


Fig 1: Three levels of image fusion

Pixel Level Fusion

In pixel level image fusion [3], firstly registration of images happens. At this point the pre-processing is preformed. Pixel level fusion meets expectations straight on pixels of source images. In pixel level image fusion, various requirements are focused for the fused results; the fusion methodology should protect beneficial data in the original source image, the fusion probably should not present any component. Pixel level fusion gets to be the primary principle mainly because it can secure

unique data of source image however much as could be expected.

Feature Level Fusion

Feature level fusion procedure would be the second phase of processing where image fusion may happen. Fusion within the feature level needs removing features from your input images. Features could be pixel intensities or edge and composition characteristics. The Several types of features are measured depending on route of images and the use of the fused image. You are going to includes the removing of feature primitives like edges, area, shape, size, length or image fragments, boasting with comparable intensity from the images being fused from unique variations of images of the comparative geographic range. Gets into something are then merged with the related features introduce from the other data images by using a pre-determined choice procedure to create the final fused image. Decision level fusion joins the outcomes from various algorithms to yield one final fused decision.

Decision Level Fusion

Decision level fusion is a really active of fusion which joins the outcomes from various algorithms to create a final fused decision.

2. IMAGE FUSION TECHNIQUES

Within the Image Fusion techniques the high-quality data from greater section of the given images is fused commonly build a resultant image whose quality surpasses considered one of the input images

2.1 Principal Component Analysis Method

Principle component analysis is often a mathematical tool which transfers a few correlated variables into a few uncorrelated variables. Principle component analysis is utilized extensively in image classification and image compression. It evaluates a small and optimal description of the data set. The 1st principal component represents much of the remainder of the difference as could reasonably be expected. To initalize with principal component is delivered to be along side direction with the greatest variance. The second principal component is compelled to lie while in the subspace perpendicular in the first. Inside this Subspace, this component focuses the direction of greatest variance. The third principal component is consumed the most extreme variance direction while in the subspace perpendicular to the original two and so on. Steps of PCA are:

- Input images size checking is completed to make certain that source images are of same size.
- At this point input images are orchestrated into column vectors. Let Z will be the ensuing column vector of dimension 2*N.
- Compute the empirical mean along every column. The dimension of Empirical means vector is 1*2.
- Subtract from each column of matrix Z. The ensuing matrix X has dimension 2*N.
- Discover covariance matrix C of matrix X.
- Process the eigen vector and eigen estimation of C and sort them in diminishing eigen value.
- Consider first column of vector which can compare to bigger Eigen value to think normalized component P1 and P2.

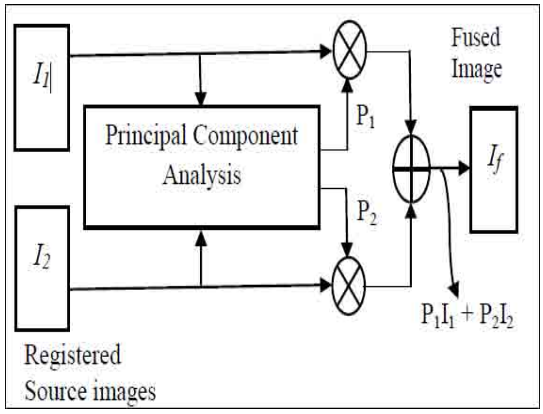


Fig 2: Image fusion using PCA [4]

2.2. IHS Transform Fusion

The IHS technique a standout in the normally utilized fusion methods for sharpening connected with an image. It's got transformed into a normal system in image dissection for color upgrade, characteristic improvement, change of spatial resolution and also the fusion of dissimilar information sets. IHS technique comprises on renovating the R, G and B bands on the multispectral image into IHS parts, supplanting the force part by the high resolution panachromatic image, and performing the inverse transformation on the way to obtain a superior spatial resolution multispectral image.

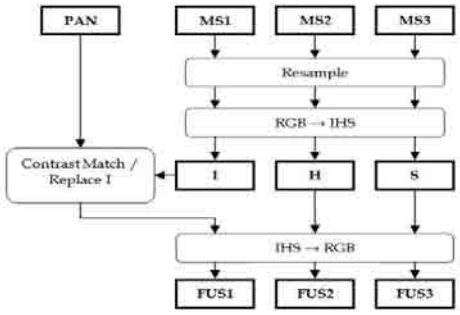


Figure 3: Intensity-Hue-Saturation (IHS)

Steps interested in IHS based image fusion:

- Transform the 3 resampled bands of the MS imagery, which speak the RGB space into IHS components.
- The Panchromatic image and power some multispectral image is matched.
- The energy some piece of MS image is supplanted from the histogram matched full resolution PAN image.
- The RGB of the newest merged MS image is gotten by processing a reverse IHS to RGB transformation.

2.3. Brovey Transform

It is likewise the color normalization transform see how to avoid of the fact that it provides a red-green-blue (RGB) color transform strategy. The Brovey transformation was formed to maintain a strategic distance from the inconveniences of the multiplicative methods. It is a easy strategy of combining together information from distinctive sensors. It is a consolidation of math operations and normalizes the spectral bands before these are duplicated with all the panchromatic image. It holds the relating spectral feature of each one pixel, and transforms all the luminance data right panchromatic image of high resolution.

The formula used by the Brovey transform is regarded as a follows:

Red = (band1/Σ band n) ∗ High Resolution Band

Green = (band2/Σ band n) ∗ High Resolution Band

Blue = (band3/Σ band n) ∗ High Resolution Band

Hi-res band = PAN.

2.4 Discrete Cosine Transform (DCT)

Spatial domain image fusion techniques are convoluted and prolonged which are difficult to be exercised on ongoing images. Besides, when the fundamental cause images are coded in Joint Photographic Experts Group (JPEG) format or once the fused image is going to be saved JPEG format, then a fusion approaches that are connected in DCT domain is going to be exceptionally efficient. To do the JPEG coding, a perception is initially subdivided into blocks of 8x8 pixels. The Discrete Cosine Transform (DCT) is going to be executed on each block. This creates 64 coefficients that are then quantized to reduce their extent. The coefficients are then reordered right one-dimensional array in the crisscross way before further entropy encoding happens. The compression is attained in 2 stages the first is aimed quantization as well as the second aimed the entropy coding procedure. JPEG decoding is overturn steps involved in encoding.

The operation utilizes a differentiation measure as choice basis to become listed on together the few blurred images in the solitary decent quality image. This complexity measure is focused around the transformation from the image from your spatial domain to the regularity domain over the processing from the DCT. The DCT procedure is a formula that focus on the regularity domain. This process isolate the image in altered size blocks to pick which source image needs to be chosen to constitute one more coming about image. DCT is central to the transformation utilized within digital image processing. DCT based image fusion are a lot better and efficient continuously framework utilizing DCT based standard of still image or video. DCT can adjust on the spatial domain image to frequency domain image.

2.5)Discrete Wavelet Transform

The wavelet transform decays the image into low-low, low-high, high-low, high-high spatial frequency bands at diverse scales. The LL band has the estimate coefficients while alternate bands contain directional data as a consequence of spatial orientation. LH band has the even detail coefficients. HL band has the vertical point of interest coefficients; HH has the diagonal detail coefficients furthermore secure the higher absolute estimations of wavelet coefficients compare to remarkable features for example edges or lines.

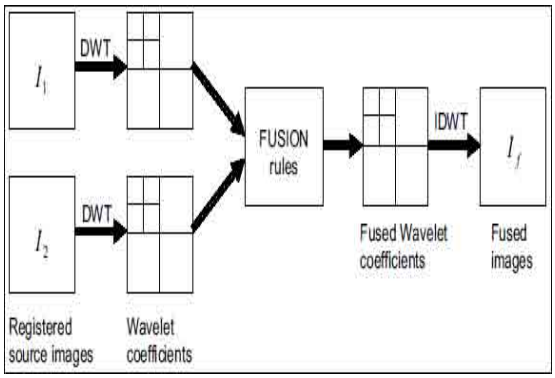


Fig 4: Discrete wavelet Transform based image fusion

The flow diagram of wavelet- based image fusion algorithm is demonstrated in Fig. 4. In wavelet image fusion system, the source images I_1 (x, y) and I_2 (x, y), are disintegrated into rough guess and itemized coefficients at obliged level using DWT. The estimate and complete coefficients of both images are joined together using fusion ruleϕ. The fused image (I_f (x, y)) could be acquired by taking the inverse discrete wavelet transform.

3. LITERATURE SURVEY

Haghighat, M et al. [4] has fixed that the picture blending is a framework to solidify information from different pictures of exactly the same scene to spread this is the supportive information. The discrete cosine change (DCT) based schedules for picture fusion are considerably better and proficient ceaselessly system. In this paper a successful system for mixture of multi-base pictures concentrated on change discovered in DCT region is presented. The test outcomes shows the capacity change of our procedure both in quality and complication diminishing in examination with a couple generally proposed methods. Ling Tao et al. [5] has inspected that therapeutic picture combination has greatly basic estimation useful for medicinal picture study and judgment. The conventional framework for wavelet combination is upgraded and an alternate calculation of restorative picture combination is presented. At that moment that picking high recurrence coefficients, the area edge intensities of each and every one sub-picture are figured to recognize versatile combination. The reduced recurrence coefficient picking is centered around edges of pictures, with the goal that the melded picture can ensure all profitable information and shows up doubtlessly. Apply the customary and improved combination calculations centered around wavelet change to breaker pictures and besides survey the combination results. It has been demonstrated that the calculation can effectively hold data of special pictures and update their edges and surface peculiarities. This new calculation surpasses conventional combination calculation centered around wavelet change. Ujwala Patil et al. [6] recommended that consolidating several enlisted pictures of the unclear spot to obtain various instructive pictures is named picture combination. Essential part investigation is just a noticeable methodology for gimmick extraction and measurement diminishment. Picture combinationand calculation joins together pyramid and important segment investigation methods and remove the product quality dissection of progressive key part examination combination calculation without suggestion picture. There is a creating necessity for the product quality examination of the combination calculations. We indicate combination utilizing wavelet and essential segment examination combination strategies and takeout creation dissection for these combination systems utilizing remarkable quality measures for mixture of data sets and show that proposes picture combination utilizing various leveled chief part investigation is great for the combination of multimodal imaged. Xing Su-xia et al. [7] has recommended that infrared and unmistakable picture combination routines can enhance the picture differentiate, and grow the night vision compelling. The rehashed infrared and noticeable pictures from the relative scene were vague by non-sub examined form let change; take following the evaluated mass found the middle value of, high-recurrence attributes segment according to the weighted of the area standard deviation share; then your combination picture is obtained by opposite non-sub inspected shape let change; the combination pictures were appear differently in terms of the effect acquired by Laplace change, wavelet change and form let change amid a boundless numeral of trails, and the product quality examination was carried out through the clamor test. Non-sub tested shape let change can accomplish pervasive combination result, and high caliber. Ahmed Abd-el-kader et al [8] has mentioned that bend let change is definitely an as recently form multi-scale changes, which is further adequate for things with bends. Picture combination suggests the combining pictures into a picture that has the incredible information without making peculiarities that are

story in the specific pictures. Two well-known applications of picture combination are located; combination of multi-center pictures and combination of multi presentation pictures. Combination effects were surveyed and balanced as shown by three measures of execution; the entropy (H), the shared data (MI) and the measure of edge data (QABIF). The three execution measures have showed that the bend let based picture combination calculation gives preferred combined picture within the wavelet calculation. The melded picture features a predominant eye perception than the info ones. Ghimire, D et al. [9]has proposed a method for image enhancement in HSV space focused around the area processing of image. In this particular technique an upgrade is connected just on V component and H and S component usually are not changed during improvement so the first color with the improved image seriously isn't modified. Relying on the subjective and objective execution assessment, the proposed system has demonstrated experienced in image improvement. The destination criteria like Detail Variance, Background Variance and statistical attributes demonstrates that proposed strategy deliver better images when compared with other systems like histogram equalization and AINDANE. Aribi, W. et al. [10] explained that the character with the medical image might be assessed by few image fusion techniques. The fusion of images improves the information to be ready by combining the information from selected images and picking a fusion technique will depend on upon the application. For instance, this paper addresses the MRI and PET images. Here, eight image fusion methods referred as Laplacian, FSD, Gradient RATIO, Morph, Contrast, DWT and SIDWT systems have talked about. The parameters considered to be the assessment of the desired info is Mutual Information, Universal Image quality Index and mean SSIM. The acquired result demonstrates that this RATIO and contrast procedures introduce the best comes about. Kiran parmar et al. [11] has analyzed that this outline is to help the image content by fusing images like computer tomography and magnetic resonance imaging images; magnetic resonance imaging gives the high-quality data on delicate tissue while computed tomography gives better more knowledge about substantial tissue. Fusing both these types of images produce a complex image that's more instructive than different signals gave by a person modality. Image fusion has become a typical operation used within medical diagnostics and therapy. Fast Discrete Curve let Transform using Wrapper algorithm based image fusion method, is execute, examine and contrasted with Wavelet based Fusion Technique. Fusion of images concentrates at diverse purposes; power through distinctive systems helps doctor to withdraw the qualities that most likely are not normally visible within an individual image by different modalities. Vivek Kumar gupta et al. [12] has analyzed that in remote sensing program the raising accessibility of space persevered sensors offer spark to picture combination calculations. Remote sensing picture combination plan at arranging the info exchange by data got which hide unique parts of the electromagnetic range at various spatial, transient and phantom determination; we can secure multi-fleeting, multi-determination and multi-recurrence picture information for basis for gimmick extraction, demonstrating and arrangement. The combined picture is quite a bit serviceable for human data. Intertwined picture is a bit more useful for programmed machine dissection errand for example characteristic extraction, division and article distinguishment. Sruthy, S et al. [13] has mentioned which the Image Fusion is the process of joining data of a couple of pictures right solitary picture which often can hold immeasurably imperative peculiarities of the all unique pictures. Here the data to combination includes set of images extracted from diverse modalities of the scene. Yield is really a superior quality picture; which utilizes upon a specific application. The marked of combination is to generate a picture which depicts a scene preferable or significantly higher over any single picture concerning some significant properties giving an instructive picture. These combination strategies are critical in diagnosing and treating disease in restorative fields. This paper concentrates on the improvement of a graphic combination technique utilizing Dual Tree Complex Wavelet Transform. The outcome demonstrates the proposed calculation carries a finer visual quality than the bottom routines. Additionally the character of the intertwined picture is assessed utilizing a collection of value measurements. Desale, R.P. et al. [14]has examined different image fusion methods such as PCA (principal Component Analysis), DCT (Discrete Cosine Transform)and DWT (Discrete Wavelet Transform) based image fusion methods. Authors have recommended picking a DWT based fusion solution to top quality and exactness applications. On this paper two algorithms focused around DWT are proposed for example, Pixel averaging and maximum pixel replacement algorithm. The execution of above said DWT's are contrasted along with the PCA and DCT fusion techniques. The examination is executed focused around seven parameters

named as PSNR, MSE, Normalize absolute error, Maximum Difference, Average difference, Normalized Cross-Correlation and structural content. The outcome portrays which the execution of DWT based fusion strategies is altogether better as contrast with an alternate routine for image fusion. Om parkash et al. [15] has analyzed that the purpose of image fusion is to take appropriate data out of a couple of images of the area right solitary image and that is much informatory and it is considerably better for human information. Spatial domain based operations make spatial distortions from the fused image. Spatial domain distortion can be totally overseen by the use of wavelet transform based image fusion processes. Using supreme greatest fusion rule wavelet coefficients at unique decomposing levels are fused. Two weighty characteristics wavelet symmetry and linear phase of BWT are took preferences (exploited) for image fusion in light that they might ensure edge data. It has been revealed that the wavelet transform technique improve fusion quality by decreasing loss of significant data usable in solitary images. Shutao Li et al. [16] has analyzed that the quick and powerful image fusion techniques is proposed to make an extremely instructive fused image through uniting numerous images. Image fusion strategy is with different two-scale decomposition of your image right first layer containing large scale variations in intensity, and also a priority layer catching little scale details. A novel guided filtering- based weighted average technique is proposed to make full consumption of spatial consistency for fusion of the bottom and priority layers. It has been revealed that the proposed system can acquire state-of-the-art execution for fusion of multispectral, multi-focus, multimodal, and multi-exposure images. Mohammed Hossny et al. [17] has discussed that image fusion methodology join together various images into individuals enlightening image. Image fusion metrics are creating from image processing variance metrics. In Image fusion metrics: evolution simply speaking the evolution of objective image fusion performance metrics along with subjective and goal acceptance. It clarify as to what way fusion execution metric create starting with image difference measurement, its understanding into image fusion connections, it limit weighting component along with the acceptance operation. R. Amutha et al.[18]has discussed that classy and efficient multi-focus image fusion framework clearly planned for wireless visual sensor framework prepared with resource constrained, unsafe setting like battlefields. The fusion of multi-focus images is focused around higher esteemed Alternating Current coefficients computed in Discrete Cosine Transform domain. Discrete cosine transform defeats the computation as well as confinement of low power gadgets and it is explored with regards to image quality and computation energy. It confirms the functional efficiency enhancement of the proposed system in yield quality as well as consumption, when contrasted to fusion techniques DCT domain.

4.CONCLUSION AND FUTURE SCOPE

Image fusion is a procedure of combining the related information from multiple images into a single image where the fused image will be more useful and accomplish than some of the input images. Image fusion means the combining of multiple images into a sole image that has the utmost information contented without producing facts that are missing in a given image. The idea of image fusion in multi-focus cameras to combine data from various images of the similar landscape in order to bring the multi focused image. Discrete cosine transform is an image fusion method which is extra appropriate and acceptable in real-time systems using discrete cosine transform based standards of motionless image or video. The image fusion methods using discrete cosine transform (DCT) are considered to be more appropriate and time-saving in real-time systems using motionless image or video standards based on DCT. But has been found that the majority of the existing researchers have ignored some of the well-liked issues of vision processing like image de-noising, image enhancement, and image restoration.

So to control these troubles a new algorithm will be proposed in near future.

REFERENCES

[1] Haghighat, Mohammad Bagher Akbari, Ali Aghagolzadeh, and Hadi Seyedarabi. "Real-time fusion of multi-focus images for visual sensor networks." In Machine Vision and Image Processing (MVIP), 2010 6th Iranian, pp. 1-6. IEEE, 2010.

[2] Tao, Ling, and Zhi-Yu Qian. "An improved medical image fusion algorithm based on wavelet transforms." Natural Computation (ICNC), 2011 Seventh International Conference on. Vol. 1. IEEE, 2011

[3] Patil, Ujwala, and Uma Mudengudi "Image fusion uing hierarchical PCA." Image Information Processing (ICIIP), 2011 International Conference on. IEEE,2011.

[4] Su-xia, Xing, et al "Image Fusion Method Based on NSCT and Robustness Analysis." Computer Distributed Control

and Intelligent Environment Monitoring (CDCIEM), 2011 International Conference on. IEEE, 2011

[5] Ahmed Abd-el-kader , Hossam El-Din Moustafa , SamehRehan "Performance Measures for Image Fusion Based on Wavelet Transform and Curvelet Transform" 28th NATIONAL RADIO SCIENCE CONFERENCE(NRSC 2011)April 26-28, 2011, National Telecommunication Institute, Egypt

[6] Ghimire Deepak and Joonwhoan Lee. "Nonlinear Transfer Function-Based Local Approach for Color Image Enhancement." In Consumer Electronics, 2011 International Conference on, pp. 858-865. IEEE,2011.

[7] Aribi, Walid, Ali Khalfallah, Med Salami Bouhlel, and Noomene Elkadri. "Evaluation of image fusion techniques in nuclear medicine." In Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on, pp. 875-880. IEEE, 2012.

[8] Parmar,kiran, RahulK.Kher, and Falgun N. Thakkar, "Analysis of CT and MRI Image Fusion Using Wavelet Transform." Communication Systems and Network Tech nologies (CSNT), 2012 International Conference on. IEEE.2012

[9] Gupta, Vivek Kumar, Amit Neog, and S. K. Katiyar "Analysis of image fusion techniques over multispectral and microwave SAR images." Communications and Signal Processing (ICCSP), International Conference on.IEEE, 2013.

[10] Sruthy, S., Latha Parameswaran, and Ajeesh P. Sasi. "Image Fusion Technique using DT-CWT." In Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Conference on, pp. 160-164. IEEE, 2013.

[11] Desale, Rajenda Pandit, and Sarita V. Verma. "Study and analysis of PCA, DCT & DWT based image fusion techniques" IEEE International Conference on Signal Processing Image Processing & Pattern Recognition (ICSIPR), Coimbatore, pp. 66-69, 7-8 Feb., 2013.

[12] Prakash, Om, Richa Srivastava, and Ashish Khare "Biorthogonal wavelet transform based image fusion using absolute maximum fusion rule." Information & Communication Technologies (ICT), 2013 IEEE Conference on. IEEE, 2013.

[13] Li, Shutao, Xudong Kang, and Jianwen Hu. "Image fusion with guided filtering."IEEE transactions on image processing: a publication of the IEEE Signal Processing Society 22.7 (2013): 2864-2875.

[14] Hossny, Mohammed, et al "Image fusion metrics: evolution in a nutshell."ComputerModelling and Simulation (UKSim), 2013 UKSim 15th International Conference on.IEEE, 2013.

[15] Phamila, Y., and R. Amutha "Discrete Cosine Transform based fusion of multi-focus images for visual sensor networks." Signal Processing 95 (2014): 161-170.

Evaluating the key findings in Image Segmentation Techniques

Rozy Kumari[1], Narinder Sharma[2]
Dept. Of Electronics and Communication Engineering
Amritsar College of Engineering and Technology
Amritsar, Punjab, India.
rozy2302@gmail.com, narinder.acet@gmail.com

Abstract: - Image segmentation plays an important role in digital image processing. Number of applications are based on the image segmentation techniques like face detection, object detection etc. A review has been conducted on different familiar image segmentation techniques. But it is established that the noise in images has an effect on the segmentation results a lot. This research work has recommended a modified enhanced region growing method using ACPC and relaxed median filter which has the capability to give exact results even when the high density of the noise is in the input image or also when image is noise free.

Keywords:- Image Segmentation, Segmentation Techniques, ACPC

1. Introduction

Image segmentation is determined as a vital and a significant operation for meaningful study and analysis of images obtained [1]. It is division of an image into homogeneous sections, for every the option criterion like intensity, color, tone or texture, etc. The aim of the segmentation method is to make simpler and modify the illustrations of an image into more significant and make easier to examine [2][3]. Several image processing techniques are based on threshold based, edge based, region based methods and cluster based. As the division of intensity in tissue is composite, threshold determination becomes difficult [4] [5]. Edge based segmentation works by finding the location of discontinuities in the image. It makes decision whether pixels are in edge or not. Results from edge detection are post processed to join edges into edge chains to symbolize the region border [6]. The region based segmentation constructs the region of panels directly. The images composed from satellite have large amount of information for examination and processing. The Image Segmentation is utilized in medical imaging like finding tumors and additional pathologies, in calculating tissue volumes, in computer-guided surgery, analysis, cure planning, examine of anatomical structure. While developing segmentation algorithms has attracted considerable attention, comparatively fewer efforts have been spent on their evaluation, though many newly developed algorithms are compared with some particular algorithms with few particular images. Moreover, most efforts spent on evaluation are just for designing new evaluation methods and only very few authors have attempted to characterize the different evaluation methods existed [7].

2. Image Segmentation Techniques

2.1 Fixation-Based Segmentation Method

Here, bottom-up image segmentation is considered. That is, we disregard (top down) assistance from object detection in the segmentation method and we imagine segmenting images without identifying objects. For a specified fixation point, segmenting the section/thing having that point is a two step process:

1. Cue Processing: Image signs like color, texture, movement and stereo produce a probabilistic border edge map in which the chances of a pixel to be at the border of any object in the picture is accumulated as its intensity.

2. Segmentation: For a specific fixation point, the best closed contour (connected set of boundary edge pixels) around that point in the probabilistic edge map. Though, the edge map includes two types of edges, that is, boundary (or depth) and internal (or texture/intensity) edges therefore it is important to be capable to distinguish among the boundary edges from the non-boundary (e.g. texture and internal) edges.

Fig.1 (a) **Fig.1 (b)**

Figure 1: For the two fixations points, indicated by the green crosses, on object in fig. 1 (a), this method segments the corresponding regions enclosing fixation points in fig. 1 (b),

2.2 The Grab Cut segmentation algorithm

It is based on Image segmentation by graph cut [8] approach for image segmentation. The innovation of this approach lies first in the managing of segmentation. Two improvements are made to the graph cuts mechanism: iterative estimation and incomplete labeling which mutually allow a significantly reduced degree of user communication for a given eminence of result. This permits Grab Cut to place a light load on the client, whose communication consists simply of dragging a rectangle about the preferred object. In doing so, the user is representing a section of surroundings, and is independent of any requirement to mark a foreground section. Another method is extended for alpha calculation, employ for border matting; where the alpha values are normalized to diminish noticeable artifacts [9].This is pursued by border matting in which alpha values are calculated in a fine strip just about the hard segmentation boundary.

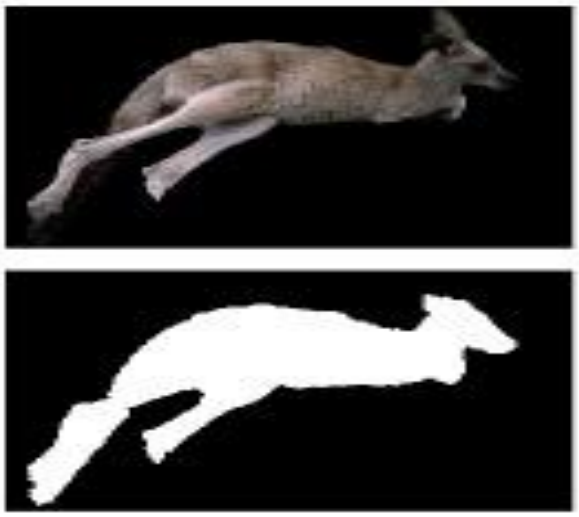


Fig 2: Grab-Cut Segmentation Method.

2.3 Normalized Cuts and Image Segmentation:

The normalized cut principle determines both the total variation between the dissimilar groups as well as the total resemblance within the groups [10]. In this process, image segmentation is delighted as a graph separating problem and suggests a novel global principle, the normalized cut, for segmenting the graph i.e. a new graph-theoretic principle is planned for calculating the integrity of an image partition, the normalized cut. The minimization of this principle can be originated as a general Eigen value problem. The eigenvectors can be applied to build excellent division of the image and the practice can be sustained recursively as preferred.

Fig 3: Normalized Cut Segmentation Method.

2.4 Graph-Based Image Segmentation

This method divides an image into regions. A predicate is identified for calculating the confirmation for a border among two sections using a graph-based demonstration of the image. A well-organized segmentation algorithm is after that developed support on this predicate, and revealed that even though this algorithm makes insatiable decisions it creates segmentations that assured global possessions. The algorithm is pertained to image segmentation by two dissimilar types of local neighborhoods in creating the graph, and demonstrates the results with equally real and synthetic images [11]. The method lopes in time almost linear in the number of graph edges and is also quick in performance. A significant feature of the process is their capacities to defend feature in low-variability image sections whereas disregard features in high-variability sections.

Fig 4: Graph-Based Segmentation Method

3. Literature Survey

Salem Saleh Al-amri [12] has concerned Mean technique, Pile technique, HDT, and EMT technique on three satellite images to choose the best segmented image. Testing and relative analysis of methods have exposed that Histogram Dependent Technique and Edge Maximization Technique are the most excellent thresholding methods which executes better as evaluated to all other thresholding methods.

Karoui [13] proposed an unsupervised image segmentation method by using level set methods and texture statistics. They confirmed that process developed by them is dissimilar from other methods since it doesn't imagine autonomous variable, and it doesn't confine to first order grey features. Feature collection step to re-adjust the weights of every feature to acquire the segmentation is integrated in the performance. In experimental stage, filter response histogram is used to evaluate the total number of distributions; haar wavelet is applied to calculate the energy of image wavelet of every band. PDE is used to re-initialize the level sets.

Yu Xiaohan [14] developed a new image segmentation technique which supports the region growing and edge detection methods. Their hybrid process assists the segmentation process to stay away from faults when both techniques are used in a different manner. Region growing is applied to find the edge pixels in the image, whereas 2nd order derivative is employed for edge detection. Experiments are performed on 3D MRI image data. Gaussian method is applied for smoothing intention after edge detection. Results have revealed that their method is enhanced in order to maintain more edge information.

Wesolkowsk [15]-[16] included the Markov Random Fields used for edge and region found hybrid color image segmentation. Line procedure is applied by using edge detection algorithm. Vector angle measure is used at the same time to calculate the distance between pixels in order to detect edges. The main difficulty with their method is that it is a pixel neighbor form and has the same restrictions of region growing process. A parameter estimation technique is applied to estimate the MRF model.

Cevahir Cigla [17] obtained a graph theoretic color image segmentation technique, and seeks to increase the normalized cut image segmentation process. They applied image with weighted un-directed graph, whereas nodes stand for the regions, and weights among nodes characterize the intensity match of neighboring regions. Their changed normalized cut technique has conquered the difficulty of over segmentation in which spare regions are formed for image. The results revealed that proposed technique to improve the NCIS algorithm.

Yong-mei Zhou [18] offered a new region-based image segmentation method with the help of mean-shift clustering process. First of all, their approach focus on color, surface, and area customs of all pixel of an image, in addition, create the sets on the basis of those features employing mean-shift clustering methodology, mark the all region, and finally make section of image on the basis of these marks. They used Matlab 7.0 to actualize their algorithm. Analysis shows that their technique present improved bring about term of speed and segmentation.

Ying-Tung Hsiao [19] proposed a new image segmentation procedure by combining morphological operator with region growing method. First of all they used morphological closed process to get better image and after that execute edge detection utilizing dilation remains edge detector. After it, they pass on developing seeds and execute the region growing process for image segmentation. Afterward than, region merging and edge detection is carried out on the images. They do experiments on table tennis, girl and MRI image. Snake boundary state method [20] is employed to get improved edge detection results. Every experiment is conducted in Visual C++.

Amjad Zaim [21] has established that segmentation of prostate boundaries from ultrasound images is a difficult job for surgical events. They planned a novel edge based segmentation method for prostate ultrasound image. Phase symmetry is used to get the edge detection on the ultrasound images. Median filter is used to decrease the noise. Edge extraction and edge connecting is used to creates the final edge based segmentation image. The main advantage is that their methods don't want any human intervention. Outcome of contour produced by their method are compared with manually segmented contours, and accuracy of 87% is found.

Xuejie Zhang [22] proposed a innovative Fast learning Artificial Neural Network (FLANN) supported color image segmentation approach for R-G-B-S-V (i.e., RGB and HSV) cluster space. In first step, noise is eliminated using 3*3 averaging filter to reduce the inequality in color distribution. In second step, pixels are transformed to RGBSV space using HSV conversions. FLANN clustering is carried out to create a cluster result of image. Next, pixels with same color are being divided. Segment number is allocated to each segment of image. Result of tolerance and neighborhood size is observed. Outcomes have shown that proposed method produced ideal segments for colors in the image.

Farhad Mohamad Kazemi [23] planned a quick C-means based preparing of Fuzzy Hopfield Neural system [24] through a specific finished goal to relay it into picture division. Target capability is employed and focused around 2-f Fuzzy HNN. This target capacity exposed the normal separation among picture pixels and group's centroids. As per creator, Fuzzy HNN provides better separation as contrast with different methods. Initially, they create groups from given information, then perform standardization, i.e. ash level pictures, compute centroids, then register separations, find new centroids, and machine new enrollment capacity worth utilizing fluffy C-implies [25]. The results have established that FHNN provides a speedier speed as contrast with dissimilar procedures of ANN.

Gloria Bueno [26] presented another approach for division of anatomical arrangement in recovery pictures. Versatile PDE models, i.e., fluffy PDE Contour model, and PDE geometrical

Contour model with Fuzzy C-Means order is utilized for division of pictures. Versatile PDE models served to discover the locale of investment. 3d mind MRI Image is utilized as a dataset. Fluffy PDE model has portion the MRI mind picture utilizing Fuzzy Clustering methodology. The model has beated “Snakes” display and diminishes some of downsides of Snakes model.

Preetha et al. [27] in paper has proposed a programmed seeded locale developing calculation for portioning shade pictures. They have evaluated some division methods, for example, threshold is centered around the neighborhood pixel data of the picture and ignore the spatial data of the pixel values hereafter they are improvident for pictures that unclear at article limits or for a variety of picture part division calculation, Histogram all the pixels are computed and issue related is clamor ,Edge strategy Based on unexpected changes in power and issue is that, it require extra post preparing by utilizing interfacing strategies to gather edge pixel into valuable edges. Edge based is to segment the picture into a few disjoint locales. What's more issue is in selecting beginning seeds. It has changed over RGB shade picture into HIS color space and performed division utilizing district developing and combining. At first a seed IS chosen with the comparability conditions and afterward by considering the size and the Euclidean separation as the homogeneity capacity locales are blended. This technique uses separate limit values for locale uniting and district developing. It permits control over the level of division by changing the forces of HSI in its Euclidean separation.

Zhu Zhengtao et al. [28] in paper have proposed quick extraction of the locale of enthusiasm, sparing valuable time. This paper analyzed the conventional picture division systems, and received locale developing procedure focused around direct checking. Such method needs not to lead entangled operation to point out beginning seeds however the known info picture structure is principal to its legitimacy. It gives a quick extraction of the area of-enthusiasm, sparing valuable time for taking after medications. This examined strategy is particularly relevant to on-line items investigation focused around machine vision, as the structure of the pictures are as of now known and are moderately settled.

Chaobing et al.[29] in paper has proposed a division via programmed seed choice and locale developing .It has utilized two methods for non-edge and smoothness to focus beginning seeds. No-edge expresses that the pixels are not on the edge or definite area and introductory seed pixel along these lines acquired must have the esteem short of what limit. Smoothness expresses that the pixels have high comparability to its neighbors and starting seed pixel got must have the esteem short of what edge. At that point these seed focuses acquired are fused to structure seed locale. By controlling the measure of area and shade separation of district, division might be accomplished tastefully.

Sakakezia et al. [30] paper "A shade surface based division technique to concentrate object from foundation" proposed a picture composition division calculation to concentrate data from complex foundation. Division is a procedure which segments a picture into different districts. From the division results, it is conceivable to distinguish districts of investment and questions in the scene, which is extremely helpful to the ensuing picture investigation. There are few programmed calculations that can work well on a substantial mixed bag of information. The issue of division is troublesome in light of picture surface. In the event that a picture contains just homogeneous shade locales, grouping routines in color space are sufficient to handle the issue. In such cases, the robotization of division is extremely crucial. It proposed a two stage model to portion the color pictures, one to partition the frontal area and foundation and an alternate model to concentrate the peculiarities of the picture. The data which the normally utilized grayscale picture is insufficient for division. The shade pictures can give more data. Accordingly, division focused around shade picture can beat a few deficiencies of ash scale picture. Both shade and composition gimmicks are considered. The surface division velocity is quicker and without human investment, the division results have additionally demonstrated noteworthy change over existing calculations.

Y.u, Jian et al. [31] in paper proposed a composition picture division strategy focused around Gaussian mixture models (gmm) and ash level co-event matrix (glcm). Composition picture division is a critical system in picture handling. It has a broad application in numerous spaces, for example, machine vision, picture investigation. Numerous sorts of measurable models have been connected to composition picture arrangement. It incorporates Markov Random Field Models (MRF) and Gaussian mixture models (GMM) expect multivariate Gaussian dispersions for the peculiarities. Surface gimmicks are concentrated by light black level co-event framework. Anyway light black level co-event network is simply quantitative portrayal of surface and not ready to be used specifically to concentrate peculiarities of composition picture. Consequently, the surface properties are portrayed by eight statics produced by light black level co-event lattice (GLCM) including mean, difference, precise second minute (ASM), entropy, opposite distinction minute (IDM), contrast, homogeneity (HOM), co-connection. Texture peculiarity space was structured by these statics and ordered Gaussian mixture models (GMM) bunching strategy whose parameters are evaluated by desire augmentation (EM) calculation to composition division. It upgrades the division exactness of composition picture and give the better division comes about over existing calculations.

4. Gaps in Literature

After conducting the literature survey it has been found that the automation of initial seed placement in region growing required to be discovered because random initial seed dependent upon regions based upon their positions and also may result inappropriate in case of complex regions.

1. In previous research work of seed placement, the technique followed was to find the edge using edge based method. Based on that edge of an object or scene centroid calculation was performed and seed placement was done on the centroid. But in this scenario it was not always possible to find the centroid of all the regions in the image. So a modified ACPC region growing algorithm which will utilize the centre of gravity to select the initial seed placement.
2. The high density of noise is as well disregarded in the presented methods so high density noise exclusion technique is necessary to enhance the results ahead.

So automation of the initial seed placement in ACPC algorithm and reducing the high density noise from images is the main motivation of this research work.

5. Conclusion and Future Scope

In this paper, a survey on various image segmentation methods has been made. After conducting the literature survey it has been found that the automation of initial seed placement in region growing required to be discovered because random initial seed dependent regions based upon their positions. In previous research work of seed placement, the method followed was to locate the edge by using edge based method. Based on that edge of an object or scene centroid calculation was performed and seed placement was done on the centroid. But in this scenario it was not always possible to find the centroid of all the regions in the image by placing the manual seed. In near future work will be extended for medical applications as well as for satellite images. We will also integrate genetic algorithm with automate the initial seed placement for better quality of segmentation and will refine the seed placement region growing algorithm.

References

[1] Ben Chaabane S, Sayadi M, Fnaiech F, Brassart E. Colour Image Segmentation using Homogeneity method and Data Fusion Techniques.*Eur. J. Adv. Signal Process*, 30: 55-71, 2009.

[2] X.Li, X.Lu, J.Tian," Application of fuzzy c-means clustering in data analysis of metabolomics", Analytical chemistry, Vol 80, no.11, pp. 4468-4475, 2009.

[3] Ganesan, P., and V. Rajini. "Segmentation and Denoising of Noisy Satellite Images based on Modified Fuzzy C Means Clustering and Discrete Wavelet Transform for Information Retrieval." *International Journal of Engineering & Technology (0975-4024)* 5.5 (2013).

[4] H. Suzuki and J. Toriwaki, "Automatic segmentation of head MRI images by knowledge guided thresholding," Comput. Med. Imag. Graph., vol. 15, no. 4, pp. 233–240, 1991.

[5] L. Lemieux, G. Hagemann, K. Krakow, and F. G. Woermann, "Fast, accurate, and reproducible automatic segmentation of the brain in T1-weighted volume MRI data," Magn. Reson. Med., vol. 42, pp. 127–135,1999.

[6] Image segmentation based on edge detection using boundary code, International Journal on innovative.

[7] Y.J.Zhang and J.J.Gerbrands, Segmentation evaluation using ultimate measurement accuracy, SPIE 1657, 449-460 (1992).

[8] Y.Y. Boykov and M.P. Jolly, "Interactive Graph Cuts for Optimal Boundary and Region Segmentation of Objects in nd Images," Proc. Eighth IEEE Int'l Conf. Computer Vision, pp. 105-112, 2001.

[9] C. Rother, V. Kolmogorov, and A. Blake, "GrabCut':Interactive Foreground Extraction Using Iterated Graph Cuts," ACM Trans. Graphics, vol. 23, no. 3, pp. 309-314, 2004.

[10] J. Shi and J. Malik, "Normalized Cuts and Image Segmentation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 8, pp. 888-905, Aug. 2000.

[11] P.F. Felzenszwalb and D.P. Huttenlocher, "Efficient Graph-Based Image Segmentation," Int'l J. Computer Vision, vol. 59, no. 2, pp. 167-181, 2004. S

[12] . S. Al-amri and N. V. Kalyankar, "Image segmentation by using threshold techniques," *Journal of Computing*, vol. 2, no. 5, May 2010.

[13] I. Karoui, R. Fablet, J. Boucher, and J. Augustin, "Unsupervised region-based image segmentation using texture statistics and level-set methods," in *Proc. WISP IEEE International Symposium on Intelligent Signal Processing*, 2007, pp. 1-5,2007.

[14] X. Yu and J. Yla-Jaaski, "A new algorithm for image segmentation based on region growing and edge detection," in *Proc. IEEE International Sympoisum on Circuits and Systems*, pp. 516-519, 1991.

[15] S.Wesolkowski and P. Fieguth, "A Markov random fields model for hybrid edge-and region-based color image segmentation," in *Proc. Canadian Conference on Electrical and Computer Engineering,*. 2002, pp. 945-949.

[16] M Sharif, J. H Shah, S. Mohsin, and M. Raza, "Sub-holistic hidden markov model for face recognition," *Research Journal of Recent Sciences*, vol. 2, no. 5, pp. 10-14, 2013.

[17] C. Cigla and A. A. Alatan, "Region-based image segmentation via graph cuts," in *Proc. 15th IEEE International Conference on Image Processing*, 2008, pp. 2272-2275.

[18] Y. M. Zhou, S. Y. Jiang, and M. L. Yin, "A region-based image segmentation method with mean-shift clustering algorithm," in *Proc. Fifth International Conference on Fuzzy Systems and Knowledge Discovery*, 2008, pp. 366-

370. Y. T. Hsiao, C. L. Chuang, J. A. Jiang, and C. C. Chien, “A contour based image segmentation algorithm using morphological edge detection,” in *Proc. IEEE International Conference on Systems, Man and Cybernetics*, 2005, pp. 2962-2967.

[19] W. Haider, M. S. Malik, M. Raza, A. Wahab, I. A. Khan, U. Zia, J. Tanveer, and H. Bashir, “A hybrid method for edge continuity based on Pixel Neighbors Pattern Analysis (PNPA) for remote sensing satellite Images,” *Int'l J. of Communications, Network and System Sciences*, vol. 5, pp. 624-630, 2012.

[20] Zaim, “An edge-based approach for segmentation of prostate ultrasouind images using phase symmetry,” in *Proc. 3rd International Symposium on Communications, Control and Signal Processing*, 2008, pp. 10-13.

[21] X. Zhang and A. L. P. Tay, “Fast learning artificial neural network (FLANN) based color image segmentation in RGBSV cluster space,” in *Proc. International Joint Conference on Neural Networks*, 2007, pp. 563-568.

[22] F. M. Kazemi, M. R. Akbarzadeh, T. S. Rahati, and H. Rajabi, “Fast image segmentation using C-means based Fuzzy Hopfield neural network,” in *Proc. Canadian Conference on Electrical and Computer Engineering*, 2008, pp. 001855-001860.

[23] M. Yasmin, M. Sharif, and S. Mohsin, “Neural networks in medical imaging applications: A survey,” *World Applied Sciences Journal*, vol. 22, pp. 85-96, 2013.

[24] W. Haider, M. Sharif, and M. Raza, “Achieving accuracy in early stage tumor identification systems based on image segmentation and 3D structure analysis,” *Computer Engineering and Intelligent Systems*, vol. 2, pp. 96-102, 2011.

[25] S. Bueno, A. M. Albala, and P. Cosfas, “Fuzziness and PDE based models for the segmentation of medical image,” in *Proc. Nuclear Science Symposium Conference Record, IEEE*, 2004, pp. 3777-3780.

[26] Preetha, M. Mary Synthuja Jain, L. Padma Suresh, and MJohnBosco. "Image segmentation using seeded region growing." Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on. IEEE, 2012.

[27] Zhengtao, Zhu, et al. "Fast capsule image segmentation based on linear region growing." Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on.Vol. 2.IEEE, 2011.

[28] Huang, Chaobing, Quan Liu, and Xiaopeng Li. "Color image segmentation by seeded region growing and region merging." Fuzzy Systems and Knowledge Discovery (FSKD), 2010 Seventh International Conference on.Vol. 2.IEEE, 2010.

[29] Calderero, Felipe, and Ferran Marques. "Region merging techniques using information theory statistical measures." Image Processing, IEEE Transactions on 19.6 (2010): 1567-1586.

[30] Jian, Y. U. (2010, December). Texture Image Segmentation Based on Gaussian Mixture Models and Gray Level Co-occurrence Matrix. In Information Science and Engineering (ISISE), 2010 International Symposium on (pp. 149-152). IEEE.

ROLE OF SIGNAL PROCESSING IN VOICE-SPEECH RECOGNITION

Sabiapreet Bedi[1]
Research Scholar
Department of ECE
ACET, Amritsar

Sandeep kaushal[2]
Associate Professor
Department of ECE
ACET, Amritsar

Gursharan Singh[3]
Research Scholar
Department of ECE
ACET, Amritsar

***Abstract*—Speech Recognition also called automatic Speech Recognition (ASR) is a digital signal process technique of converting speech signal into same sequence of words and the research issues in ASR are like various types of speech classes, speech representation, and feature extraction techniques. So, the problem which are existing and technique used to solve these problems are designed by researchers. The problems that are existing in speech recognition (SR) and the various techniques to solve these problems have been constructed by various research scholars. In the present paper is an effort for presenting a dynamic network with a multistream structures and observations of articulator feature classifier scores which models by varying a degree of co-articulation in a principled way. This paper concludes various deep processing structure which provides improvements for genre and structure with which they are in corporate including various layer width and significant the factors.**

***Keywords*—Automatic Speech Recognition (ASR), Articulator feature, Digital signal, Feature extraction techniques, Speech Representation.**

I. INTRODUCTION

The fundamental purpose of speech is communication i.e., the transmission of messages. According to Lawrence R.Rabiner [1] a message represented as a sequence of discrete symbols can be quantified by its information content in bits, and the rate of transmission of information is measured in bits/seconds (bps).Yuan Meng [2] says Digital Signal Processing (DSP) is the most commonly used hardware that provides good development flexibility and requires relatively short application development cycle. Tez Yoneticis [3] says speech is the primary communication medium between people. This communication process has a complex structure consisting not only the transmission of voice, the language ,gestures ,the subject and the capability of the listener contribute .Disimitrios S.Koliousis [4] says the overall work of voice-speech processing is expected to be applied to an efficient, flexible, and robust human-machine interface system, capable of directing robotic units performing military missions, without debilitating, hampering, or interfering with a war fighter's field operations.M.A.Anusuya [5] says the main goal of speech recognition area is to develop techniques and systems for speech input to machine. Speech is the primary means of communication between humans. Mehryar Mohri [6] says Finite-state acceptors and transducers have been successfully used in many natural language-processing applications, for instance the compilation of morphological and phonological rules and the compact representation of very large dictionaries. Nelson Morgan [7] says Speech recognition methods converged by 1990 into statistical approaches based on the hidden Markov model (HMM), while artificial neural network (ANN) approaches in common use tended to converge to the multilayer perception (MLP) incorporating back-propagation learning. Fernando Pereira [8] says A weighted transducer puts weights on transitions in addition to the input and output symbols. Weights may en- code probabilities, durations, penalties, or any other quantity that accumulates along paths to compute the overall weight of mapping an input string to an out- put string. Richard M.Stern [9] says a continuing problem with current speech recognition technology is the lack of robustness with respect to environmental vari- ability. For example, the use of microphones other than the ARPA standard Sennheiser HMD-414 "close-talking" headset (CLSTLK) severely degrades the performance of systems like the original SPHINX system, even in a relatively quiet office environment. Joris Pelemans [10] says Automatic Speech Recognition (ASR) is still no match for Human Speech Recognition (HSR) and it is likely that this won't change in the near future. Nevertheless, ASR has already proven its value in a lot of applications: children are using automatic tutors to improve their reading skills; doctors are gaining time and money using diction software; disabled people are able to control the computer with voice but not with keyboard.

II. BASIC MODEL OF SPEECH RECOGNITION:

In speech processing and communication for the most part, was motivated by people s desire to build mechanical models to emulate human verbal communication capabilities. Speech is the most natural form of human communication and speech processing has been one of the most exciting areas of the signal processing. Speech recognition technology has made it possible for computer to follow human voice commands and understand human languages. Based on major advances in statistical modelling of speech, automatic speech recognition systems today find

widespread application in tasks that require human machine interface, such as automatic call processing in telephone networks, and query based information systems they provide updated travel information, stock price quotations, weather reports, Data entry, voice dictation, access to information: travel, banking, Commands, Avionics, Automobile portal, speech transcription, Handicapped people (blind people) supermarket, railway reservations etc. This report reviews major highlights during the last six decades in the research and development of automatic speech recognition, so as to provide a technological perspective. Although many technological progresses have been made, still there remain many research issues that need to be tackled. . The recognition process is shown below (Fig .1).

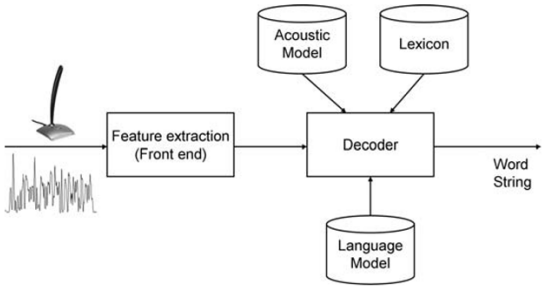


Fig 1: Speech recognition system [16]

III. TYPES OF SPEECH RECOGNITION:

Speech recognition systems can be separated in several different classes by describing what types of utterances they have the ability to recognize. These classes are classified as the following:

A. Isolated Words

B. Connected Words

C. Continuous Speech

D. Spontaneous Speech

A. Isolated Words

Isolated word recognizes attain usually require each utterance to have quiet on both side of sample windows. It accepts single words or single utterances at a time .This is having "Listen and Non Listen state". Isolated utterance might be better name of this class.

B. Connected Words

Connected word systems (or more correctly 'connected utterances') are similar to isolated words, but allows separate utterances to be 'run-together' with a minimal pause between them.

C. Continuous Speech

Continuous speech recognizers allow users to speak almost naturally, while the computer determines the content. (Basically, it's computer dictation). Recognizers with continuous speech capabilities are some of the most difficult to create because they utilize special methods to determine utterance boundaries.

D. Spontaneous Speech

At a basic level, it can be thought of as speech that is natural sounding and not rehearsed. An ASR system with spontaneous speech ability should be able to handle a variety of natural speech features such as words being run together, "ums" and "ahs", and even slight stutters.

IV. ROLE OF AUTOMATIC SPEECH RECOGNITION (ASR) IN VOICE-SPEECH RECOGNITION

Speech Recognition is a special case of pattern recognition. There are two phase in supervised pattern recognition, viz., Training and Testing. The process of extraction of features relevant for classification is common in both phases. During the training phase, the parameters of the classification model are estimated using a large number of class examples (Training Data) During the testing or recognition phase, the feature of test pattern (test speech data) is matched with the trained model of each and every class. The test pattern is declared to belong to that whose model matches the test pattern best.

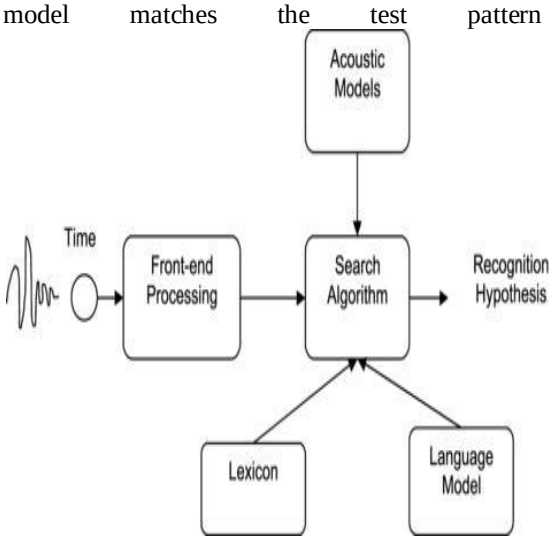


Fig 1.2, Basic model of Automotive Speech Recognition [17]

V. SPEECH RECOGNITION TECHNIQUES

The goal of automatic speaker reorganisation is to analyze, extract characterize and recognize information about the speaker identity. The speaker reorganisation system may be viewed as working in a four stages.

A. Analysis

B. Feature extraction

C. Modelling

D. Testing

A. Analysis

Speech data contain different type of information that shows a speaker identity. This includes speaker specific information due to vocal tract, excitation source and behaviour feature. The information about the behaviour feature also embedded in signal and that can be used for speaker recognition. The speech analysis stage deals with stage with suitable frame size for segmenting speech signal for further analysis and extracting. The speech analysis technique done with following three techniques.

B. Feature Extraction

The speech feature extraction in a categorization problem is about reducing the dimensionality of the input vector while maintaining the discriminating power of the signal. As we know from fundamental formation of speaker identification and verification system, that the number of training and test vector needed for the classification problem grows with the dimension of the given input so we need feature extraction of speech signal.

C. Modelling

The objective of modelling technique is to generate speaker models using speaker specific feature vector. The speaker modelling technique divided into two classification speaker recognition and speaker identification. The speaker identification technique automatically identify who is speaking on basis of individual information integrated in speech signal The speaker reorganisation is also divided into two parts that means speaker dependant and speaker independent. In the speaker independent mode of the speech reorganisation the computer should ignore the speaker specific characteristics of the speech signal and extract the intended message .on the other hand in case of speaker reorganisation machine should extract speaker characteristics in the acoustic signal The main aim of speaker identification is comparing a speech signal from an unknown speaker to a database of known speaker .The system can recognize the speaker, which has been trained with a number of speakers. Speaker recognition can also be divided into two methods, text- dependent and text independent methods. In text dependent method the speaker say key words or sentences having the same text for both training and recognition trials.

VI. SPEECH SYNTHESIS (TEXT-TO-SPEECH)

Speech synthesis is the reverse process to the recognition.The advances in this area improves the computers usability for visually impaired people.

TEXT-TO-PHONE ME CONVERSION: Once the synthesis processor has determined the set of words to be spoken, it must derive pronunciations for each word. Word Pronunciations may be conveniently described as sequences of phonemes, which are units of sound in a language that serve to distinguish one word from another.

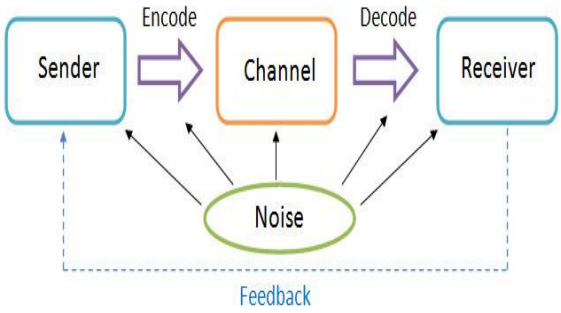


Fig 1.3: Defining the communication between sender and receiver, [18]

VII.THE TECHNIQUE

A. VOICE ENGINE

Software is developed for training and testing speech interface. As a sample application, the machine is trained for numbers (0-9), and some mathematical operators. The input numbers and operators are provided to machine through microphones in the form of wave files Features are extracted from these speech signals and passed to parametric forms for further processing. Extracted parameters are sent to training unit. Total 25 samples are collected for training from 5 different age-group users (male and females), five attempts from each user for every word. The generated results are outputted through speaker.

VIII. ADVERSE CONDITIONS IN SPEECH RECOGNITION

A. Noise

We use the noise free environment to train and test we get, about 80% accuracy. But if the room is noisy either in training phase or in testing phase accuracy is reduces to around 60%.

B. Distortion

To implement this we do not require any special hardware other than the computer machine, a microphone, speakers or headphones with microphone. If these attachments are not installed and configure properly we get distorted input signals, which reduces the accuracy.

C. Articulation Effects

Many factors affect the manner of speaking of each individual, like the distance f microphones from the user

and its position, also speech added with psychological effect while providing input, these effects the accuracy.

IX. TECHNIQUES OF SPEECH RECOGNITION

A. The Fourier Transform

Fourier's Theorem essentially states that the frequency content of any signal can be described as the sum of a specific set of sine waves. The sine wave is the only pure frequency and any distortion of this shape represents harmonics of some fundamental frequency. Thus any wave, no matter how oddly shaped, can be broken down into its component sine wave. The Fourier transform is one of the most commonly used methods of signal analysis. It is simply a mathematical transformation that changes a signal from a time domain representation to a frequency domain representation thereby allowing one to observe and analyze its frequency content. Plotting a Fourier transform gives us a visual representation of the relative proportion of different frequencies in an input signal.

B. Phase Response

Ideally, a filter should have a"linear" phase response. This means that there is a constant time delay difference from the input for all input frequencies. If the phase response is not linear, then different frequencies would be delayed by different amounts. For example: when opera music is put through a filter, a cymbal crash might be heard over the singer's voice instead of after.

C. Sampling

Sampling is the process of taking a continuous time signal and representing it by a series of discrete data points. Any (band limited) signal can be represented in this way as long as the samples are equally spaced and are close enough together in time. Sampling theory makes our life easier by efficiently converting a signal from the analog world to the digital world and back again to the virtually world and met them again.

X. METHODS OF FILTERING SPEECH

A. FIR Filters

In the moving average FIR filter, the values that multiply the input values xn−1 etc, are all the same. That is the coefficients of the filter are all the same.

B. IIR Filters

Recursive digital filter can be designed in which the output of the filter depends both on current and previous inputs as well as previous outputs. For such filters, the impulse response has infinite duration and they are called Infinite Impulse Response (IIR) filters.

C. IIR Impulse Response

The impulse response for the system defined through the difference equation below

$$Y_n = 1/2[\, Y_n - 1 + X_n] \qquad (1)$$

Put $X_n = \delta_n$ and then

$$Y_n = 1/2[Y_n - 1 + X_n]$$

$$H_0 = 0 + 1/2 \times 1 = 1/2$$

$$H_1 = 1/2 \times 1/2 + 0 = 1/4$$

$$H_2 = 1/2 \times 1/4 + 0 = 1/8$$

$$H_3 = 1/2 \times 1/8 + 0 = 1/16$$

$$H_4 = 1/2 \times 1/16 + 0 = 1/32$$

$$H_5 = 1/2 \times 1/32 = 1/64$$

$$H_n = 1/2, 1/4, 1/8, 1/16, 1/32.1/64, ...$$

XI. APPLICATIONS OF SPEECH RECOGNITION

*A. Isolated word recognition***:**

The system was capable of recognizing a single word command (from a small vocabulary of single word commmands.

B. Connected word recognition:

This technology opened up a class of applications based on recognizing digit strings and alphanumeric strings

C. Continuous or fluent speech recognition

D. Speech understanding systems (so-called unconstrained dialogue systems):

They are capable of determining the underlying message embedded within the speech, rather than just recognizing the spoken words.

E. Spontaneous conversation:

These systems which are able to both recognize the Spoken material accurately and understand the meaning of the spoken material.

XII. CONCLUSION

In the present paper the technique developed in each stage of speech recognition system has been discussed also presented the list of technique with their properties for Feature extraction. The filtering methods have been discussed meticulously which is an important aspect of digital signal processing .The present paper attempts to

provide a comprehensive survey of research on speech recognition.

REFERENCES

[1.] Lawerence R.Rabiner Perceptual linear predictive (PLP) analysis of speech. Journal of the Acoustical Society of America, 87:1738-1752, 1990.

[2.] Yuan Meng "Multiband-excitation vocoder" IEEE Trans. Acoust., Speech, Signal Processing, ASSP-36(2) pp.236-243

[3.] Tez Yoneticis, and S. Balashek, "Automatic recognition of spoken digits," J. Acoust. Soc. Amer., vol. 24, no. 6, pp. 627–642, 1952

[4.] Dimitrios S.Koliousis, and G. E. Hinton, "Phone recognition with the mean-covariance restricted Boltzmann machine," in Advances in Neural Information Processing 23. Cambridge, MA: MIT Press, 2010.

[5.] M.A.Anusuya Signal Processing and Linear Systems. Oxford University Press, 2002. ISBN 0195219171.

[6.] Mehryar Mohri Discrete-time signals processing (2nd Ed.). Prentice Hall, 1999. ISBN 0137549202.

[7.] Nelson Morgan, Hermann Ney, and A. Eiden. Language-Model Look-Ahead for Large Vocabulary-laree Speech Recognition. In Proceedings of the International Conference on Spoken Language Pro-cessing (ICSLP'96), pages 2095–2098. University of Delaware and Alfred I. DuPont Institute, 1996.

[8.] Fernando Pereira and Michael Riley. Finite State Language Processing, chapter Speech Recognition by Composition of Weighted Finite Automata, the MIT press 1997

[9.] Richard Master, Acoustical and Environmental Robustness in Automatic Speech Recognition , Kluwer Academic Publish- ers, Boston, MA, 1993.

[10.] Joris Pelemans, Alleva, F., Hon, H., Hwang, M., Lee, K., and Rosenfeld, R., "The SPHINX-II Speech Recognition Sys- tem: An Overview", Computer Speech and Language, 2:137- 148, 1993.

[11.] M. van Gompel, "CLAM: Computational Linguistics Applica- tion Mediator. Documentation.ILKTechnicalReport1202",htt://ilk.uvt .nl/downloads/pub/papers/ilk.1202.pdf, 2012.

[12.] K. Demuynck, A. Puurula, D. Van Compernolle and P. Wambacq, "The ESAT 2008 system for N-Best Dutch speech recognition benchmark", in Proc. ASRU, 2009, pp. 339–343.

[13.] K. Demuynck, T. Laureys and S. Gillis, "Automatic generation of phonetic transcriptions for large speech corpora", in Proc. ICSLP, 2002, vol. I, pp. 333–336.

[14.] V. Steinbiss, B.-H. Tran and H. Ney, "Improvements in beam search", in Proc. ICSLP, 1994, pp. 2143–2146.

[15.] R. Fielding, "Architectural Styles and the Design of Network- based Software Architectures", Ph.D. thesis, University of Cali- fornia, Irvine, 2000.

[16.] K. Eneman, J. Duchateau, M. Moonen, D. Van Compernolle and H. Van hamme, "Assessment of dereverberation algorithms for large vocabulary speech recognition systems", in Proc. ECSCT, 2003, pp. 2689–2692. [11] M. Van Segbroeck and H. Van hamme, "Advances in missing.

[17.] http://masters.donntu.edu.ua/2008/fvti/verenich/library /th_eng.htm

[18.] L ink.springer.com/article/10.1007%2Fs10772-008-9009-1

[19.] http://www.mau.com/safety-blog/bid/77358/Safety-News-Update-Safety-NOT-Lost-in-Translatio

[20.] Alan V. Oppenheim, A.S. Willsky, and I. Young. Signals and Systems. Englewood Cliffs, NJ: Prentice - Hall, 2000

Contrast Stretching and its various techniques - A Review

Navneet Kaur
Department of Computer Science and Technology
Amritsar College of Engineering and Technology
Navneet.kaur634@gmail.com

Aarti
Department of Computer Science and Technology
Amritsar College of Engineering and Technology
Aarti.acet@yahoo.com

***Abstract*— *In this paper, we will present different techniques for contrast stretching. Contrast stretching is used to enhance the images using different techniques. It improves the quality of images. Various contrast stretching techniques which are local contrast stretching, global contrast stretching, partial contrast stretching, bright and dark contrast stretching. This paper involves the complete study of contrast stretching techniques used on different images. Partial contrast stretching is one of the best techniques. It is used to increase the contrast level and brightness level of the images and it is based on the original brightness and contrast level of images.*

Keywords*— *Image enhancement, Contrast stretching, Bright and dark stretching, local and global stretching, partial stretching.

I. INTRODUCTION

Image Enhancement is the technique that is used to improve the visual appearance of an image. The image enhancement is that technique which improves the interpretability or perception of information for human viewers in images. It also improves the image quality so that the resultant picture is better than the original picture. Image enhancement (IE) remove, blur and noise, increasing contrast and reveling details are the examples of the enhancement operations. Existing Techniques of Image Enhancement:

a) Interpolation: Interpolation is an image Enhancement technique which is used for image scaling in astronomy geosciences studies, facial reconstruction and geographical information systems (R). It is used to produce new resolution enhanced and enhanced or shaper version of an image.

b) Histogram Equalization: Histogram Equalization is another technique of image enhancement Histogram Equalization is the point operation that maps the input images to the output images. The main objective of Histogram Equalization is to standardize the intensities that are from unequal level intensities to the equal level intensities to the equal level intensities [8]. This technique usually increases the global contrast of the images. This technique can lead to the better views of medical images like bone structure in X-ray image.

c) Log Transformations: Log Transformation is the technique to improve the images. It maps a narrow range of low input grey level values into a wider range of output values.

d) Contract stretching – Contrast consists to the difference between the intensity of two adjacent pixels in a picture. Low contrast images emerged from non-uniform lighting conditions, nonlinearity or small dynamic range of the imaging sensor [8]. It is the technique of Image enhancement which attempts to improve the contrast in an image by stretching the range of the intensity values.

II. LITERATURE SURVEY

This section presents related literature concerning contrast stretching and its different techniques. Dah-Chung Chang and Wen-Rong Wu, Member (1998) [1] "Image Contrast Enhancement Based on a Histogram Transformation of Local Standard Deviation" In this paper, we present a new ACE algorithm that eliminates these problems. First, a mathematical model for the LSD distribution is proposed by extending Hunt's image model. Then, the CG is formulated as a function of the LSD. The function, which is nonlinear, is determined by the transformation between the LSD histogram and a desired LSD distribution. Using our formulation, it can be shown that conventional ACE's use linear functions to compute the new CG's.

Prasad Nagelli, C. Lokanath Reddy and B.T.R. Naresh Reddy (2014) [2] "Blurred Image Enhancement Using Contrast Stretching, Local Edge Detection and Blind Deconvolution" In this paper contrast stretching is used for obtaining deblurred image. In the proposed method local edge detection is applied on original as well as contrast stretched image. The set of edges obtained from both the images are fussed in order to get sharper edges. The original image and contrast stretched image is converted into gray scale image from RGB image before applying local edge detection to avoid detection of false edges.

Jaspreet Kaur, Amita Choudhary (2012) [3] worked on "Comparison of Several Contrast Stretching Techniques on Acute Leukemia Images". In this paper, several contrast enhancement techniques such as local contrast stretching, global contrast stretching, partial contrast stretching, bright and dark contrast stretching techniques are applied on the leukemia images. The comparison for all the proposed image enhancement techniques was carried out to find the best technique to enhance the acute leukemia images. The presented contrast

enhancement techniques in this paper are effective in enhancing the contrast of leukemia images. From those five techniques, partial contrast gives the best result and hopefully could give extra information for nucleus and cytoplasm of acute leukemia images.

N.R.Mokhtar et al.(2009) [4] proposed "Image Enhancement Techniques Using Local, Global, Bright, Dark and Partial Contrast Stretching for Acute Leukemia Images". In this paper several contrast enhancement techniques which are local contrast stretching, global contrast stretching, partial contrast stretching, bright and dark contrast stretching. All techniques are applied on the leukemia images. The comparison for all the proposed image enhancement techniques was carried out to find the best technique to enhance the acute leukemia images. The results show that the partial contrast stretching is the best technique that helps to improve the image quality.

Aditi Majumder, Sandy Irani [5] proposed "Contrast Enhancement of Images using Human Contrast Sensitivity". In this paper, Suprathreshold human contrast sensitivity function is used to achieve contrast enhancement of images. Greedy algorithm is used in this technique. In this paper, this fact is applied very effectively to design a contrast enhancement method for images that improves the local image contrast by controlling the local image gradient.

Sanjeev Kumar, Dr.Vijay Dhir, Sourabh Mehra (2014) [6] worked on **"**Analysis & Implementation of Contrast Enhancement Techniques Using Medical Images". In this paper, Contrast stretching techniques are first implemented in gray scale and then extended to color images by individually enhancing the color components. This paper deals with contrast enhancement of x-ray images and presents here a new approach for contrast enhancement. Comparatively analysis of proposed technique against the major contrast enhancement technique has been performed.

Raja Rajeswari.V,N. Ramesh (2013) [7] "Contrast Stretching Enhancement Techniques For Acute Leukemia Images" In this paper the presented contrast enhancement techniques are effective in enhancing the contrast of leukemia images. From those 5 techniques, in local contrast stretching, features of leukemia cells can be easily seen and nucleus and cytoplasm of immature cell becomes clearer. Bright contrast stretching extracts color of cytoplasm is enhanced and shape of cytoplasm can be easily seen. In dark contrast stretching nucleus becomes clearer. Partial contrast stretching is suitable for all different types of images. Nucleus, cytoplasm and background regions can be seen clearly. Partial contrast gives the best result and hopefully could give extra information for nucleus and cytoplasm of acute leukemia images.

Gabriel Babatunde Iwasokunl and Oluwole Charles Akinyokun (2014) [8] "Image Enhancement Methods: A Review" Image processing is faced with a number of challenges ranging from unequal resolutions, format variations, non uniform illuminations, distortions and noise. It is also affected by Orientation and contrast differences. In view of these challenges, most digital image processing applications or devices employ enhancement procedure prior to the use of the captured image for intended purposes. This paper reports on the review of some of the existing digital image enhancement methods with emphasis on methodologies, strengths, limitations and application areas.

III. CONTRAST STRETCHING AND THIER EXISTING TECHNIQUES

Contract stretching – Contrast stretching is the technique of Image enhancement which attempts to improve the contrast in an image by stretching the range of the intensity values. It changes the range of the digital numbers and distribution that assigned to each pixel in an image. For contrast stretching a new upper and lower pixel value is needed to be specified over which image is to be normalized [2]. Contrast stretching process plays an important role in enhancing the quality and contrast of medical images. This technique is used to expand the range of brightness values in an image. In contrast stretching Contrast is the difference between the intensity of two adjacent pixels in an image. It improves the contrast in an image by stretching its range of intensity values to a desired range. It increases the dynamic range of gray levels to improve the image quality. It also enhances the image by increasing the contrast between the different parts of the actual image. The various techniques of contrast stretching are given below. The original image is consisting of normal image, bright Image and dark image. The image is shown in figure 1. [4]

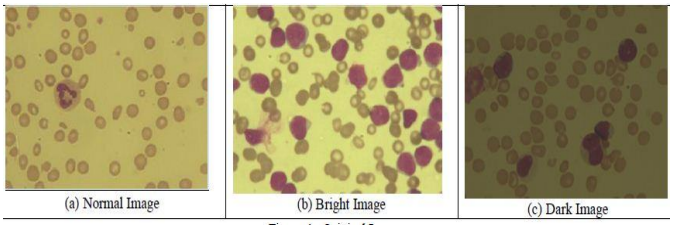


Figure1Original image

The techniques of contrast stretching are as follows:

1) Local Contrast Stretching: - It equalizes the contrast in the image and makes it easier to see the details in the areas that are originally very light or dark. This enhancement method is used for locally adjusting each picture value to improve the quality of structures in the light and dark area of the image at the same time. Local contrast stretching technique is used to improve the appearance of large scale light dark transitions or small scale edges [3]. It is performed by sliding windows known as KERNEL. Local contrast stretching is consisting of all color palate range to determine the minimum and maximum for all RGB color image. The range of each color will be used for contrast stretching process to represent each range of color. This will give each color palate a set of minimum and

maximum values [3]. The image after local contrast stretching is shown in figure2 [4].

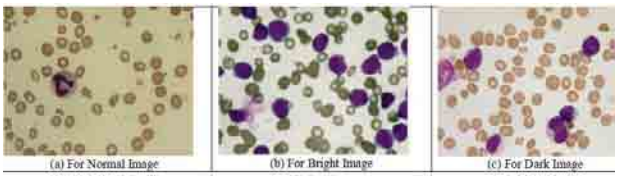


Figure2 Image after local contrast stretching

2) Global Contrast Stretching: Global contrast stretching is consisting of all color palate range at once to determine the minimum and maximum range for all RGB color image. The mixture of RGB color will give only one value for both maximum and minimize for RGB color. This maximum or minimum value will be used for contrast stretching process [3]. The following figure 3 shows the images after global contrast stretching [4].

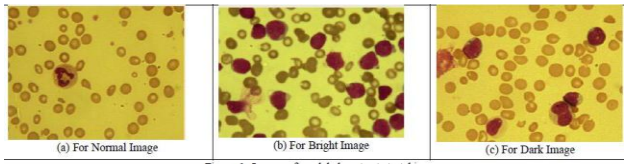


Figure 3 Image after global contrast stretching

3) Partial Contrast Stretching: - It is a linear mapping function which is used to increase the contrast level and brightness level of the image. This technique of contrast stretching is based on Original brightness and contrast level of the images to be adjusted. In this maximum and minimum color levels determines the color range of output image. When the mapping process start, the system will find the range where the majority of the input pixel converge for each color spaces [10]. In the input images RGB model is used to find the range for the red blue and green intensities and then the average is calculated for the upper and lower color values of the three color space. The figure 4 shows the images after partial contrast stretching [4].

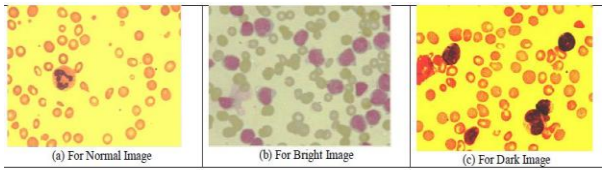


Figure 4 Image after partial contrast stretching

4) Bright Contrast Stretching: - Bright stretching is a process that uses auto scaling method which is a common linear mapping function to enhance the brightness and contrast level of an image. Bright stretching method is based on linear mapping function used for enhancing the brightness and contrast Level of the images [3]. Images after Bright contrast stretching are shown in below figure 5. [4]

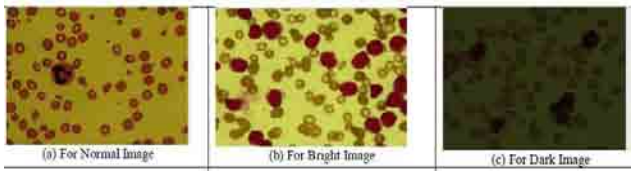


Figure 5 Image after bright contrast stretching

5) Dark Contrast Stretching:-Dark stretching is that technique of contrast stretching which is also known as part of partial contrast stretching. It is the transpose of bright stretching technique. The process tends to stretch the range of image value which is less than the threshold value. On the other side, it compresses the range of image values which are greater than the threshold value. Images after dark contrast stretching are as follows I figure 6. [4]

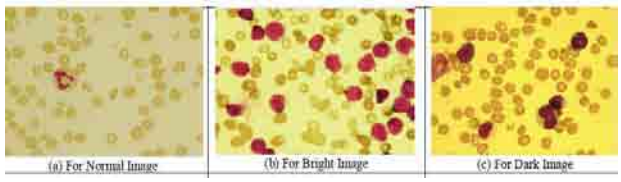


Figure 6 Image after dark contrast stretching

IV. CONCLUSION

The presented contrast stretching techniques are useful to enhance the contrast of the images. Partial contrast stretching is the best technique from all other techniques. This technique is effective in enhancing the contrast of the images. It also gives the finest result as compared to other techniques. These techniques are used in various medical images and we apply these techniques on those images. The partial contrast stretching technique removes the limitations of the other techniques by using better method. From those five techniques, partial contrast gives the best result and hopefully could give extra information for images.

REFERENCES

[1] Dah-Chung Chang* and Wen-Rong Wu"Image Contrast Enhancement Based on a Histogram Transformation of Local Standard Deviation" IEEE TRANSACTIONS ON MEDICAL IMAGING, VOL. 17, NO. 4, AUGUST 1998

[2] Prasad Nagelli1, C.Lokanath Reddy1 and B.T.R. Naresh Reddy1 "Blurred Image Enhancement Using Contrast Stretching, Local Edge Detection and Blind Deconvolution" International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 247-252

[3] Jaspreet Kaur, Amita Choudhary "Comparison of Several Contrast Stretching Techniques on Acute

Leukemia Images" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 1, July 2012

[4] N.R.Mokhtar, Nor Hazlyna Harun, M.Y.Mashor, H.Roseline , Nazahah Mustafa, R.Adollah , H. Adilah, N.F.Mohd Nasir " Image Enhancement Techniques Using Local, Global, Bright, Dark and Partial Contrast Stretching For Acute Leukemia Images" Proceedings of the World Congress on Engineering 2009 Vol I.

[5] Aditi Majumder, Sandy Irani "Contrast Enhancement of Images using Human Contrast Sensitivity" Computer Science Department, University of California, Irvine

[6] Sanjeev Kumar, Dr.Vijay Dhir, Sourabh Mehra **"**Analysis & Implementation of Contrast Enhancement Techniques Using Medical Image",international Journal of Advanced Research in Computer Science and Software Engineering ISSN:2277 128X Volume 4, Issue 5, May 2014

[7] Raja Rajeswari.V,N. Ramesh "Contrast Stretching Enhancement Techniques For Acute Leukemia Images**"** Vol 04, Special Issue01; 2013

[8] Gabriel Babatunde Iwasokunl and Oluwole Charles Akinyokun2 **"**Image Enhancement Methods: A Review", British Journal of Mathematics & Computer Science 4(16): 2251-2277, 2014.

[9] Ms. Seema Rajput, Prof.S.R.Suralkar "Comparative Study of Image Enhancement Technique",IJCSMC, Vol. 2, Issue. 1, January 2013,pg.11-21

[10] M.K. Osman1 M.Y. Mashor 1 H. Jaafar2 "Color Image Enhancement using Bright and Dark Stretching Techniques for Tissue based Tuberculosis Bacilli Detection" Proceedings of the International Conference on Man-Machine Systems (ICoMMS)11 – 13 October 2009.

Privacy Concern of Facebook which is one of the major Tools for Big Data

KavishaDuggal
Assistant Professor(Computer science)
Lovely Professional University
Jalandhar, India
e-mail:Kavisha_duggal@yahoo.com

Gaurav Srivastava
Student (Computer Applications)
Lovely Professional University
Phagwara,India
e-mail: gaurav.shan786@gmail.com

Pawan Singh
Student (Computer Applications)
Lovely Professional University
Phagwara,India
e-mail: Pawansingh4576@gmail.com

Abstract:Today Facebook is the most popular social networking site. It is the easiest and the reasonable way to connect with the people. Facebook stores a large amount of data dynamically, but the main thing to decrypt is the technique and mode used by it. Facebook employs a lot of effort to carry its security, but still problem of hacking prevails. A Facebook Id is basically hacked when it's open with one or more user at a same time. Here a new technique is represented, in which a user is allowed to opteither for single user or multiple user access. In the former session will be locked for that particular IP Address. User cannot open his account until previous account is logged out or session expires. While in the multiple user access the session of that particular IP address is dynamic. User can open his account anywhere and at any time.

Keyword:Big data, Facebook, Security, Life of data, Access mode.

I. Introduction

Now- a-days there are more than 2 billion people on Facebook. Today Facebook is the best medium to communicate. There are more than 1 million likes or updates in one particular day. It is very difficult to manage all such updates, so the Facebook needs more storage to store these updated data also. The data that is stored, they are stored using the concepts of Big data with Hadoop. Big data in real time system with the concept of middleware that take place by message passing and delivery so publishing application and sensors can send data without worrying about where it needs to go and how it needs to get there and Hadoop provides a framework for large scale data of parallel processing by using the distributed file system. The Second problem faced by the Facebook is of Security. It is the most vital elementwhich has to be kept in account. Though, ample security measures are taken but Facebook ids are hacked through phishing.FB stands for two reasons: its success, both in terms of membership and importance of information available on it and the fact that, where other networks catered to new users, the information is uniquely and personally identified[1]. People don't realize that their id's have been hacked or traced by someone else. The most possibilities of hacking are, when an id is opened at a same instance by two users. The confliction of IP address causes the database to be confused so here there is an easy chance for hacker to hack the Facebook id.To reduce these hacking exercise a concept of "Single and multi-access in Facebook", has to be introduced wherein a user can decide that he/she needs one IP address or more than one at a time. In single access a user has only one IP address which is made locked until the session expires. After the session get expirethen the user has to again select that which type of access user wants.

II. Flow Chart for granting the access to the Facebook

This flow chart helps us to understand the internal working of grant permission to the user that which If He wants to use his Facebook with single access and to lock his IP address then he can else he can also use multi access IP address. This helps user to be more flexible with their Facebook accounts.

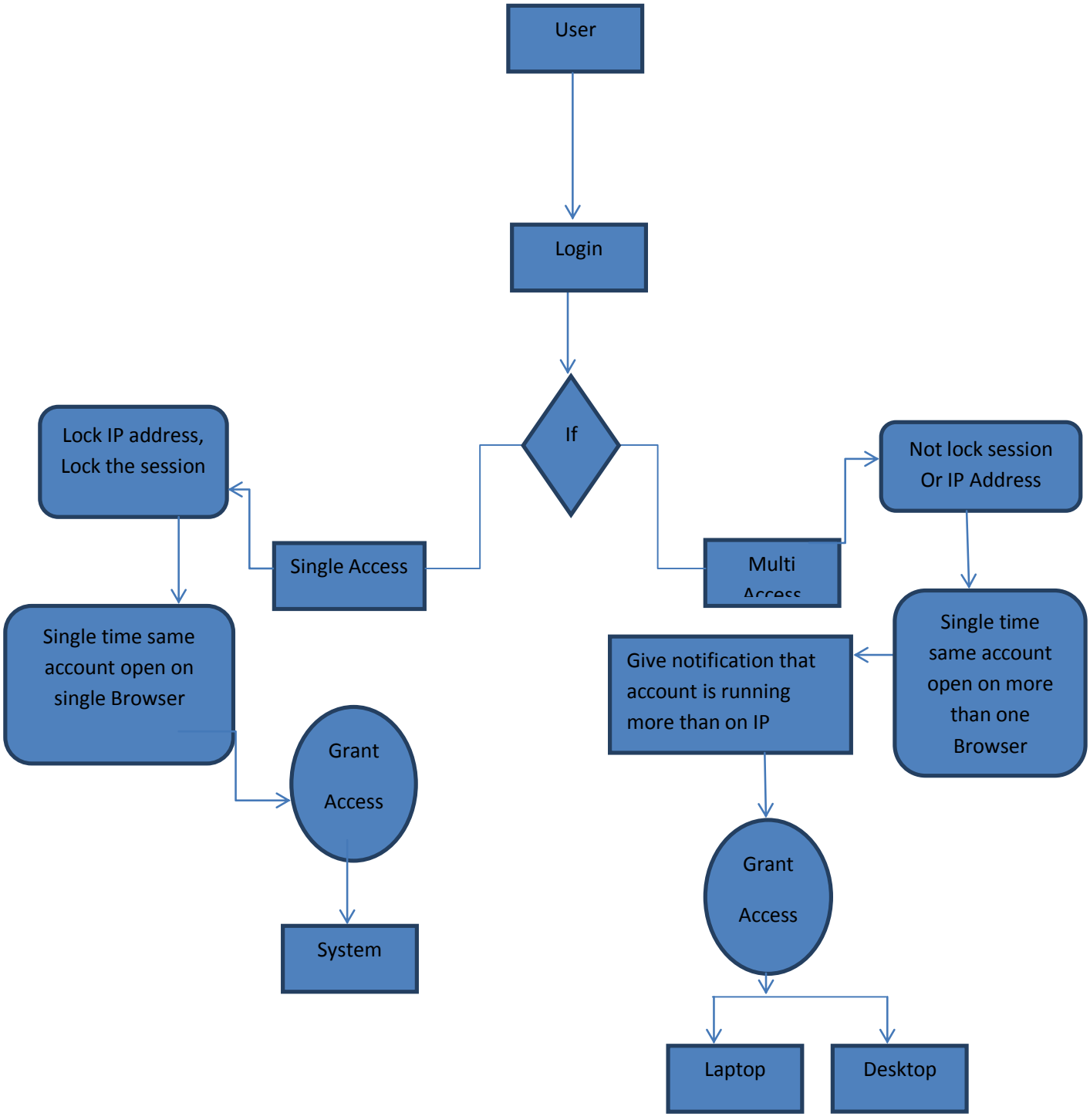
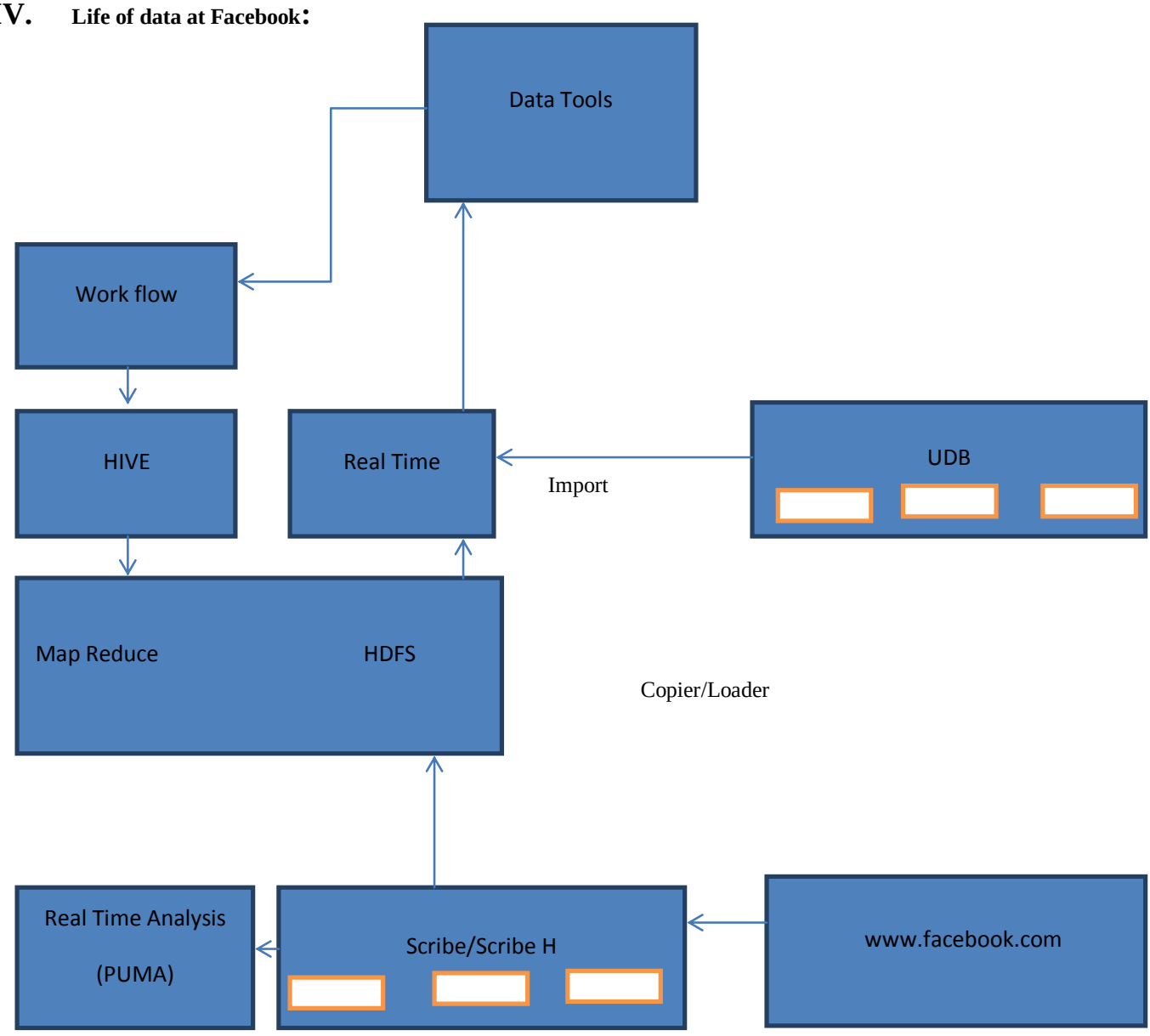


Figure 1:Selection of access (Multi or Single).

III. Methodology :

Inthis terminology the user is given a choice to choose between the single access and multiple accesses for its particular ID. When a user will login the tab for single access and multiple access will be provided and user can select one option according to his requirement. Today it, is necessary to give flexibility to the user, because user feel more comfortable with more security. So, this methodology helps the user—whenuser goes for single access then his Web IP address lock for the particular session, if anybody wants to access the same account from some another place then it will notify that the account it is already in use. It will only give authorization at another place only when he the particular account is being logged out. So user felt more relax and didn't bother about his account. But if the user wants that he uses his account on system as well as mobile then the its web IP address session will not lock and provide the notification that your account is running more than one browser and there should not be any particular (slot) session for that system he can easily use it .

IV. Life of data at Facebook:



Here when the user login his account then his data is scribe (scribe then its go real time analysis) but if scribe H(then go for HDFS)Hadoop distributed File system.[3] HDFS is designed to fault tolerant to run on the commodity hardware.The main objective of the HDFS is to store data reliable even at the time of the failure, the failure occurred and it's known as "Name Node failure". It is a failure of single point in HDFS and Data Node store the data in HFMS. After that the data is mapped, means its check the size of the data that how much big the data is .After that access become faster because the data is transfer to the data tool (provide a debug , maintain ,refactor build of data) .

V. Big Data Role:

Big data play a very important role in that field where the data is very-very big and anonyms. In Facebook there are 3.5 billion of content and 500+ terabyte of data access every day .Every day there are 2.7 billion of likes and 300 billion likes in every 30 minute. Its roughly take 150 terabyte of space [8].
More things about the storing of data in face book:

2.5B content item shared.
2.7B likes.
300M-photos Uploaded.
100+PB disk in Single HDFS cluster.
105 TB data scanned via Hive (30 min)
70,000 queries executed.
500+TB new data ingested [8].
Big data mainly concern three things that are volume, variety and velocity of structured and unstructured data for pouring the data through networks into processors and storage device.

Here **volume** (petabytes, Exabyte, and terabytes) stand for increasing the amount of data-which is created by machine and human, for future use it store all the information and secure it for further access. Now the term is **variety** of data means increasing the number of data types that need to be handled through the simple e-mail, credit card data logs record. It includes the sensor and other machine collect information for scientific studies, record of health care etc. The term **velocity** means to speed up high for accessing the data for the end point too source point[7].

VI. Conclusion

Today everybody is more conscious for the security on their account. They were want easy access with high security .Here the chance of hacking is too much less if the person is go for single access, because when single access is selected then only one account is accessible at that time means same account is not open any other place, only then the same account is open when the person is logout, and is the person go for multi access there the at the same single account can be open more than one place. The Big data store the data with the help of Hadoop Distributed System.

VII. Reference:

[1]. Alessandro Acquisti and Ralph Gross, "Imagined Communities Awareness, Information Sharing, and Privacy on the Facebook" Carnegie Mellon University PET 2006.
[2]. Randal E. Bryant, Carnegie Mellon Randy H. Katz, Berkeley Edward D. Lazowska "Big-Data Computing: Creating revolutionary breakthroughs in commerce, science, and society" December 22, 2008.
[3].DhrubaBorthakur "The Hadoop Distributed File System" March 2012.
[4].Ralph Kimball "Data Warehouse in the Era of Big Data Analytics" Kimball University 2009.
[5].Oracle "Big Data For The Enterprise". White paper.
[6]. Global Pulse "Big Data for Development: Challenges & Opportunities" May 2012.
[7].Peter Fingar "Consider Big Data as the Most Important Thing for Business since the Internet" December 2011.
[8].Josh Constine, "How Big Is Facebook's Data? 2.5 Billion Pieces of Content and 500+ Terabytes IngestedEveryDay",http://techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day/.
[9].Jerzy Surma "The Privacy Problem in Big Bata Applications: An Empirical Study on Facebook"Department of Management Systems Warsaw School of Economics Warsaw, Poland.SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013.

Evaluation Of Various Segmentation Techniques For Color Image Processing

Sachindeep Kaur
M.Tech Scholar
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
sachindeep29@gmail.com

Navneet Bawa
Associate Professor
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
bawa.navneet@gmail.com

***Abstract*:- Image segmentation is a very popular method utilized to split an image into numerous segments based upon their illuminate. The image segmentation has plays very crucial role in many vision applications like face detection, object recognition, content-based image retrieval, medical imaging, face recognition etc. This paper has focused on various image segmentation techniques that can be used to divide the image into various regions. The overall goal of this paper is to evaluate the various key features of existing techniques. This paper focuses on various limitations of the existing work. The review shows that the most of the existing methods suffer from over segmentation issue as well as methods may produce poor results when noise is presented in input images.**

Keywords:- Image Segmentation, Regions, Over Segmentation.

1. INTRODUCTION

One of the most significant means of information transmission in these days considered are the images. As a result the image processing is an essential means in a variety of fields like video coding, computer vision and medical imaging. Image processing generally encompasses a huge variety of techniques which are utilized in wide range of applications. A lot of image analysis processes depends on image segmentation. It is a process of partitioning an image into different regions having same features [1] and is often used to extract region of interests. Segmentation forms a set of homogeneous and having an important effect regions, such that the pixels in every partitioned region possess an identical set of properties or attributes. The sets of properties of the image includes gray levels, contrast, spectral values, or texture properties, etc. The result of segmentation is a number of homogeneous regions, each having unique label.

Every segment represents some information to user in the form of color, intensity, or texture. Therefore, it is essential to isolate the boundaries of any image in the form of its segments [2]. This process of segmentation will allocate a single value to each pixel of an image with the aim of making it easy to differentiate among various regions of any image. This differentiation in different segments of image is done on the basis of three properties of image, i.e., texture , color and intensity of that image. The selection of any image segmentation technique is done after observing the problem domain [3].

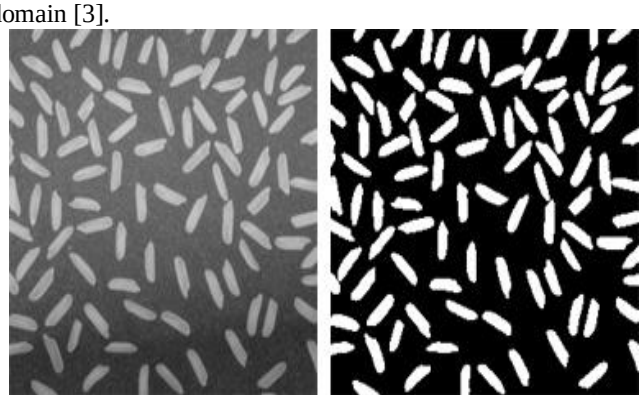


Fig 1: a) Input Image b) Segmented Image

Most of the segmentation algorithms have general steps for image segmentation as in Fig. 3. Noise present in image degrades the segmentation process. The noise must be removed by filtering process. Noises are of various types like salt-pepper noise, Poison noise, etc. Various filters like Mean filter, Median filter, Wiener filter, etc can be used for noise removal .

Fig 2: a) Input Image b) Color Segmented Image

2. IMAGE SEGMENTATION TECHNIQUES

Well-known techniques of image segmentation which are still being utilized by the researchers are line detection, point detection, Edge Detection, Threshold, Histogram processing , Region based methods, and Watershed Transformation. As images are separated into two types on the basis of their color, i.e. gray scale and color images, therefore image segmentation for color images is completely dissimilar to gray scale images, e.g., content based image retrieval[4], [5]. Moreover, which algorithm is robust and works well depends on the type of image [6].

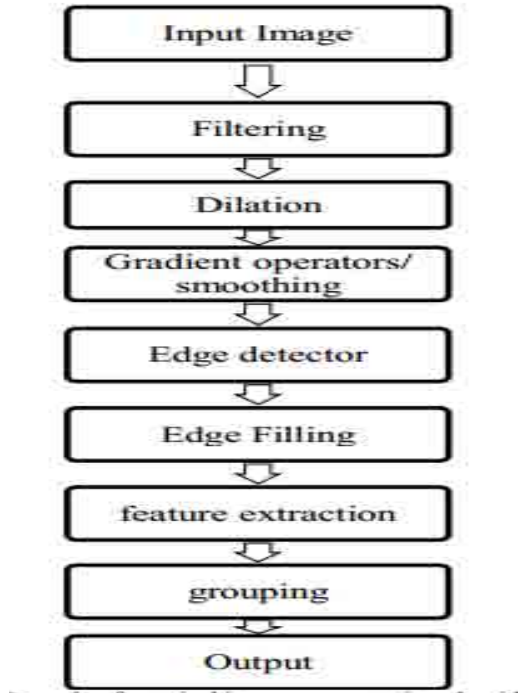


Fig 3: Typical Steps of Segmentation Algorithm

Various Image Segmentation Techniques are:

i. Edge Based Image Segmentation

Edge detection is a basic step for image segmentation process [7]. It divides an image into object and its background. Edge detection divides the image by observing the change in intensity or pixels of an image. Gray histogram and Gradient are two main methods for
edge detection for image segmentation [8]. Several operators are used by edge detection method, i.e., Classical edge detectors, zero crossing, Laplacian of Guassian(LoG)[9], and color edge detectors etc [10].

ii. Region Based Image Segmentation

Region based segmentation is easy as compare to additional methods and also noise resilient. It divides an image into different regions based on pre-defined criteria, i.e., color, intensity, or object. Region based segmentation methods are classified into three main categories, i.e., region growing, region splitting, and region merging [11].

iii. Fuzzy Theory Based Image Segmentation

Fuzzy set theory is utilized so as to analyze images, and make available accurate information from any image. Fuzzification function can be used to remove noise from image as well [12]. A gray-scale image can be transformed easily into a fuzzy image by by means of a fuzzification function. Different morphological operations can be combined with fuzzy method to get better results [13]. Fuzzy k-Means and Fuzzy C-means (FCM) are widely used methods in image processing [14].

iv. Threshold Based Image Segmentation

Histogram thresholding is used to segment the given image; there is certain pre-processing and post-processing techniques required for threshold segmentation [15]. Main thresholding techniques proposed by researchers are Mean method, P-tile method, Histogram dependent technique, Edge Maximization technique, and visual technique.

v. Artificial Neural Network (ANN) Based Image Segmentation

In Artificial Neural Network, each neuron corresponds to the pixel of an image. Image is mapped to the neural network. Image in the form of neural network is taught using training samples, and then connection between neurons, i.e., pixels are found. Then the new images are segmented from the trained image [40]. Some of the neural networks for image segmentation are Hopfield, BPNN, FFNN, MLFF, MLP, SOM, and PCNN. Segmentation of image using neural network is perform in two steps, i.e., pixel classification and edge detection [16].

vi. Partial Differential Equation (PDE) Based Image Segmentation

Partial Differential Equations or PDE models are widely used in image processing, and specially in image segmentation. They use active contour model for segmentation reason. Active Contour model or Snakes transform the segmentation problem

into PDE. Some famous methods of PDE used for image segmentation are Snakes, Level-Set, and Mumford shah method [17].

vii. Fixation-Based Segmentation

Here, bottom-up image segmentation is considered. That is, we ignore (top down) contributions from object recognition in the segmentation process and we expect to segment images without recognizing objects. For a given fixation point, segmenting the region/object containing that point is a two step process: **Cue Processing**: Visual cues such as color, texture, motion and stereo generate a probabilistic boundary edge map wherein the probability of a pixel to be at the boundary of any object in the scene is stored as its intensity, **Segmentation**: For a given fixation point, the optimal closed contour (connected set of boundary edge pixels) around that point in the probabilistic edge map However, the edge map contains both types of edges, namely, boundary (or depth) and internal (or texture/intensity) edges so it is important to be able to differentiate between the boundary edges from the non-boundary (e.g. texture and internal) edges.

Fig. 4: For the two fixations points, indicated by the green crosses, on two different objects , this method segments the corresponding regions enclosing those fixations points in image b.

viii. Graph-Based Image Segmentation

This method segments an image into regions. A predicate is defined for measuring the evidence for a boundary between two regions using a graph-based representation of the image. An efficient segmentation algorithm is then developed based on this predicate, and shown that although this algorithm makes greedy decisions it produces segmentations that satisfy global properties. The algorithm is applied to image segmentation using two different kinds of local neighborhoods in constructing the graph, and illustrate the results with both real and synthetic images [11]. The algorithm runs in time nearly linear in the number of graph edges and is also fast in practice. An important characteristic of the method is its ability to preserve detail in low-variability image regions while ignoring detail in high-variability regions.

Fig 5: Graph-Based Segmentation Method

3. RELATED WORK

Patil R.V. et al. [18] guarantees that if the quantity of groups is assessed in precise way, K-means picture division will give better comes out. They proposed another strategy in view of edge recognition to gauge number of bunches. Stage congruency is utilized to distinguish the edges. At that point these edges are used to discover groups. Limit and Euclidean separation is utilized within request to make groups. K-means is used to discover the last division of picture. MATLAB is utilized to actualize the proposed method. Tests are performed on nine distinctive pictures and results demonstrates that number of groups is exact and ideal.

Fabijańska Anna et al. [19] presented another technique utilizes Variance Filter for edge identification in picture division process. Their technique discovered the edge position utilizing Variance Filter. Sobel Gradient channel with K-means is additionally used to concentrate the edges and contrasted and the proposed strategy. The impact of sifting window estimate on deciding edges is likewise talked about and it is found that if the 9×9 window is utilized to concentrate edges then edge is finished faultlessly match the state of item in the . If there should arise an occurrence of bigger points of interest pictures, a little sifting window is proffered. Results have demonstrated that their proposed procedure beat Sobel Edge Detector.

Khokher Muhammad Rizwan et al. [20] displayed another strategy for picture division utilizing Fluffy Rule based framework and Graph Cuts. Creators have firstly fragmented the ash scale, shade, and composition pictures utilizing Graph Cuts. Weights are appointed to the peculiarities of picture utilizing Fuzzy Rules. Their calculation meets expectations by firstly separating the peculiarities of picture, figure the

constants utilizing fuzzy guidelines, figure the weighted normal of constants to find the closeness grid, parcel the chart utilizing Standardized Graph Cut technique.

Samet Refik et al. [21] proposed another Fuzzy Rule based picture division system to fragment the rock flimsy fragment pictures. They take RGB picture of rock flimsy fragment as info and give portioned mineral picture as yield. Fluffy C Means is likewise connected on rock meager pictures furthermore comes about are analyzed of both systems. Firstly, the client will take example picture from minerals; gimmicks are recognized on the premise of red, green and blue parts of picture. Enrollment capacity is characterized for each part utilizing Fuzzy principles. Every enrollment function represents the shade's conveyance in the picture. Solid and powerless focuses are characterized, though solid focuses are considered as seed focuses and powerless focuses turn into their parts. Results have demonstrated that proposed system is better than FCM algorithm.

Zhang Fengchun et al. [22] presents a variety model utilizing fourth request PDE with second request PDE for finger vein picture de-noising. Midpoint Threshold division strategy is utilized to concentrate the area of engage faultlessly. fourth request PDE has lessened the commotion extremely all things considered, while second request PDE has approximated the limits viably. It could be seen from trials that PSNR estimation of proposed technique is build by 2 db. Technique is contrasted and edge based division calculation and it is discovered that proposed technique has section the true finger vein picture correctly.

4. GAPS IN EARLIER WORK

Following are the various gaps in earlier work on image enhancement techniques.

i. **Isolated regions:** Most of the existing techniques have focused on the complex regions. Not much work done for the images with mixed regions.
ii. **Principal region extraction:** The effect of the regions on the segmentation has been neglected by many researchers.
iii. **Effect of color:** The effect of the color on the segmentation results has also been neglected by many researchers.
iv. **Accuracy and complexity:** The results [base paper] has shown that the FELICM has shown better results when the window size 11*11. But 11*11 mask will result in high computational time complexity. Also result for standard mask size i.e. 3*3 it has shown poor results than PCA algorithm.

5. CONCLUSION & FUTURE SCOPE

The survey has shown that the most of the existing techniques have focused on the complex regions. Therefore not much work has been done for the images with mixed regions. The review has shown that the techniques which are based on fuzzy logic are more effective than the available techniques on image segmentation. The effect of the regions on the segmentation has been neglected by many researchers. The effect of the color on the segmentation results has also been neglected by many researchers. In near future a new integrated variance based PCA and mean-shift based approach to improve the accuracy of the segmentation procedure will be proposed further. The motivation behind the proposed approach is simple and effective.

References

[1] Rafael C. Gonzalez, Richard E. Woods, “Digital Image Processing”, Pearson Education, 2002.
[2] G. Seerha, “Review on recent image segmentation techniques,” International Journal on Computer Science and Engineering, 2009.J. Acharya, S. Gadhiya, and K. Raviya, “Segmentation techniques for image analysis: A review,” International Journal of Computer Science and Management Research, vol. 2, pp. 2278-733, 2013.
[3] M. Yasmin, S. Mohsin, I. Irum, and M. Sharif, "Content based image retrieval by shape, color and relevance feedback," Life Science Journal, vol. 10, 2013.
[4] M. Rehman, M. Iqbal, M. Sharif, and M. Raza, "Content based image retrieval: survey," World Applied Sciences Journal, vol. 19, pp.404-412, 2012.
[5] M. M. S. J. Preetha, L. P. Suresh, and M. Bosco, "Image segmentation using seeded region growing," in Proc. International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 576-583, 2012.
[6] M. Sarif, M. Raza, and S. Mohsin, “Face recognition using edge information and DCT,” Sindh Univ. Res. Jour. (Sci. Ser.), vol. 43, no. 2, pp. 209-214, 2011.
[7] S. Lakshmi and D. V. Sankaranarayanan, “A study of edge detection techniques for segmentation computing approaches,” IJCA Special Issue on “Computer Aided Soft Computing Techniques for Imaging and Biomedical Applications” CASCT, 2010.
[8] M Sharif, S Mohsin, M. Y. Javed, and M. A. Ali , “Single image face recognition using laplacian of gaussian and discrete cosine transforms,” Int. Arab J. Inf. Technol., vol. 9, no. 6, pp. 562-570, 2012.
[9] B. Sumengen and B. Manjunath, “Multi-scale edge detection and image segmentation,” in Proc. European Signal Processing Conference, 2005.
[10] H. G. Kaganami and Z. Beij, “Region based detection versus edge detection,” IEEE Transactions on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1217-1221, 2009.

[11] S. Naz, H. Majeed, and H. Irshad, “Image segmentation using fuzzy clustering: A survey,” in Proc. 6th International Conference on Emerging Technologies, 2010, pp. 181-186.
[12] I. Irum, M. Raza, and M. Sharif, “Morphological techniques for medical images: A review,” Research Journal of Applied Sciences, vol. 4, 2012.
[13] D. Hu and X. Tian, “A multi-directions algorithm for edge detection based on fuzzy mathematical morphology,” in Proc. 16th International Conference on Artificial Reality and Telexistence--Workshops, 2006, pp. 361-364.
[14] P. Singh, “A new approach to image segmentation,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, April 2013.
[15] D. Suganthi and Dr. S. Purushothaman, “MRI segmentation using echo state neural network,” International Journal of Image Processing, vol. 2, no. 1, 2008
[16] X. Jiang, R. Zhang, and S. Nie, “Image segmentation based on PDEs model: A survey”, in Proc. 3rd International Conference on Bioinformatics and Biomedical Engineering, 2009, pp. 1-4.
[17] R. Patil and K. Jondhale, "Edge based technique to estimate number of clusters in k-means color image segmentation," in Proc. 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 117-121, 2010.
[18] A. Fabijanska, "Variance filter for edge detection and edge-based image segmentation," in Proc. International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), pp. 151-154, 2011.
[19] M. R. Khokher, A. Ghafoor, and A. M. Siddiqui, "Image segmentation using fuzzy rule based system and graph cuts," in Proc. 12th International Conference on Control Automation Robotics & Vision (ICARCV), pp. 1148-1153, 2012.
[20] R. Samet, S. E. Amrahov, and A. H. Ziroglu, "Fuzzy rule-based image segmentation technique for rock thin section images," in Proc. 3rd International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 402-406, 2012.
[21] F. Zhang, S. Guo, and X. Qian, "Segmentation for finger vein image based on PDEs denoising," in Proc. 3rd International Conference on Biomedical Engineering and Informatics (BMEI), pp. 531-535, 2010.
[22] J. Xiao, B. Yi, L. Xu, and H. Xie, "An image segmentation algorithm based on level set using discontinue PDE," in Proc. First International Conference on Intelligent Networks and Intelligent Systems, ICINIS'08., pp. 503-506, 2008.

PERFORMANCE EVALUATION OF AUDIO WATERMARKING TECHNIQUES UNDER VARIOUS ATTACKS

Sukhwinder Kaur[1], Vijay Kumar Banga[2]
Department of Electronic and Communication Engineering
Amritsar College of Engineering and Technology
Amritsar, Punjab, India.
malhi_sukh@ymail.com,, vijaykumar.banga@gmail.com

***Abstract* —A digital watermarking is a technique, which is used to defensive digital information like images, videos and audio as it's provides copyright tenure. Digital watermarking emerges as a device for defending the multimedia data from copyright infraction. It is a method for classification multi-media data, for example digital images, text documents, video and audio clips, by trouncing secret information in the data. In this paper various audio watermarking techniques are discussed. Audio watermarking is supplementary difficult than image watermarking due to the lively incomparability of hearing power over the visual field. The embedded watermark is a binary image. The different encryption and decryption techniques are used for hiding the secret image so no one concealing their existence. The embedding of an encryption watermark is distributed uniformly in the areas of low frequencies components is that these components power is elevated sufficient to embed the watermark in such a manner that the watermark is impossible to hear and it should not easy to remove. The various watermark techniques DCT, DWT, LSB have been designed and implemented in MATLAB tool. Various performance metrics has been taken for experimental purpose. It has been found that without attack and with digital delay attack, noisy attack, filter attack DWT using HAAR is quite effective technique over others.**

***Keywords*— watermarking, tenure, digital delay attack, noisy attack, filter attack, DCT, DWT, LSB.**

I. INTRODUCTION

In the recent years with the development of internet technology it's very easy to accessing the unauthorized digital or multimedia information. For the protection of multimedia unauthorized information watermarking technique is used. Watermarking is imperceptible or hidden information in an audio or an image, or any object of value. In this process embedding any information in a signal is very difficult to remove. A watermark is a unique electronic identifier typically used to identify ownership of copyright. Watermarking has become increasingly important to enable copyright defense and tenure verification. Digital watermarking is a technique by which copyright information is embedded into the host signal in a way that the hidden information is imperceptible and robust against intentional and unintentional attacks. In the definition of watermarking digital watermarking is a type of indicator secretly embedded in a noise-tolerant signal such as audio or image data. It is usually used to recognize ownership of the official document of such signal. For the protection of multimedia unauthorized information watermark technique is used. Watermarking is imperceptible or hidden information in an audio or an image, or any object of value. In this process embedding any information in a signal is very difficult to remove. An watermark is a unique electronic identifier typically used to identify ownership of copyright [1].Watermarking has become increasingly important to enable copyright defense and tenure verification. Digital watermarking is a technique by which copyright information is embedded into the host signal in a way that the hidden information is imperceptible and robust against intentional and unintentional attacks.

The Watermark Data usually look up to the data, or message, one desires to embed in an acoustic stream. While an audio watermarking knowledge doesn't essentially necessitate an unbending formation for this information, we originate that in the circumstance of mainly applications; their duration is together predetermined and recognized in advance. The nature of this information is obviously tied to the application. Watermarks can basically transmit distinctive identifiers, which may be related to huge amounts of expressive data through middle databases, or the information they carry can be self-reliant

Audio watermarking technology it is possible to implant supplementary information in an audio track. Audio digital watermarking technology is the new way of audio reproduction, which can pre-implant the particular data as a watermark to the audio signal which exceed the information on behalf of the owner distinctiveness and verify the user's authenticity. The person ear cannot recognize an auditory variation. Audio watermarking technology therefore affords a chance to create

copies of a recording which are imaginary by addressees as indistinguishable to the creative but which may diverge from one an added on the basis of the embedded data. It is very difficult to secure digital information especially the audio and audio watermarking has become a challenge to developers because of the impact it has created in preventing copyrights of the music [2]. It is necessary to maintain the copyright of the digital media, which is one form of logical property. Digital watermarking is a technique by which copyright information is embedded into the host signal in a way that the embedded information is imperceptible, and robust against intentional and unintentional attacks. An audio watermarking technique can be classified into two groups based on the domain of operation. One type is time domain technique and the other is transformation based method. The time domain techniques include methods where the embedding is performed without any transformation. Watermarking is employed on the original samples of the audio signal. Sometimes digital data can be easily used to copy modified and distributed in an illegal way. The copyright protection, intellectual protection & material right protection for authors, owners, buyers & distributers is necessary & the authenticity of content factors to solving problems.

II. COMPONENTS AND FEATURES OF AUDIO WATERMARKING

a) Watermark Data

The Watermark information typically refers to the message, individual needs to embed in an audio stream. Although an audio watermarking technology doesn't essentially have need of an unbending formation for these messages, we originate that in the context for the most part of applications, their duration is together permanent and well-known in advance. The nature of this data is obviously tied to the application. Watermarks are able to basically carry unique identifiers, which may be related to huge amounts of expressive information in the course of middle databases, or the message they transmit can be self-contained.

b) Raw and Effective Data Rate

As for mainly communication systems, an auditory watermarking structure will characteristically contribute part of its unrefined information rate to a variety of error security and modification techniques. The amount and the nature of the select error improvement design are perceptibly functions of the watermark's function. The preference is characteristically resulting as a concession between the preferred Watermark Data Length, the preferred quantity of error security, and the characteristic environment the watermark is predictable to survive. In any case, individual should not be expecting valuable data rates that are much larger than 50 bits per sec or so [16]. This should not approach as a revelation, recalling the similarities linking a transparent auditory watermark and an exceptionally low signal to noise ratio (SNR) communication channel.

C) Watermark Data Length

In the radiance of the characteristic information speed one can expectation for, it is perceptibly in the designer's benefit to describe the direct probable Watermark information that answers his requirements. A shorter watermark will be frequent more regularly contained by the acoustic substance and it will consequently be obtainable within slighter chunks of the watermarked objects [17]. Also, a watermark extractor will have a better chance at getting better a shorter (and more frequently repeated) watermark from greatly contaminated versions of the acoustic objects by exploiting the redundancy of the watermark channel.

III. LITERATURE REVIEW

Chen Xuesong et al. (2008)[8] has proposed that embedding audio watermark into an audio signal was researched in the DWT province and an algorithm of additive audio watermarking based on SNR adaptive to verify a scaling parameter. The intensity of embed watermark based on the Human Audio System is greatest as much as feasible and a balance between robustness and imperceptible. The watermarking signal can be extracted by blind detection in the receiving end.Yan Yang et al. (2009) [9] has proposed the novel technology of embedding image data into the audio signal and additive audio watermarking algorithm based on DCT domain.AC DCT coefficients play different influence in robust and inaudibility. In this proposed method the experimental results demonstrate that the watermark is inaudible and this algorithm is robust to common operation of digital audio signal processing, such as low pass filtering, smoothing, adding noise and so on. Singhal, A et al. (2011) [10] Digital watermarking is the method of embedding copyrighting data into digital media configuration. They are chosen to be imperceptible to the end users. Singhal, A et al. propose a novel acoustic watermarking technique. The algorithm proposed uses multilevel wavelet decomposition, DCT and Singular Value Decomposition (SVD) to accomplish robustness and inaudibility. Mat Kiah et al. (2011) [11] with the increasing practice of digital multimedia, the security of intellectual property rights difficulty has become a very significant issue. Every day, thousands of multimedia documents are organism uploaded and downloaded. Therefore, multimedia copyrights become an imperative issue to keep the intellectual property for the authors of these documents. Mat Kiah et al. has discussed the domains of digital audio steganography, the properties of H.A.S, the audio and the digital demonstration transmission environments, and its software metric. A.R.Elshazly et al.(2012) [12] has discussed to get better protection and robustness of digital audio watermarking

algorithms, based on mean-quantization in DWT domain. The algorithm has a good protection because only the authorized can detect the copyright information embedded to the host audio signal. The watermark can be blindly extracted without understanding of the original signal. To evaluate the performance of the existing audio watermarking method, objective superiority tests as well as bit error rate (BER), normalized cross correlation(NCC), peak-signal to noise ratio (PSNR) are conducted for the watermark and Signal-to-Noise Ratio(SNR) for auditory signals. Simulation outcomes demonstrate to our approach not only makes confident robustness against ordinary attacks, but it also additional improves systemic protection and robustness against malevolent attack. Xinkai Wang et al. (2013) [3] has proposed combining the robustness of vector norm with that of the approximation components after the discrete wavelet transform (DWT), a blind and adaptive audio watermarking algorithm. In order to improve the robustness and imperceptibility, a binary image encrypted by Arnold transform as watermark is embedded in the vector norm of the segmented approximation components, the count of which depends on the size of the watermark image, after DWT of the original audio signal through quantization index modulation (QIM) with an adaptive quantization step selection scheme. Ghobadi et al. (2013) [13] The attention of researchers has audio for the reason that of the audio ability to hide information. There is a number of researches to hide information in audio using watermarking technique. A number of of them tried to make use of the watermark technique to defend the audio file of any tampering. Ghobadi et al. has defined in this paper concern by using contemptible audio watermarking and preserves audio files from any tampering. The technique provides together embedding and extraction solutions. Janardhanan et al. (2013)[14] has discussed digital auditory watermarking involves the method of embedding keen on a host acoustic signal, a perceptually perceptible digital signature carrying a message concerning the host signal. A method of digital audio watermarking using wavelet transform is functional to watermark Indian traditional (music) songs. Investigations were performed by means of Haar, Daubechies and Symlet wavelets intended for time-frequency decomposition of the audio signal in order to implant watermark bits keen on the wavelet coefficients. Simulations are performed through embedding at dissimilar levels of wavelet transform and the outcomes are encouraging with Daubechies wavelet. Robustness of the algorithm was in addition analysed by as well as additive white Gaussian noise, denoising, and resampling. Jani, Yatish Y. et al.(2014)[15] has discussed globalization and internet are the two major reasons for fast dispersion of the multimedia information and appropriate to that tenure and exclusive rights of multimedia files are not generally confined by the providers. Digital watermarking is individual of the top ways for exclusive rights protection. Researchers are trying to formulate new techniques that increase the protection, Robustness and many more effects.

VI.COMPARITATIVE ANALYSIS

In order to do performance evaluation of the different audio watermarking techniques; MATLAB tool issued in this paper. The results are taken by without any attack and also with digital delay attack to check the performance of audio watermarking techniques.

Table 1 Signal To Noise Ratio Evaluation

SOUND NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	57.2218	63.7842	55.8757	81.6948
Sound2	62.6465	72.9561	47.6099	86.3061
Sound3	66.5257	79.1534	58.0646	92.3544
Sound4	57.1016	63.7826	55.1090	83.5334
Sound5	61.4342	61.3489	35.3860	79.8865

Table 1: is showing the quantized analysis of the signal to noise ratio. As signal to noise ratio need to be increase therefore the DWT HAAR is showing the better results than the available methods as signal to noise ratio is less in every case.

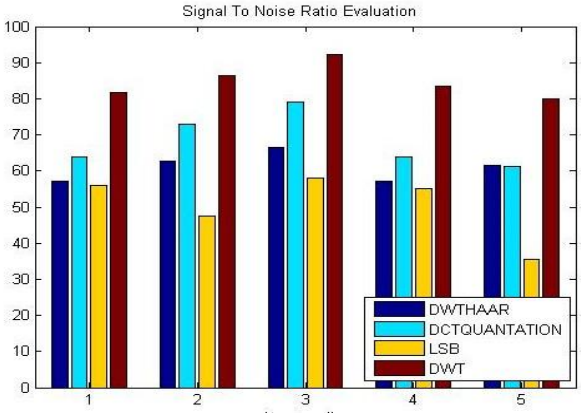


Figure 1: SNR of DWT,LSB, DCT Quantization & DWT HAAR

Figure1. has shown the analysis of the signal to noise ratio of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is increase in SNR value of audio with the use of DWT HAAR over other methods. This increase represents improvement in the signal quality of the audio.

Table 2 Bit Error Rate Evaluation

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.0175	0.0157	0.0179	0.0122
Sound2	0.0160	0.0137	0.0210	0.0116
Sound3	0.0150	0.0126	0.0172	0.0108
Sound4	0.0175	0.0157	0.0181	0.0120
Sound5	0.0163	0.0125	0.0283	0.0114

Table 2: is showing the quantized analysis of the BER. A bit error rate need to be reduced therefore the DWT HAAR is showing the better results than the available methods as bit error rate is more in every case.

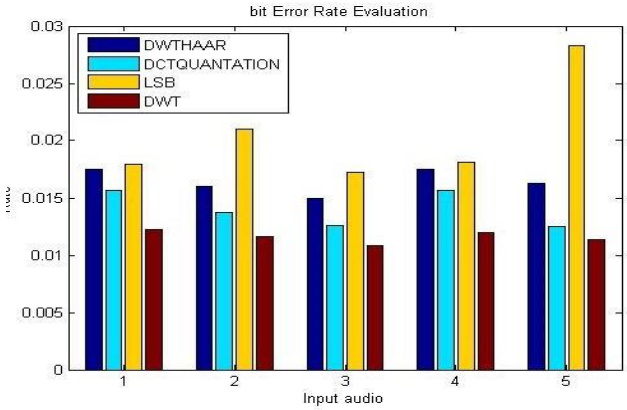


Figure2: BER of DWT , LSB, DCT QUANTIZATION & DWT HAAR

Figure2. has shown the analysis of the BER of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in BER value of audio with the use of HAAR method over other methods. This decrease represents improvement in the signal quality of the audio.

Table 3 Mean Square Error Evaluation

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.4041	0.0892	0.5509	0.0014
Sound2	0.4209	0.0392	0.0113	0.0018
Sound3	0.3721	0.0203	2.6111	0.0019
Sound4	0.4153	0.0892	0.6570	0.0021
Sound5	0.4025	0.0057	0.1016	0.0009

Table 3: is showing the quantized analysis of the MSE. As MSE need to be reduced therefore the DWT HAAR is showing the better results than the available methods MSE is more in every case.

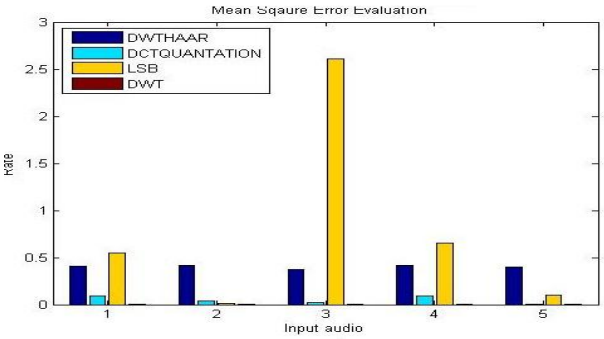


Figure 3: MSE of DWT, LSB, DCT QUANTIZATION & DWT HAAR

Figure3. has shown the analysis of the MSE of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in MSE value of audio with the use of DWT HAAR over other methods. This decrease represents improvement in the objective quality of the audio.

Table 4 Root Mean Square Error Evaluation

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.6357	0.2986	0.7422	0.0380
Sound2	0.6487	0.1980	3.6635	0.0426
Sound3	0.6100	0.1426	1.6159	0.0312
Sound4	0.6444	0.2986	0.8106	0.0307
Sound5	0.0163	0.0758	4.7288	0.0306

Table 4 is showing the comparative analysis of the RMSE. Table has clearly shown that is less in our case therefore the DWT HAAR has shown significant results over the other available methods.

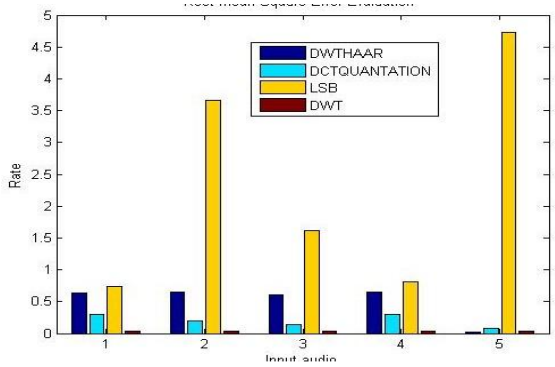


Figure 4: RMSE of DWT, LSB, DCT QUANTIZATION & DWT HAAR

Figure4. has shown the analysis of the RMSE of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in RMSE value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 5. Root Mean Square Error Evaluation with Digital Delay Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.6494	922.7066	0.7423	0.0381
Sound2	0.6594	850.5693	3.6638	0.0018
Sound3	0.6488	1.2383	1.6159	0.0417
Sound4	0.6101	922.7109	0.8106	0.0308
Sound5	0.6483	745.6578	12.7297	0.0334

Table 5 is showing the comparative analysis of the root mean square error with digital delay attack by using different watermarking techniques. Table has clearly shown that is less in our case therefore the DWT HAAR has shown significant results over the other watermarking methods.

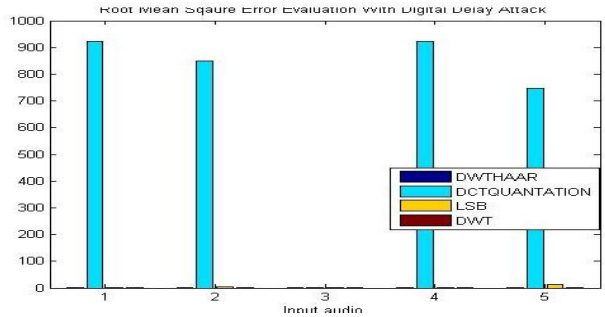


Figure 5: RMSE of DWT, DWT HAAR, LSB, DCT QUANTIZATION With Digital Delay Attack

Figure5. has shown the analysis of the RMSE of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in RMSE value of audio with the use of audio watermarking technique DWT HAAR over other watermarking methods. This decrease represents improvement in the objective quality of the audio signal.

Table 6 Signal To Noise Ratio Evaluation with Digital Delay Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	57.0369	6.0147	55.8755	81.6698
Sound2	62.6462	0.2937	47.6093	86.2877
Sound3	66.5251	0.3766	58.0645	89.8337
Sound4	57.2201	6.0164	55.1089	83.4999
Sound5	61.2468	0.0309	35.3854	87.0153

Table 6 is showing the quantized analysis of the SNR with digital delay attack. As signal to noise ratio need to be increase therefore the DWT HAAR is showing the better results than the available methods as signal to noise ratio is less in every case.

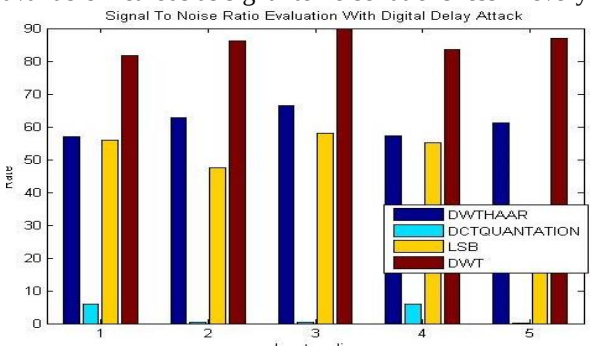


Figure 6: SNR of DWT, DWT HAAR, LSB, DCT QUANTIZATION With Digital Delay Attack Improvement in the objective quality of the audio.

Figure6 has shown the analysis of the SNR of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is increase in SNR value of audio with the use of DWT HAAR over other methods. This increase represents

Table 7: Mean Sqaure Error Rate Evaluation with Digital Delay Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.4217	8.5139	0.5509	0.0015
Sound2	0.4209	7.2347	13.4232	0.0018
Sound3	0.3722	1.5333	58.0645	0.0017
Sound4	0.4041	8.5140	55.1089	9.5170

Sound5	0.4202	5.5601	162.0449	0.0011

Table 7 is showing the quantized analysis of the MSE with digital delay attack. As mean square error need to be reduced therefore the DWT HAAR is showing the better results than the available methods as mean square error is more in every case.

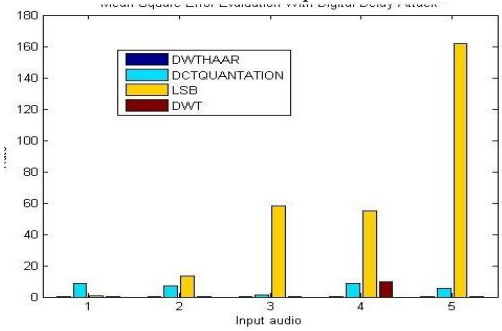


Figure 7: MSE of DWT, DWT HAAR, LSB, DCT QUANTIZATION with Digital Delay Attack

Figure7 has shown the analysis of the MSE of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in MSE value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 8. Bit Error Rate Evaluation With Digital Delay Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.0175	0.1663	0.0179	0.0122
Sound2	0.0160	3.4033	0.0210	0.0116
Sound3	0.0150	2.8556	0.0172	0.0111
Sound4	0.0175	0.1662	0.0181	0.0120
Sound5	0.0163	32.3370	0.0283	0.0115

Table 8 is showing the quantized analysis of the BER with digital delay attack. A bit error rate need to be reduced therefore the DWT HAAR is showing the better results than the available methods as bit error rate is more in every case.

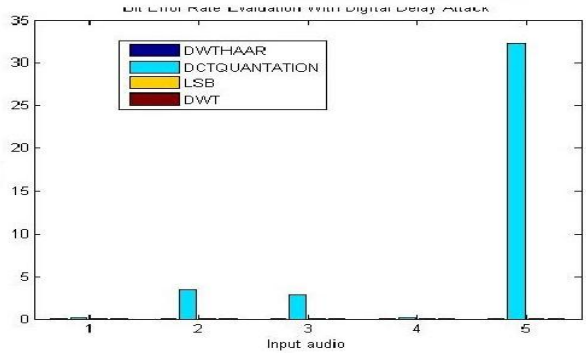


Figure 8: BER of LSB ,DWT ,DWT HAAR & DCT QUANTIZATION with Digital Delay Attack

Figure8. has shown the analysis of the BER of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in BER value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 9 Signal to Noise Ratio Evaluation with Filter Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	56.9040	64.4038	55.8755	73.6335
Sound2	62.5250	72.2536	47.6079	79.9163
Sound3	66.3112	78.4436	58.0414	80.2469
Sound4	57.1498	68.7778	55.0201	71.7454
Sound5	60.9963	75.2691	35.3859	75.1863

Table 9 is showing the quantized analysis of the signal to noise ratio with filter attack. As signal to noise ratio need to be increase therefore the DWT HAAR is showing the better results than the available methods as signal to noise ratio is more in every case.

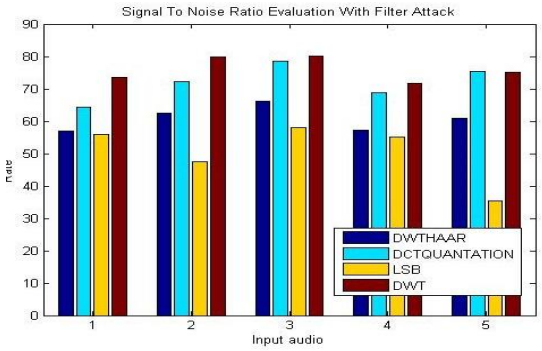


Figure 9: SNR of LSB,DWT ,DWT HAAR & DCT QUANTIZATION With Filter Attack

Figure9 has shown the analysis of the SNR of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is increase in SNR value of audio with the use of DWT HAAR method over other methods. This increase represents improvement in the objective quality of the audio.

Table 10. Bit Error Rate Evaluation With Filter Attack

AUDIO NAMAE	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.0176	0.0155	0.0179	0.0136
Sound2	0.0160	0.0138	0.0210	0.0125
Sound3	0.0151	0.0127	0.0172	0.0125
Sound4	0.0175	0.0145	0.0182	0.0139
Sound5	0.0164	0.0133	0.0283	0.0133

Table 10 is showing the quantized analysis of the BER filter attack. A BER need to be reduced therefore the DWT HAAR is showing the better results than the available methods as BER is more in every case.

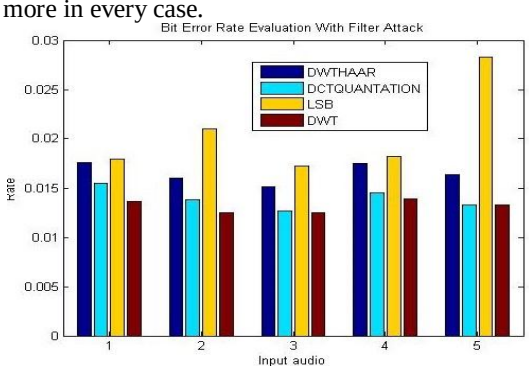


Figure 10: BER of LSB, DWT, DWT HAAR & DCT QUANTIZATION with Filter Attack

Figure 10 has shown the analysis of the BER of different audio signal using audio watermarking by DWT transform(Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in BER value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 11 Mean Sqaure Error Rate Evaluation with Filter Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.4348	0.0773	0.5586	0.0092
Sound2	0.4328	0.0461	13.4275	0.0079
Sound3	0.3910	0.0239	2.6251	0.0158
Sound4	0.4041	0.0282	0.6706	0.0143
Sound5	0.4452	0.0166	16.0449	0.0170

Table 11 is showing the quantized analysis of the MSE with filter attack. As MSE rate need to be reduced therefore the DWT HAAR is showing the better results than the available methods as MSE is high in every case.

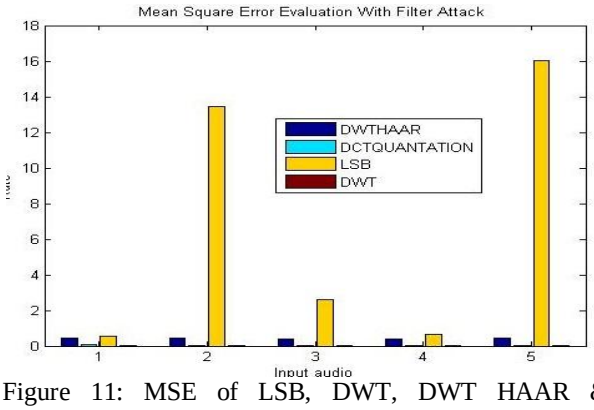


Figure 11: MSE of LSB, DWT, DWT HAAR & DCT QUANTIZATION with Filter Attack

Figure11. has shown the analysis of the MSE of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in MSE value of audio with the use of DWT HAAR method over other methods.

This decrease represents improvement in the objective quality of the audio.

Table 12 Root Mean Square Error Evaluation with Filter Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.6594	0.2781	0.7474	0.0961
Sound2	0.6579	0.2146	0.0210	0.0888
Sound3	0.6253	0.1547	1.6202	0.1257
Sound4	0.6409	0.1680	0.8189	0.1194
Sound5	0.6672	0.1290	2.7290	0.1302

Table 12 is showing the comparative analysis of the RMSE with filter attack. Table has clearly shown that is less in our case therefore the DWT HAAR method has shown significant results over the available methods.

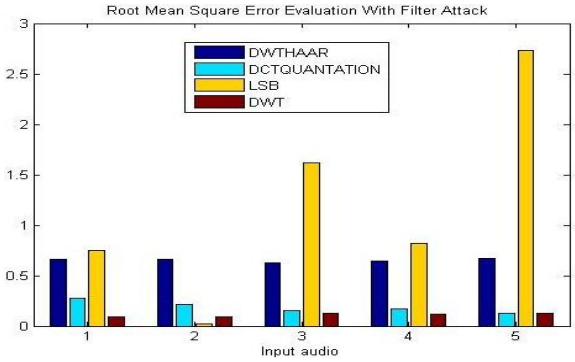


Figure 12: RMSE of HAAR, DWT, LSB& DCT QUANTIZATION with Filter Attack

Figure12 has shown the analysis of the RMSE of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in RMSE value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 13 Root Mean Square Error Evaluation with Noisy Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	212.9727	213.5107	212.3264	212.981
Sound2	196.9163	196.1147	195.4824	196.895
Sound3	290.7558	290.8365	290.5992	290.718
Sound4	212.1959	208.3894	212.5513	212.364
Sound5	209.7479	212.9727	209.1156	209.629

Table 13 is showing the comparative analysis of the RMSE with noisy attack. Table has clearly shown that is less in our case therefore the DWT HAAR has shown significant results over the other methods.

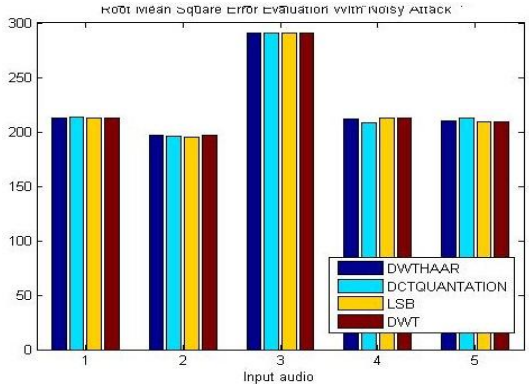


Figure13: RMSE of LSB, DWT, DWT HAAR & DCT QUANTIZATION with Noisy Attack

Figure13 has shown the analysis of the RMSE of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in RMSE value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 14 Signal To Noise Ratio Evaluation with Noisy Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	6.7201	6.6981	6.7465	7.7197
Sound2	13.0022	13.0377	13.0657	14.0082
Sound3	12.1622	12.9598	12.9669	13.9633
Sound4	11.0478	6.7066	6.7356	12.7432
Sound5	6.7502	11.1042	13.0657	14.0526

Table 14 is showing the quantized analysis of the SNR with noisy attack. As signal to noise ratio need to be increase therefore the DWT HAAR is showing the better results than the available methods as SNR is more in every case.

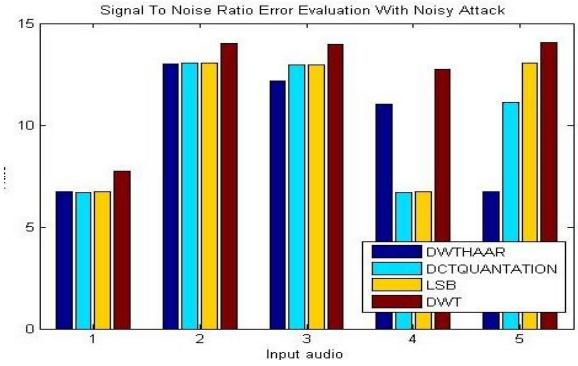


Figure 14: SNR of LSB, DWT, DWT-HAAR & DCT QUANTIZATION with Noisy Attack

Figure14 has shown the analysis of the SIGNAL TO NOISE RATIO of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in MSE value of audio with the use of proposed method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 15 Mean Square Error Rate Evaluation with Noisy Attack

AUDIO NANE	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	4.5357	4.5587	4.5083	3.5361
Sound2	3.8776	3.8461	3.8214	3.8768
Sound3	8.4539	8.4586	8.4448	7.4517
Sound4	4.5027	4.5481	4.5178	3.5099
Sound5	4.3994	4.3426	4.3730	3.3945

Table 15 is showing the quantized analysis of the MEAN SQUARE ERROR with noisy attack. As MSE need to be reduced therefore the DWT HAAR is showing the better results than the available methods as mean square error is more in every case.

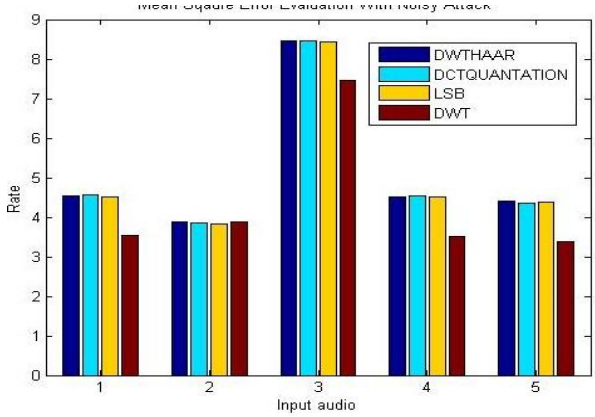


Figure 15: MSE of LSB, DWT,DWT-HAAR & DCT QUANTIZATION with Noisy Attack

Figure15 has shown the analysis of the ROOT MEAN SQUARE ERROR of different audio signal using audio watermarking by DWT transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in RMSE value of audio with the use of proposed method over other methods. This decrease represents improvement in the objective quality of the audio.

Table 16: Bit Error Rate Evaluation With Noisy Attack

AUDIO NAME	DWT	LSB	DCT QUANTI--ZATION	DWT HAAR
Sound1	0.1488	0.1493	0.1482	0.1388
Sound2	0.0769	0.0767	0.0765	0.0569
Sound3	0.0771	0.0772	0.0771	0.0571
Sound4	0.1481	0.1491	0.1485	0.1283
Sound5	0.0905	0.0901	0.0903	0.0805

Table 16 is showing the quantized analysis of the BIT ERROR RATE with noisy attack. A BER need to be reduced therefore the DWT HAAR is showing the better results than the available methods as bit error rate is less in every case.

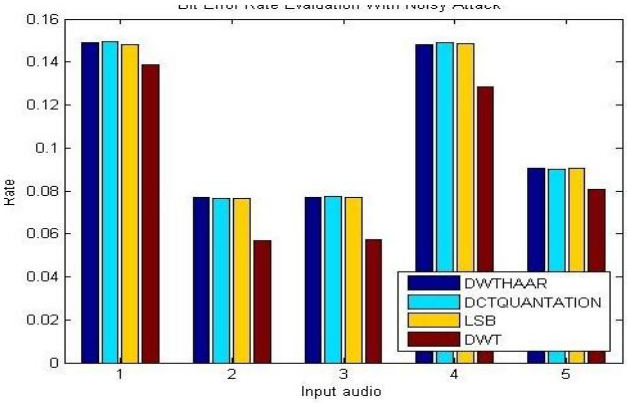


Figure 16: BER of LSB, DWT, DCT QUANTIZATION & DWT HAAR with Noisy Attack

Figure16 has shown the analysis of the BIT ERROR RATE of different audio signal using audio watermarking by DWT transform transform (Brown Color), watermarking by DWT HAAR transform (Blue Color), watermarking by LSB transform (Yellow Color), by watermarking DCT QUANTIZATION (Sky blue Color). It is very clear from the plot that there is decrease in BER value of audio with the use of DWT HAAR method over other methods. This decrease represents improvement in the objective quality of the audio.

VI. CONCLUSION

In this paper various watermarking techniques has been discussed. All these techniques are very important in embedding a signal that applies a digital signature in a form of noise and helps to protect the documents from the various possible attacks. These techniques can also be easily applied to the audio signal for protecting it from the possible attacks and provides the security to the documents. Audio watermarking has found to be most popular technique to secure images when they are containing useful information. One can also use audio watermarking for copy right protection.The various watermark techniques DCT, DWT, LSB have been designed and implemented in MATLAB tool. Various performance metrics has been taken for experimental purpose. It has been found that without attacks digital delay attack DWT using HAAR is quite effective technique over others.
It is concluded that digital watermarking technique is very Impressive for and for protection against attacks.

REFERENCES

[1] Gold, Ben, Nelson Morgan, and Dan Ellis. Speech and audio signal processing: processing and perception of speech and music. John Wiley & Sons, 2011

[2] Gopalan , Kaliappan. "Audio steganography using bit modification." Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on. Vol. 1. IEEE, 2003

[3] Wang, Xinkai, et al. "A norm-space, adaptive, and blind audio watermarking algorithm by discrete wavelet transform." Signal Processing 93.4 (2013): 913-922.

[4] LENG, Xiao-Xu, and Jun XIAO. "A robust zero-watermarking algorithm based on Haar wavelet and normalization." Journal of Graduate University of Chinese Academy of Sciences 3 (2013): 021.

[5] Yin, Chao, and Shujuan Yuan. "A Novel Algorithm for Embedding Watermarks into Audio Signal Based on DCT." Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012. Springer London, 2013.

[6] Wang, Rangding, et al. "A Novel Audio Aggregation Watermarking Algorithm Based on Copyright Protection." International Journal of Computational Intelligence Systems ahead-of-print (2013): 1-13.

[7] Chadha, Ankit, and Neha Satam. "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution." arXiv preprint arXiv:1311.1083 (2013).

[8] LI, Yan-ping, Zhen-min TANG, and Bo QIAN. "Audio watermark algorithm robust to desynchronization based on speech parameter model." Computer Engineering 9 (2008): 066.

[9] Yang, Yan, Rong Huang, and MintaoXu. "A Novel Audio Watermarking Algorithm for Copyright Protection Based on DCT Domain." Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on. Vol. 1. IEEE, 2009

[10] Singhal, Achintya, Anurag Narayan Chaubey, and Chandra Prakash. "Audio watermarking using combination of multilevel wavelet decomposition, DCT and SVD." Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on. IEEE, 2011

[11] .Mat Kiah, M. L., et al. "A review of audio based steganography and digital watermarking." International Journal of Physical Sciences 6.16 (2011): 3837-3850.

[12] Elshazly, A. R., M. M. Fouad, and M. E. Nasr. "Secure and robust high quality DWT domain audio watermarking algorithm with binary image." Computer Engineering & Systems (ICCES), 2012 Seventh International Conference on. IEEE, 2012

[13] Ghobadi, Alireza, et al. "Blind audio watermarking for tamper detection based on LSB." Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013.

[14] Janardhanan, C. M., and C. Sathish Kumar. "Performance Analysis of Discrete Wavelet Transform based Audio

Watermarking on Indian Classical Songs." International Journal of Computer Applications 73 (2013).
[15] .Jani, Yatish Y., Yagnesh J. Parmar, and Chintan J. Kavathiya. "A Review on New Technique for Embedding Image into Audio as a Watermark using DCT." International Journal of Computer Applications 88 (2014).
[16] Rhoads, Geoffrey B., and J. Scott Carr. "Signal processing of audio and video data, including assessment of embedded data." U.S. Patent No. 8,391,545. 5 Mar. 2013.
[17] Brundage, Trent J., EE Ellingson, BT Hannigan. "Digital watermarking apparatus and methods." U.S. Patent No. 7,957,553. 7 Jun. 2011.

Comparative Analysis of Various Text compression Techniques

Vicky Kumar
GIMET
vickykumar0802@gmail.com

Maninder Pal Singh
GIMET
mannisingh2009@gmail.com

Abstract-- This paper comprises different Text compression algorithms of text files: Huffman, Shannon-Fano, Arithmetic, LZ, LZW algorithm techniques. We compare these algorithms on different text files of different sizes in terms of compression scales. The original words in a text file are transformed into codewords having length 2 and 3. The most commonly used words are 2 length codewords and the 3 length codewords for better compression. Thesecodewords are chosen in such a way that the spaces between words in the original text file can be removed altogether with recovering a substantial amount of space.

Keywords- Data compression, Text Compression, Huffman Coding, Shannon-Fano Coding, Arithmetic Coding, LZ Coding, LZW.

I. INTRODUCTION

Text is a significant part of most files that digital technology users create. For example, these files could be: Word or PDF documents, emails, cellphone texts (SMS format) or web pages.

The highestcapacity of storage devices is currently available; Text compression has important applications in the areas of data transmission and data storage because we require easy ways and means to store and transmit different types of data such as text, image, audio, and video, and hence reduce execution time and memory size [1].

The general principle of Text compression algorithms in text files is to transform a string of characters into a new string which contains the same information to transform a string which considerably reduced as measured by scales such as: compression size, compression ratio, processing time or speed, and entropy.

II. COMPRESSION TECHNIQUE

Compression technique are used to reduce the volume of information can be stored into reduce the communication bandwidth required for its transmission over the networks.

Compression is used for different types of data, Example: documents, sound, video. It is either applied to transfer a file into a disk or over a network.To ensure that the file is fit on the storage device, or both. The aim of compression to reduce the quantity of the file size and to keep the quality of the original data.

a) Lossless compression

Lossless compression algorithm is minimize the amount of source Information to be transmitted in such a way that, when the compressed information is decompressed, there is no loss of information. Lossless compression is therefore said to be reversible. [2]

b) Lossy compression

The aim of lossy compression algorithm is normally not to reproduce an exact copy of the source information after decomposition but rather a version of its compression which is perceived by the recipient as a true copy (approx). [2]

Example: Digitized images in audio and video streams. In such cases, the sensitivity of the human eye or ear is seen any fine details that may be missing from the original signal after decompressions are not detectable.

Types of Text Compression Techniques

Lossless – Compressed then Decompressed data is an exact replication.

- WinZip
- General Purpose (HTTP, ASCII, Morse Code)
- Media (TIFF, PNG, FLAC, MPEG-4 (ALS), GIF)
- Very few video codecs are lossless

Lossy – There is some distortion between original and reproduced.

- Images (JPEG)
- Videos (MPEG)
- Audio (MP3)

Lossless Compression Techniques

- RLE (Run Length Encoding)
- Huffman Method
  - Using tables
- Lempel-Ziv
  - Also LZW (Lempel-Ziv Welch)
- DEFLATE
  - Used in PKZIP, GZIP, PNG

III. COMPRESSION ALGORITHMS

i. Huffman Coding

Huffman algorithm is the oldest and most widespread technique for data compression. It was developed by David A. Huffman in 1952 and used in compression of many types of data such as text, image, audio, and video. It is based on building a full binary tree bottom up for the different symbols that are in the original file after calculating the frequency/probability for each symbol and put them in descending order.

The codewords for each symbol from the binary tree, giving shorter code words for symbols with large probabilities and longer code words for symbols with small probabilities.

Huffman algorithm assigns every symbol to a leaf node, Root node and Branch node of a binary code tree. The tree structure results from combining the nodes step-by-step until all of them are embedded in a root tree. The algorithm always combines the two nodes providing the lowest frequency in a bottom up procedure. The new interior nodes having the sum of frequencies of both child nodes. This is also called as Huffman code tree.

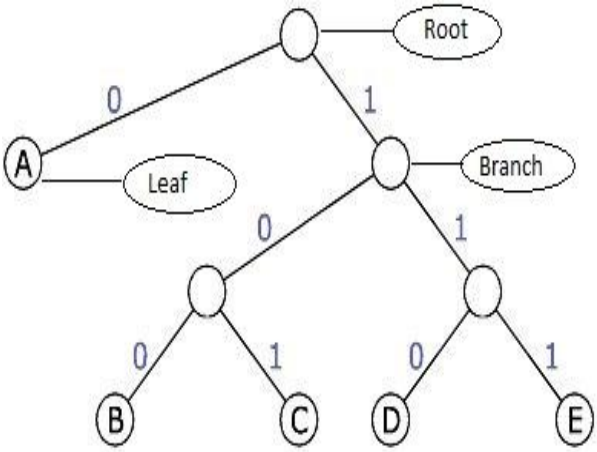


Fig. 2: - Huffman Tree

The branches of the tree represent the binary values 0 and 1 according to the rules for common prefix-free code trees. The path from the root tree to the corresponding leaf node defines the particular code word.

Applications:-

- It is a binary tree.
- Branches assigned value 0 or 1
- Root node – base of the tree
- Branch node – Point at which branch divides
- Leaf node – termination point

Huffman Encoding is of two types: -

a. Static Huffman Coding
b. Dynamic Huffman Coding

a. Static Huffman Coding

- Static Huffman coding assigns variable length codes to symbols based on their frequency of occurrences in the given message. Low frequency symbols are encoded to used many bits, and high frequency symbols are encoded using lesser bits.
- The message is to be transmitted is first analyzed and frequencies of its constituent characters.
- The coding process generates a binary tree, and the Huffman coding tree of the branches labeled with bits (0 and 1).

b. Dynamic Huffman Coding

- Previous method requires both transmitter and the receiver to know the table of codewords relating to the data being transmitted .
- In this method encoder and decoder build the Huffman tree , hence the codeword table dynamically.
- If the character to be transmitted is currently present in the tree its codeword is determined and sent in the normal way.

ii. Shannon-Fano Coding

At about 1960 Claude E. Shannon (MIT) and Robert M. Fano (Bell Laboratories) wasdeveloped bya coding procedure to generate a binary code tree. The procedure evaluates the symbol's probability and assigns code words with a corresponding code length.

Compared to other methods Shannon-Fano coding is easy to implement. In practical operation Shannon-Fano coding is not great importance. This is especially caused by the lower code efficiency in comparison to Huffman coding as demonstrated later.

iii. Arithmetic Coding

In Arithmetic coding optimal compression ratio for a data source is generally described with respect to Claude Shannon's [6] definition of source entropy [5]; a measure of the source information and therefore the average number of bits required to represent it.

The latest invention of arithmetic coding [7] has provided a method which is guaranteed to transmit a message in a number of bits which can be made arbitrarily close to its entropy with respect to the model which is used.

Applications

- More complex than Huffman coding.

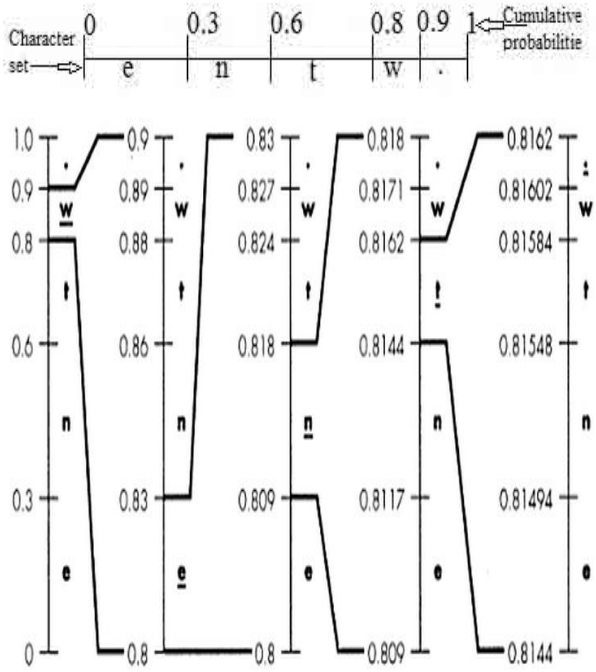
- The first step is to divide the numeric range from 0 to 1 into a number of different characters present in the message to be sent (even termination character) and the size of each segment by the probability of the related characters.
- Hence decoder follows same procedure as that of encoder
- Complete message - fragmented into multiple smaller strings
- Each is encoded separately.
- Resulting set of codewords sent as a block of floating point numbers each in a known format

Example:

Consider the transmission of a message comprising a string of characters with probability of

e=0.3, n=0.3, t=0.2, w=0.1, .=0.1

Sol. We assume that the character string/message to be encoded in the single word "went.".



Hence the codeword for the complete string in any number with in the range:

i.e. 0.81602≤codeword>)0.8162.

iv. Lempel-Ziv Coding (LZ)

A variety of compression methods is based on the fundamental work of Abraham Lempel and Jacob Ziv. Their original algorithms are traditionally denoted as LZ77 and LZ78. A variety of derivates were introduced in the meantime. It is common practice to add the first letter of the person's name that had invented the extended format:

- Lempel-Ziv 77 (LZ77)
- Lempel-Ziv-Storer-Szymanski (LZSS)
- Lempel-Ziv 78 (LZ78)
- Lempel-Ziv-Welch (LZW)

v. Lempel-Ziv-Welsh (LZW)

In 1977, Abraham Lempel and JakobZiv created the first of what we now call the LZ family of substitution compressors. In 1984, while working for Unisys, Terry Welch modified the LZ78 compressor for implementation in high-performance disk controllers. Ziv and Lempel [8] have proposed a coding technique which involves the adaptive matching of variable length strings. The result was the LZW algorithm that is found today. It is a general compression algorithm having a capacity of working in different types of data, creating a table of strings commonly occurring in the data being compressed and replacing the actual data with references into the table [3]. The original Lempel-Ziv approach to data compression was first published in 1977[4]. Terry Welch's refinements to the algorithm were published in 1984[4]. The algorithm is surprisingly simple. In a nutshell, LZW compression replaces strings of characters with single codes. It does not do any analysis of the incoming text; it just adds every new string of characters it sees to a table of strings. Compression occurs when a single code is output instead of a string of characters [4].

The table, a "dictionary" of all the single character with indexes 0...255, is formed during encoding/compression starts and is used in decoding/de-compression. Codes 0-255 refer to individual bytes, while codes 256-4095 refer to substrings [4].

III. COMPARISON OF HUFFMAN CODING AND SHANNON-FANO CODING WITH AN EXAMPLE

Example: - Construct a Shannon-Fano Code & Huffman Code and Compare the results.

$P(x_1) = 0.40$, $P(x_2) = 0.19$, $P(x_3) = 0.16$,

$P(x_4) = 0.15$, $P(x_5) = 0.10$.

1) Shannon-Fano Coding

x_i	$P(x_i)$	Step 1	Step 2	Step3	Code(n_i)
x_1	0.40	0	0		00
x_2	0.19	0	1		01
x_3	0.16	1	0		10
x_4	0.15	1	1	0	110

x_5	0.10	1	1	1	111

Entropy of system, H(X)

$H(X) = \sum_{i=1}^{M} P(x_i).I(x_i)$

Therefore, $I(x_i) = \log_2 \frac{1}{P(x_i)}$ or $-\log_2 P(x_i)$.

$I(x_1) = \log_2 \frac{1}{0.40} = 1.32$

$I(x_2) = \log_2 \frac{1}{0.19} = 2.39$

$I(x_3) = \log_2 \frac{1}{0.16} = 2.64$

$I(x_4) = \log_2 \frac{1}{0.15} = 2.73$

$I(x_5) = \log_2 \frac{1}{0.10} = 3.32$

So, $H(X) = \sum_{i=1}^{5} P(x_i).I(x_i)$

H(X) = 0.40x1.32+0.19x2.39+0.16x2.64+
0.15x2.73+0.10x3.32 = 2.15Bits/message

Length, $L = \sum_{i=1}^{M} P(x_i).n_i$

$L = \sum_{i=1}^{5} P(x_i).n_i$

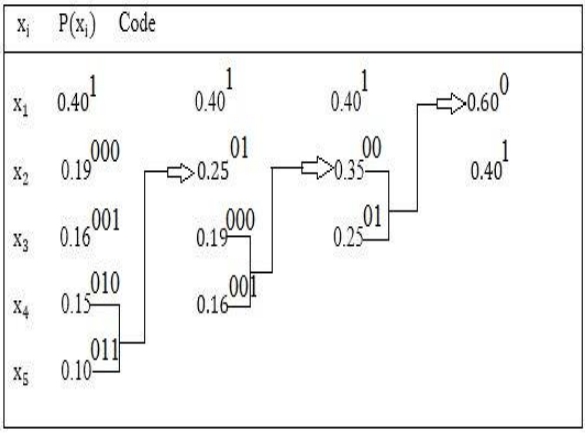
Therefore, L = 0.40x2+0.19x2+0.16x2+
0.15x3+0.10x3 = 2.25 Bits/message

Efficiency, n = H(X)/L

n = 2.15/2.25 = 0.9556 = 95.56%.

Therefore, Shannon-Fano Coding can compressed the data (approx.) 95%.

2) Huffman Coding



x_i	$P(x_i)$	Code(n_i)
x_1	0.40	1
x_2	0.19	000
x_3	0.16	001
x_4	0.15	010
x_5	0.10	011

Entropy of system, H(X)

$H(X) = \sum_{i=1}^{M} P(x_i).I(x_i)$

H(X) = 0.40x1.32+0.19x2.39+0.16x2.64+
0.15x2.73+0.10x3.32 = 2.15 Bits/message

$L = \sum_{i=1}^{M} P(x_i).n_i$

$L = \sum_{i=1}^{5} P(x_i).n_i$

Therefore, L = 0.40x1+0.19x3+0.16x3+
0.15x3+0.10x3 = 2.2 Bits/message

Efficiency, n = H(X)/L

n = 2.15/2.2 = 0.9772 = 97.72%.

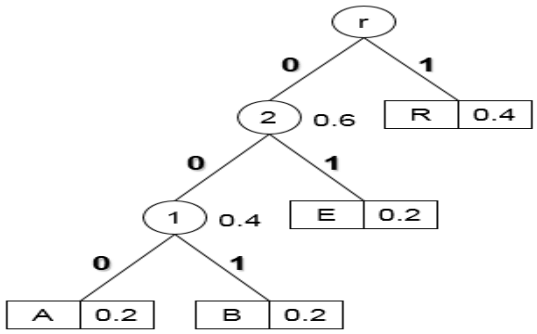
Therefore, Huffman coding can compressed the data (approx.) 97%.

As compare to Shannon-Fano Coding and Huffman Coding, Huffman Coding compresses more reliable than Shannon-Fano Coding.

IV. COMPARISON OF HUFFMAN CODING AND ARITHMETIC CODING WITH AN EXAMPLE

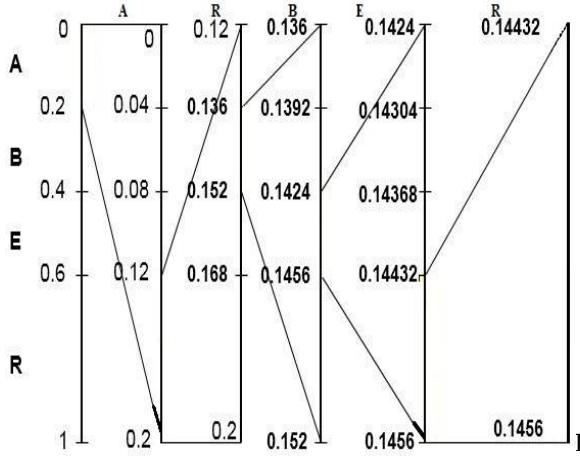
Example: -Consider the string ARBER. The probabilities of symbols A, B, E, and R are:

Symbol	A	B	E	R
Frequency	1	1	1	2
Probability	20%	20%	20%	40%



Symbol	Code
A	000
B	001
E	01

R 1



The final interval for the input string ARBER is [0.14432, 0.1456). The compression ratio of the arithmetic coding for different Text sizes is higher than the Huffman coding. By increasing the text size, the improvement of the compression ratio of the arithmetic coding increases more than the Huffman coding.

V. COMPARISON OF HUFFMAN CODING AND LZW WITH AN EXAMPLE

Example: - The comparison of Huffman vs LZW

No. of Exp.	Original Data Size	Huffman	LZW	LZW based Huffman	Huffman based LZW
01	4.70 MB	2.67 MB	1.87 MB	2.59 MB	1.83 MB
02	2.19 MB	1.20 MB	933 KB	1.24 MB	912 KB
03	26 KB	18.5 KB	12 KB	21.1 KB	11.5 KB
04	71.6 KB	48 KB	21.9 KB	39.1 KB	21 KB
05	2.44 MB	1.40 MB	980 KB	1.32 MB	959 KB
06	4.63 MB	2.61 MB	1.85 MB	2.54 MB	1.82 MB
07	9.53 MB	5.42 MB	3.77 MB	5.30 MB	3.69 MB
08	18.8 MB	10.6 MB	7.51 MB	10.5 MB	7.35 MB
09	7.08 MB	4.02 MB	2.81 MB	3.93 MB	2.75 MB
10	25.9 MB	14.6 MB	10.3 MB	14.4 MB	10.1 MB

In all these cases of compression Huffman based LZW performs well. It compresses a data to almost 38% or less from its original size where the remaining three never gives such better compressed data.

Different standard scales of compression measurement

- Compression size: The size of the new file in bits after compression is complete.
- Compression ratio: The ratio of the compression size in to the original file size expressed as a percentage.
- Processing time or speed in millisecond: The ratio of the time required for compressing the whole file to the number of symbols in the original file expressed as symbol/ millisecond.
- Entropy: The ratio of the compression size to the number of symbols in the original file expressed as bits/symbol.

VI. LATEST TECHNOLOGIES

1) Entropy encoding is a term referring to lossless coding technique that replaces data elements with coded representations. Entropy encoding in combination with the transformation and quantization results in significantly reduced data size. For any conventional multimedia coding, entropy encoding is a bit assigning and lossless module. Based on the available channel band width, the appropriate bit-rate can also be achieved by using recursive property of our proposed encoding algorithm. Here two level of recursion has been considered for the proposed algorithm. The experiments were conducted in various multimedia data such as text, image, audio and video sequences. It is observed that the proposed algorithm outperforms the existing entropy encoding algorithms such as Huffman and arithmetic coding in terms of compressed file size, encoding and decoding time.

2) A new hybrid predictive coding scheme for lossy data compression is introduced and studied here. The proposed technique attempts to improve the compression performance of a conventional adaptive predictive coder through three levels of prediction. The first level estimates and removes a time-varying mean signal. The second level uses DFT and IDFT to estimate and remove the predictable high frequency subband component of the signal, whereas the third level performs the adaptive predictive coding of the polited signal.

VII. CONCLUSION

Compression is a significant technique in the multimedia computing field. This technique can bereduce the size of data and transmitting and storing the reduced data on the Internet and storage devices are faster and cheaper than uncompressed data. In other words, these algorithms are important parts of the multimedia data compression standards. Texts are always compressed with lossless compression algorithms. This is

because of loss in a text will change its original concept. Repeated data is great importans in text compression. If a text has many repeated data, it can be compressed to a high ratio. This is due to the fact that compression algorithms generally eliminate repeated data. For such as real-time applications, Huffman algorithm can be used.

REFERENCES

[1] Elabdalla, A. R. and Irshid, M. I.,"An efficient bitwise Huffman coding technique based on source mapping". Computer and Electrical Engineering 27 (2001) 265 – 272.

[2] Multimedia Communications: Applications, Networks, Protocols and Standards by Fred Halsall.

[3] Michael Heggeseth, Compression Algorithms: Huffman and LZW, CS 372: Data Structures, December 15, 2003.

[4] Mark Nelson, LZW Data Compression, Dr. Dobb's Journal, October 1989.

[5] I.Witten, R. Neal, and J. Cleary, "Arithmetic coding for data compression," Communications of the ACM, vol. 30, no. 6, pp. 520–540, June 1987.

[6] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, July and October, 1948.

[7] R. Pasco, "Source coding algorithms for fast data compression," Ph.D. disiertation, Stanford Univ., Stanford, CA, 1976.

[8] J Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," IEEE Trans. Inform. Theory, vol. IT-24, pp. 530-536, Sept. 1978.

[9] Kumar,A., "Information Technology and Multimedia (ICIM)", pp. 1 – 5, International Conference on 14-16 Nov. 2011.

[10] Bar-Ness, Y."Circuits and Systems", 300-303 vol. 1, IEEE International Symposium on 8-11 May 1989.

Implementing Watermarking Relational Databases Using Genetic Algorithm and Honey Bee Optimization

Er Gagandeep Singh
M.Tech Scholar,
Punjab Technical University
gagandeep.engineer@gmail.com

Er Sandeep Kad
Associate Prof., Dept. of Information Technology
ACET, Amritsar
sandeepkad@acetamritsar.org

Abstract— **The main reason for the development of digital watermarking research is the endeavor for coming up with innovations to protect intellectual properties of the digital world. Digital watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. It may be visible or invisible. Proposed a hybrid model optimization in which the embedding and extracting algorithms of watermarking in discrete wavelet transform are combined with GA-HBO based optimization techniques for watermarking. The proposed technique is implemented over the MATLAB.**

***Index Terms*— Watermarking, Genetic Algorithm, Honey Bee Optimization, DWT, PSNR, MSE.**

1. INTRODUCTION

With the tremendous use of World Wide Web, authors of digital media can easily distribute their works by making them available on Web pages or other public assembly. To overcome the problems of piracy, one method is to embed additional information in terms of image, text, etc and only distribute the media that contains this additional information [1]. This embedded data which is in terms of information about the media, author, copyright or license information is termed as watermark.

Watermark is an open problem that aimed to one goal. This goal is how to insert [error/mark/evidence so on] associated with a secret key known only by the data owner In order to prove the ownership of the data without lossless of its quality. In, general watermark is small, hidden perturbations in the database used as an evidence of its origin. Inserting mark into original data used to demonstrate the ownership. Watermark should not significantly affect the quality of original data and should not be able to destroy easily. The goal is to identify pirated copies of original data.

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark. For visible identification. The process of watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

Original Image Watermark Image with Watermark

Fig 1: Watermark and Image

2. LITERATURE REVIEW/RESEARCH BACKGROUND RELATED SEARCH

The technique used to hide a small amount of digital data in a digital signal in such a way that it can‟t be detected by a standard playback device or viewer. In Digital Watermarking, an indelible and invisible ‘message’ is embedded into both the image and the audio track of the motion picture as it passes through the server. According to R. Agarwal, piracy of digital assets such as image, video, audio and text can be protected by inserting a digital watermark into the data thus providing a promising way to protect digital data from illicit copying and manipulation [7]. After embedding the watermark, the data and watermark are in-separable.

This paper [2] provides an introduction of Genetic Algorithm, its basic functionality. The basic functionality of Genetic Algorithm includes various steps such as selection, crossover, and mutation. This paper also focuses on the comparison of Genetic Algorithm with other problem solving technique. The details of labs that basically concentrate on the research and development of Genetic Algorithm is also included. The details of labs include the various projects that are carried out on Genetic Algorithm.

Mona M. Suliman [11] et al have incorporated PSO with GA in hybrid technique called GPSO. This paper proposes the use of GPSO in designing an adaptive medical watermarking algorithm.

Baris Yuce [14] et al have explained that optimization are search methods where the goal is to find an optimal solution to a problem, in order to satisfy one or more objective functions, possibly subject to a set of constraints. In this paper the authors have described an optimization algorithm called the Bees Algorithm, inspired from the natural foraging behavior of honey bees, to find the optimal solution.

Sonia Sood [15] have proposed a novel method for watermarking relational databases based on hybrid model optimization in which the embedding and extracting algorithms of watermarking in discrete wavelet transform (DWT) are combined with Genetic Algorithm (GA)-Bacterial Foraging Algorithm (BFO) based optimization techniques for watermarking

3. PROPOSED TECHNIQUES

The proposed watermarking technique consists of the following scheme:

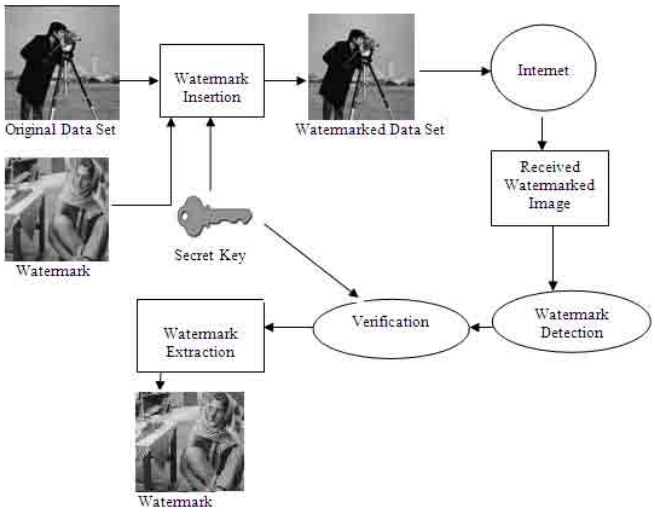


Fig 2: Digital Watermarking Scheme

In this scheme we are having two input images - one is original image and another is watermark image along with security key and the output is watermarked image. Original image is taken as input and water mark will be inserted on image with using a secret key to obtain water mark inserted output image. Secret Key is inserted for additional security purpose. The water marked signal is then transmitted or stored, usually transmitted to another person.

The parameters used in this paper are:

PSNR – The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image. The PSNR values can be obtained using following formula:

$$PSNR=20\log10\ (pixel\_value/\sqrt{mse})$$

MSE – Mean Squared Error is essentially a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of similarity/fidelity or, conversely, the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors. The MSE between the signals is given by the following formula:

$$MSE = (1/N)\Sigma i|x\ (i)- e\ (i)|2$$

Here x and e are the encrypted watermarked audio signals respectively and N is the number of samples in the audio signal [15].

In ideal case PSNR should be infinite and MSE should be zero. But it is not possible for watermarked image. So, large PSNR and small MSE is desirable.

4. EVALUATION AND RESULTS

Phase 1:

Firstly we develop a particular GUI for this implementation. After that we develop a code for the loading the original mage and message image or message in the Matlab database.

Phase 2:

Develop a code using hash partitioning technique. After that we apply it on the selected image and develop code for GA & HBO algorithm. When we apply the GA & HBO algorithm on the image then we got more accuracy than another technique.

Phase 3:

Develop a code for the finding the watermarked data. Then we got the image with message data this is called Embedding technique. For the embedding process and to make it more secure we apply the security key.

Phase 4:

After that we develop code for the extraction process. Within the extraction process we develop code for the message

extraction from the watermarked file. After the extraction process we got the original image and message data by using the key.

a. Original Image b. Watermark c. Image with Watermark

Fig 3: Image a and b are taken as input and image c is output

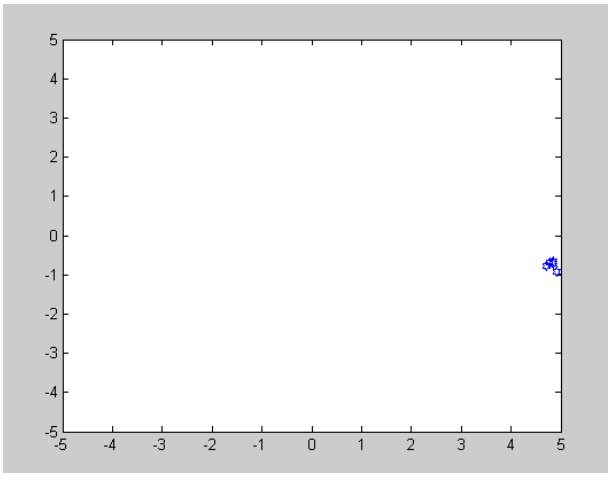


Fig 4: GA with HB Optimization

	GA with HB
PSNR	47.5389
MSE	114.602

Table 1: GA with HBO – PSNR and MSE Values

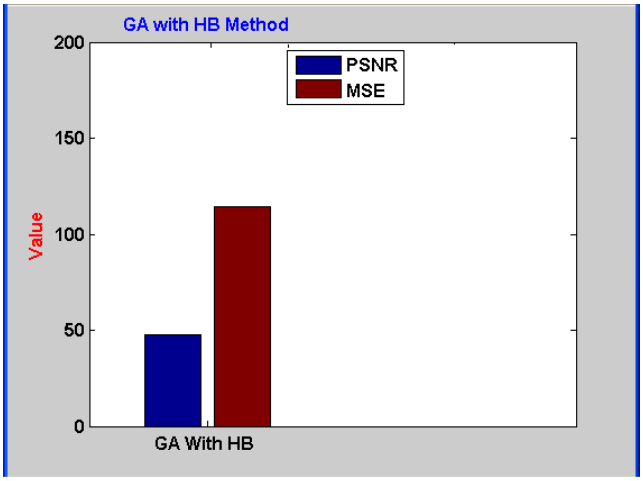


Fig 5: Graph Representation of PSNR and MSE

5. CONCLUSION

In this paper we have proposed a method for watermarking using genetic algorithm and honey bee. The results are formed by following the two basic parameters that are PSNR and MSE. In future we can increase the number of parameters for computing more results.

REFERENCES

[1] Lin, T.C., Lin, C.M., 2009. "Wavelet-based copyright-protection scheme for digital images based on local features ". Information Sciences 179, 3349–3358.

[2] Anita Thengade, Rucha Dondal," Genetic Algorithm – Survey Paper", MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April, 2012, Proceedings published by International Journal of Computer Applications® (IJCA)ISSN: 0975 – 8887.

[3] Paquet, A.H., Ward, R.K., Pitas, I., 2003. "Wavelet packet-based digital watermarking for image verification and authentication". Signal Processing 83, 2117–2132.

[4] F. Petitcolas, R. Anderson, and M. Kuhn. Attacks on Copyright Marking Systems. Lecture Notes in Computer Science, 1525:218– 238, April 1998.

[5] M. Swanson, M. Kobayashi, and A. Tewfik. Multimedia Data-Embedding and Watermarking Technologies. Proceedings of the IEEE, 86:1064–1087, June 1998.

[6] R. Sion, M. Atallah, and S. Prabhakar. Rights Protection for Relational Data. IEEE Transactions on Knowledge and Data Engineering, 16(6), June 2004.

[7] Mohamed Shehab, Elisa Bertino and Arif Ghafoor, "Watermarking Relational Databases Using Optimization-Based Techniques", IEEE Transaction on Knowledge and Data engineering, VOL. 20, NO. 1, January 2008.

[8] R. Agarwal and J Kieman, Watermarking relational databases In Proceedings of 28th International In Proceedings of 28th International Conference on very large databases, Hong Kong, China, 2002.

[9] Brijesh B. Mehta, Udai Pratap Rao," A Novel approach as Multi-place Watermarking For Security in Database"Dept. of Computer Engineering, S. V. National Institute of Technology, Surat, Gujarat.

[10] Prof.Bhawana Ahire, Prof. Neeta Deshpande," Watermarking relational databases: A Review",IOSR Journal of Engineering (IOSRJEN) ISSN: 2250-3021 Volume 2, Issue 8.

[11] Mona M. Soliman, Aboul Ella Hassanien, Neveen i. Ghali and hoda M. Onsi,"The way of Improving PSO Performance: Medical Imaging Watermarking Case Study", RSCTC 2012, LNAI 7413, pp. 237-242 2012.

[12] I.Daubechies, "Ten Lectures on Wavelets", Society for Industrial and Applied Mathematics, Philadelphia, PA, 1992.

[13] Goldberg, David E., "Genetic Algorithms in Search, Optimzation & Machine Learning", Addison-Wesley, 1989.

[14] Baris Yuce, Michael S. Packianather, Ernesto Mastrocinque, Duc Truong Pahm and Alfedo Lambiase,"Honey Bees Inspired Optimization Method: The Bees Algorithm",Insects 2013,4,ISSN 2075-4450.

[15] Sonil Sood, Ajay Goyal," Watermarking Relational Databases using Genetic Algorithm & Bacterial Foraging Algorithm", International Journal of Information & Computation Technology,ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1877-1884.

[16] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Water mark for Digital Images," Proc. IEEE Int. Conf on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[17] D. Das, N.K. Singh and A.K Singh, "A comparison of Fourier transform and wavelet transform methods for detection and classification of faults on transmission lines", IEEE Power India Conference, New Delhi, 10-12 April, 2006.

[18] J. Delaigle, C. De Vleeschouwer, and B.Macq,"Psychovisual Approach to Digital Picture Water marking," Journal of Electronic Imaging, vol. 7, no. 3,pp. 628-640, July 1998.

[19] D. Soumyendu, D.Subhendu,B.Bijoy, "Steganography And Steganalysis: Different Approaches", Information Security Consultant, International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications.

[20] Frank Hartung, Martin Kutter, "Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7,pp. 1085 – 1103, July 1999.

[21] Sawsan Morkos Gharghory "Hybrid Of Particle Swarm Optimization With Evolutionary Operators To Fragile Image Watermarking Based on DCT", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011, DOI : 10. 5121/ijcsit. 2011. 3310 141.

[22] T. T. Tran, T. T.Nguyen, andH. L.Nguyen, "Global optimization using levy flight," in Proceedings of the 3rd National Symposium on Research, Development and Application of Information and Communication Technology (ICT.rda '06), Hanoi, Vietnam, September 2004.

[23] S. He, "Training artificial neural networks using l´evy group search optimizer," Journal of Multiple-Valued Logic and Soft Computing, vol. 16, no. 6, pp. 527–545, 2010.

[24] Taha El Areef, Hamdy S. Heniedy, S . Elmougy, and Osama M. Ouda, "Performance Evaluation of Image Watermarking Techniques", Third International Conference on Intelligent Computing and Information Systems, Faculty of Computer & Information Sciences, ICICIS 7002 ,March 15-18, 2007, Cairo.

[25] Bijan Fadeena and Nasim Zarei,"Hyprid DCT-CT "Digital Image Adaptive Watermarking", 3rd International Conference on Advances in Database, Knowledge, an data Applications, IARIA 2011.

[26] Jayalakshami M., S. N. Merchant, Uday B. Desai, "Digital Watermarking in Contourlet Domain", 18th International Conference on Pattern Recognition, 2006.

[27] Bijan Fadeena and Nasim Zarei,"Hyprid DCT-CT "Digital Image Adaptive Watermarking", 3rd International Conference on Advances in Database, Knowledge, an data Applications, IARIA 2011.

EVALUATING THE KEY FINDINGS OF DIGITAL IMAGE WATERMARKING TECHNIQUES

Navdeep sandhu
M.Tech Scholar
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
nav.sandhu18@gmail.com

Ms. Navneet Bawa
Associate Professo
Department of CSE
Amritsar College of Engineering and Technology
Amritsar, India
bawa.navneet@gmail.com

ABSTRACT:-
Digital image watermarking is a process of hiding the images in a cover image for secure transmission or for the purpose of the copy right protection of digital images. This paper focuses on evaluating the shortcomings of the DCT, SVD and DWT based image watermarking techniques. This work focuses on the various techniques that are used for securing the data transmission over internet by using the concept of the watermarking. Much important information is communicated over the internet now. So securing the transmission is an important area of research. The overall objective of this paper is to evaluate the shortcomings of existing techniques on digital image watermarking.

KEYWORDS:- ATTACKS, SVD, DCT, DWT,WATERMARKS.

1.INTRODUCION

The approach of the Internet has brought about a lot of people new open doors for the creation andconveyance of substance in advanced structure. Applications incorporate electronic promoting, realtime featurealso sound conveyance, computerized archives and libraries, and Web distributed. A critical issuethat emerges in these applications is the security of the privileges of all members. It has beenperceived for a long while that current copyright laws are lacking for managing advancedinformation. This has prompted an investment towards creating new duplicate prevention and securityinstruments. One such exertion that has been drawing in expanding investment is focused around computerizedwatermarking strategies.

Digital watermarking is the procedure of hiding secret data in a digital medium. This information should be imperceptibly embedded in a manner that allows it to be extracted or detected later for security purposes. Various types of digital watermarking techniques for various media have been developed and categorized into three classes i.e. robust, fragile and semi-fragile. These classes are application-dependent. Digital watermarking being a potential mechanism of information security has established a lot of consideration from researchers over the last few decades and consequently has undergone a systematic research. A lot of methods and techniques have been proposed and implemented so far. The host values selected and the way the watermark is being embedded are two significant factors that conclude the effectiveness of the technique.

An invisible watermarking technique, in general, consists of an encoding process and a decoding process. Here, the watermark insertion step is represented as:

$$X` = EK(X,W) \quad (1)$$

where X is the original image, W is the watermark information being embedded, K is the user_s insertion key, and E represents the watermark insertion function. We adopt the notation throughout this chapter that for an original image X, the watermarked variant is represented as X`. Depending on the way the watermark is inserted, and depending on the nature of the watermarking algorithm, the detection or extraction method can take on very distinct approaches. One major difference between watermarking techniques is whether or not the watermark detection or extraction step requires the original image. Watermarking techniques that do not require the original image during the extraction process are called oblivious (or public or blind) watermarking techniques. For oblivious watermarking techniques, watermark extraction works as follows:

$$\hat{}W= DK0(\hat{}X\ 0) \quad (2)$$

where ˆX 0 is a possibly corrupted watermarked image, K0 is the extraction key, D represents the watermark extraction/detection function and ˆW is the extracted watermark information . Obvious schemes are attractive for many applications where it is not feasible to require the original image to decode a watermark. Invisible watermarking schemes can also be classified as either robust or fragile. Robust watermarks are often used to prove ownership claims and so are generally designed to withstand common image processing tasks such as compression, cropping, scaling, filtering, contrast enhancement, printing/scanning, etc., in addition to malicious attacks aimed at removing or forging the watermark .There is a wide range of applications of digital watermarking including copyright protection, authentication, finger-print, copy control and broadcast monitoring etc. For different kinds of applications digital watermarking should show different properties [1]. They can be usually categorized onto two categories: spatial domain watermarking schemes and frequency domain watermarking schemes. In spatial domain data is embedded straightly by altering pixel values of host image, while in transform domain data is embedded by altering transform domain coefficients. Watermark is distributed unevenly over the image in transform domain which makes enemy difficult to detect. Transform domain shows more toughness against a variety of attacks so it is more preferred then spatial domain.

2. DIGITAL WATERMARKING APPLICATIONS

Digital watermarks have been broadly and successfully deployed in billions of media objects across a wide range of applications. The following application areas are described in detail with information of how the technology works, case studies highlighting some of the most prevalent real world uses and links to related information that you may find useful.

a. Content identification and management
b. Content protection for audio and video content
c. Forensics and piracy deterrence
d. Content filtering (includes blocking and triggering of actions)
e. Communication of ownership and copyrights
f. Document and image security
g. Authentication of content and objects (includes government IDs)
h. Broadcast monitoring
i. Locating content online

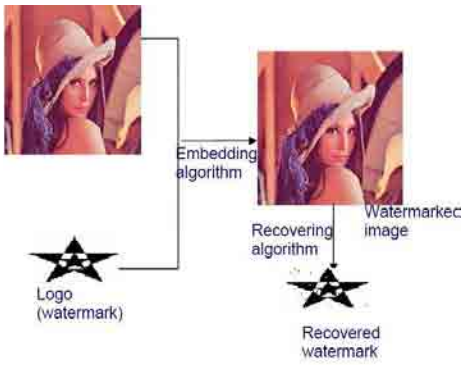


Fig 1: Watermarking Process.

Digital watermarking is use to conceal the proprietary information in multi-media by embedding an ownership data into given data. This ownership data is known as watermark and the given data is called host data. The watermark should be embedded into host data (image, audio or video) in such a way that it should not only robust against common attack but also in opposition to malicious attacks. Watermarking algorithm mainly consist of an embedding and an extraction algorithm.

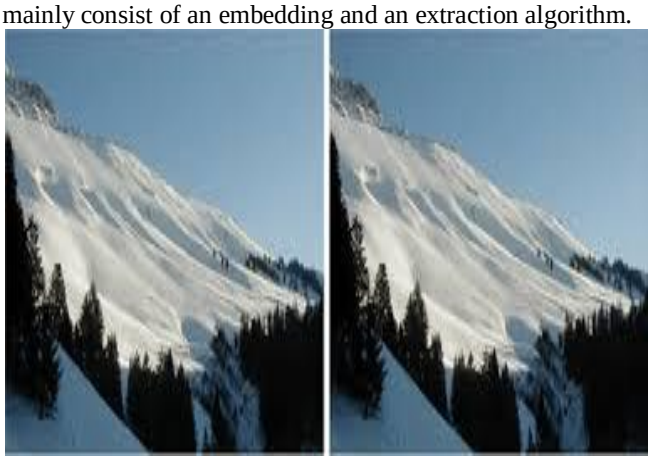


Fig 2: A) Input Image B) Watermarked Image

2. Watermarking Techniques

Watermarking techniques can be broadly classified into two categories according to operation domain: Spatial and Transform domain methods. Early image watermarking schemes operated directly in spatial domain. The spatial domain methods modify the original image's pixel values directly. But poor robustness against various attacks which was mostly associated with poor robustness properties. In contrast, in the transform domain such as, discrete cosine transform (DCT) wavelet transforms (WT) and singular value decomposition (SVD) provide more advantages and better performances will be obtained in compare with those of spatial ones in most of recent researches. Basically, a set of basic requirements is evaluated for a watermarking scheme to be effective. These requirements can be categorized as follows: (1) imperceptibility, (2) robustness, (3) capacity.

The following transform domain techniques are mostly used in image watermarking:

A. **DISCRETE COSINE TRANSFORM**

Discrete Cosine Transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. DCT divide the information energy in the bands with low frequency and DCT popularity in data compression techniques such as JPEG and MPEG. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of the image.FL is use to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques [3]. DCT represents data in terms of frequency space. DCT based watermarking techniques are robust compared to spatial domain techniques. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. The Discrete Cosine transform has been widely used for source coding in context of JPEG and MPEG and was later also considered for the use of embedding a message inside images and video.

Two-dimensional discrete cosine transformation and its inverse transform are defined as [13]:

$$C(u,v)=\alpha(u)\alpha(v)$$
$$\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

$$f(x,y)=$$
$$\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)c(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

where,u,v = 0,1,2…… N-1
x,y = 0,1,2……N-1

α(u) is defined as follows:
α(u) = √1/Nu=0;
α(u) =√2/Nu=1,2……N-1

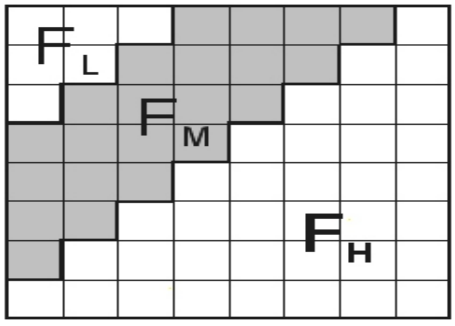


Fig.3 Discrete Cosine Transform regions

The major benefits of DCT include its high energy compaction properties and availability of fast algorithms for the computation of transform. The energy compaction property of the DCT results in transform coefficients with only few coefficients having values, thus making it well suited for watermarking. Embedding rules in DCT domain are more robust to JPEG/MPEG.

B.LWT DOMAIN WATERMARKING Lifting Wavelet Transform (LWT) proposed by Wim Sweldens is an advancement of DWT [15]. LWT is basically second generation wavelet transform in which the filters are not designed explicitly but it is based on "Lifting scheme" . LWT has many advanta&es over first generation wavelet. It is faster (by a factor of two) than traditional wavelet and it can be used to generate a multi resolution analysis that does not fit a uniform grid. LWT requires lesser memory space as compare to DWT. The LWT transform coefficients are integers, so remove weakness of quantizing errors from traditional wavelet transform. LWT decompose original image into four non-overlapping
502
multi-resolution sub bands of data: LL, HL, LHandHH. We use LL sub band to embed the watermark data by cascading with DCT.

C. DISCRETE WAVELET TRANSFORM:

DWT is currently used in a wide variety of signal processing applications, such as in audio and video compression and removal of noise in audio. Wavelets have their energy concentrated in time and are well suited for the analysis of transient time varying signal. To understand the basic idea of the DWT we focus on one dimensional signal. A signal splits into two parts, usually high frequencies and low frequencies. This process is continuing until the signal has been entirely decomposed [3]. DWT is preferred, because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The hierarchical property of the DWT offers the possibility of analyzing a signal at different resolutions and orientations. To understand the basic idea of the DWT we focus on one dimensional signal. A signal splits into two parts, usually high frequencies and low frequencies. This process is continuing until the signal has been entirely decomposed. The Figure shows basics of DWT approach for image processing.

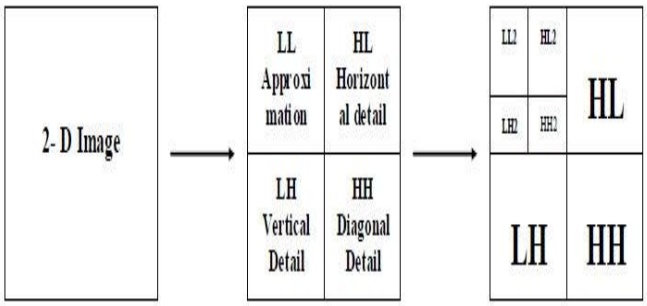


Fig.4 Wavelet Based Transform

The wavelet transform is given by equation 1.In the wavelet Domain whereWi denotes the coefficient of the transformed image. Xi denotes the bit of the watermark to be embedded. Here α is a scaling factor. And (u, v) represents basic transformed functions [2].

I Wu,v = Wi + α|Wi| Xiwhere u, v € HL,LH (1)

D. Singular Value Decomposition

SVD is a linear algebra technique used to solve many mathematical problems. It is a robust watermarking scheme for audio signals. SVD has been employed for different image applications. Such as compression, hash extraction and image watermarking. In image watermarking applications, the singular values of the host image are adapted in order to embed the watermark. SVD is able to efficiently represent the algebraic properties of an image. SVD techniques can be applied to any kind of images. If it is a gray scale image the matrix values are considered as intensity values and it could be modified directly or changes could be done after transforming images into frequency domain [5] [11] [12].

Let A be a general real (complex) matrix of order m×n. The singular value decomposition is the following factorization [14]

$A = U \times S \times V^T$ (2)

Where, U and V are orthogonal (unitary) and S =diag (σ1, σ2, ...,σr), where σi, i = 1,…, r are the singular values of the matrix A with r = min (m, n) and satisfying:

$\sigma_1 \geq \sigma_2 \geq \ldots\ldots \geq \sigma_r$ (3)

Use of SVD in digital image processing has some advantages which are listed as follows:

1. How big is the matrices from SVD transformation should definitely not square and may well be a rectangle.
2. Singular values in an electronic image are less affected if general image processing is performed. It indicates that for a tiny perturbation put into an image, its SVs don't change fast.
3. Singular values contain intrinsic algebraic image properties, where singular values correspond to the brightness of the image and singular vectors reflect geometry characteristics of the image.

SVD can effectively reveal essential property of image matrices, so it's been used in many different image processing applications such as for example noise estimation and digital watermarking.

3. RELATED WORK

Zebbiche et al. (2014) [1] has discussed a powerful wavelet-based fingerprint image watermarking scheme utilizing an efficient just perceptual weighting (JPW) model. In this, JPW model three human visual system characteristics has been defined, namely: spatial frequency sensitivity, local brightness masking and texture masking, to compute a weight for each wavelet coefficient, which may be then used to control the amplitude of the inserted watermark. Fingerprint images perceptually differ from natural images and a JPW model adapted to such images has been enhancing the robustness of watermarking scheme. Mainly this technique has shown a definite superiority over numerous related state-of-the-art masking techniques.

Zhu Yong et al. (2013) [2] has described the digital watermarking is a crucial way of copyright protection, that decomposes RGB for along with image and embeds the algorithm of multiple watermarks in the grayscale image of R, G. The algorithm has increases the number of watermark embedded and solves the interference problem of embedding multiple watermarks. This algorithm has good robustness to resist Shearing attack, Gaussian noise attack and JPEG compression attack.

Ketas Raval et al. (2013) [3] has explained the the business of security and authenticity of digital data in digital communication. In multimedia communication, digital images and videos have many applications. Although, watermarking algorithms are employed for copyright protection and security. But, all the watermarking algorithms transform the host image and embedding of the watermark information is done in robust way. Also, the uncompressed digital image transmission needs more space for storage and bandwidth.

Divecha Nidhi et al. (2013) [4] has described digital image watermarking is really a technology that's been developed to secure digital content from illegal use. Author proposed the implementation and performance analysis of two different watermarking schemes based on DCT-DWT-SVD. These techniques have been used to look for the effectiveness for imperceptibility and robustness in which peak signal noise ratio and normalized cross-correlation parameters are used.

Shojanazeri Hamid et al. (2013) [5] has described the state-of-the-art in video watermarking techniques. With the growth of Internet services and various storage technologies made video piracy being an increasing problem. Thus, research in copyright protection mechanisms and content authentication, where certainly details include digital watermarking has been receiving an increasing interest from scientists especially in designing a seamless algorithm for effective implementation. Basically digital watermarking involves embedding secret symbols called watermarks within video data which works extremely well later for copyright detection and authentication verification purposes. It gives a crucial review on various available techniques.

Qianli Yang et al. (2012) [6] has introduced an electronic digital watermarking algorithm with gray image predicated on two dimensions which are discrete wavelet and cosine transform for protecting digital media copyright efficiently. Where, the image is transformed into discrete wavelet domain 3 times, then split the image into sub-blocks, which can be lower in horizontal direction and full of vertical direction, and then transform every block into discrete cosine domain, and are embedded into cover image. Eventually, the key image is obtained by reverse transform of wavelet and cosine domain.

Hailiang Shi et al. (2012) [7] has described an RST invariant watermarking scheme using DWT-SVD and logistic map the spot that the watermark is a successfully meaningful grayscale logo. Where, the embedding is done by modifying the singular values of the approximation subband of the host image with logistic map encrypted watermark, and and so the watermark image is reconstituted. The results demonstrate that this scheme will have a way to withstand various geometric attacks and some common signal processing such as for example additive noise.

Mangaiyarkarasi, P. et al. (2011) [8] has presented a brand new digital image watermarking predicated on Ridgelet Transform (RT) and extraction using Independent Component Analysis (ICA). RT is a multiple resolution transform and it's great for describing the signals with high dimensional singularities. Also, high robustness and good imperceptibility is obtained using ridgelets. The embedded watermark is extracted using ICA, and the main benefit of this extraction technique is that it extracts the watermark in spatial domain itself and will not require any transformation process and will not require the initial image.

Al-Gindy, A. et al (2011) [9] has introduced a brand new copyright protection technique using colour watermarks. Where, the watermark is really a RGB colour image where each pixel is represented by 24 bits. Then, the RGB colour watermark is preprocessed by converting it into binary sequence. The preprocessed colour watermark is embedded multi-times into the green channel of the RGB host image by modifying the lower frequency coefficients of the DCT transformation. This new technique can resist classical attacks such as for example JPEG compression, low pass filtering, median filtering, cropping, and scaling attacks. In this, the recovery method is blind. Since, it doesn't have the initial host image for extraction.

Prsasad. R.M. et al (2010) [10] has discussed a strong invisible watermarking scheme for embedding and extracting an electronic digital watermark in an image to protect it from copyrights. The invisible insertion of the watermark image into the initial image is completed in wavelet domain using Haar wavelet transform. In this, the authors create a mask matrix utilizing the original image through MD5 algorithm and random matrix. The mask matrix was used in embedding and extraction processes. For extracting watermark, the partnership degree involving the mask matrix and the watermark embedded wavelet coefficients is computed.

4. CONCLUSION AND FUTURE WORK

Following are the various limitation of SVD watermarking:
Existing technique provide poor results in case there is attacks.The modification in SVD is neglected by many researchers to improve the robustness further.The usage of standard SVD is easily crack-able by the hacker or cracker.
The LWT reduces the time for extraction and embedding. There is still scope for improvement while working on image watermarking. There are some attacks like rotation and cropping on which almost all the proposed image watermarking algorithm shows less robustness.
The Conclusion shows that the LWT technique is used to overcome the shortcomings of the svd technique. In some of calculations, LWT gives comparative result compared to DCT and DWT and on some of benchmark parameters LWT gives better results than DCT and DWT techniques.

REFERENCES

[1] Zebbiche, Khalil, and Fouad Khelifi, "Efficient wavelet-based perceptual watermark masking for robust fingerprint image watermarking," IET Image Processing 8, pp.23-32, January 2014.
[2] Zhu, Yong, Xiaohong Yu, and Xiaohuan Liu, "An image authentication technology based on digital watermarking,**"** IEEE International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS), pp.179-183, May 2013.
[3] Raval, Keta, and S.Zafar, **"**Digital Watermarking with Copyright Authentication for Image Communication", IEEE International Conference on Intelligent Systems and Signal Processing (ISSP), pp.111-116, March 2013.
[4] Divecha, Nidhi, and N.N.Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking

algorithms for color images,**"** IEEE International Conference on Intelligent Systems and Signal Processing (ISSP), pp.204-208, March 2013.
[5] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad, "Video Watermarking Techniques for Copyright Protection and Content Authentication," IEEE International Journal of Computer Information Systems and Industrial Management Applications, vol.5, pp. 652–660,2013.
[6] Qianli, Yang, and Cai Yanhong, "A digital image watermarking algorithm based on discrete wavelet transform and discrete cosine transform," IEEE International Symposium on Information Technology in Medicine and Education, vol.2, pp.1102-1105, August2012.
[7] Shi, Hailiang, Nan Wang, Zihui Wen, Yue Wang, Huiping Zhao, and Yanmin Yang, "An RST invariant image watermarking scheme using DWT-SVD," IEEE International Symposium on Instrumentation and Measurement, Sensor Network and Automation(IMSNA), vol.1, pp.214-217, August 2012.
[8] Mangaiyarkarasi, P., and S.Arulselvi, "A new digital image watermarking based on Finite Ridgelet Transform and extraction using ICA," IEEE International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), pp.834-841, March 2011.
[9] Al-Gindy, Ahmed, Hana Younes, Amira Shaleen, and Hala Elsadi, "A graphical user interface watermarking technique for the copyright protection of colour images using colour watermarks," IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), pp.354-358, December 2011.
[10] Prasad, R.M., and Shivaprakash Koliwad, "A robust wavelet-based watermarking scheme for copyright protection of digital images," IEEE International Conference on Computing Communication and Networking Technologies (ICCCNT), pp.1-9, July 2010.
[11**]** Ghosh, Sudip, Pranab Ray, Santi P.Maity, and Hafizur Rahaman, "Spread Spectrum Image Watermarking with Digital Design," IEEE International Conference on Advance Computing (IACC), pp.868-873, March 2009.
[12] Dorairangaswamy, M.A., and B.Padhmavathi, "An effective blind watermarking scheme for protecting rightful ownership of digital images," IEEE Region 10 Conference in TENCON, pp.1-6, January 2009.

Weapon Detection in Human Body Using DWT Image Fusion

Navpreet Singh
Research Scholar
Department of ECE
ACET,
Amritsar.

Sandeep Kaushal
Associate Professor,
Department of ECE,
ACET,
Amritsar.

Guneet Kaur
Assistant Professor
Department of ECE
ACET,
Amritsar

***Abstract*—The detection of weapons hidden below a person's cloths is very much important to the improvement of the security of the public as well as the safety of public assets like airports, malls and railway stations etc. The focus of this paper is to develop a new algorithm to fuse a colour visual image and a corresponding IR image for such a concealed weapon detection application with the help of fusion technology.**

Keywords—concealed weapon detection, colour image, IR image, DWT Image fusion.

I. INTRODUCTION

We have recently witnessed the series of bomb blasts in Mumbai, Delhi etc. Terrorist implant Bombs in buses and underground stations. Many people are killed and many injured. This situation is not limited to India but it can happen or already happened anywhere and anytime in the world. In these entire cases concealed weapon detection (CWD) by scanning the images gives only satisfactory results. But we want a technology which gives us best result. So we try to bring the eventual deployment of automatic detection and recognition of concealed weapons. It is a technological challenge that requires innovative solutions in sensor technologies and image processing. The problem also presents challenges in the legal arena; a number of sensors based on different phenomenology as well as image processing support are being developed to observe objects below people's clothing. Now image fusion has been identified as a key technology to achieve improved CWD procedures. In our current work we focus on fusing visual and low cost IR images for
CWD.
Infrared images are depends on the temperature distribution information of the target to form an image. Usually the theory follows here is that the infrared radiation emitted by the human body is absorbed by clothing and then re-emitted by it. In the IR image the background is almost black with little detail because of the high thermal emissivity of body. The weapon is darker than the surrounding body due to a temperature difference between it and the body (it is colder than human body). The visual image is a mental image that is similar to a visual perception. The resolution in the visual image is much higher than that of the IR image. It is nothing but a RGB image that supports human visual perception. But there is no useful information on the concealed weapon in the visual image. The human visual system is very sensitive to colours. To utilize this ability if we apply this image with other image in fusion technique we get a better fused image that helps for detection.

II. BRIEF REVIEW

Imaging techniques based on a combination of sensor technologies and processing will potentially play a key role in addressing the concealed weapon detection problem. One critical issue is the challenge of performing detection at a distance with high probability of detection and low probability of false alarm. Concealed Weapon using the radar image are proposed by Yu-Wen Chang [1,2] in which drawbacks such as glint and specular reflection, these problems should be able to be overcome. A new algorithm proposed by Zhiyun Xue [3] in which fuse a colour visual image and a corresponding IR image for such a concealed weapon detection application in which they have great success. So fusion is an important step, we use here DWT fusion. Some more improve method are there such as Chu-Hui Lee [4] produce a easy applications to adjust for anytime, and anywhere you like, make sure that may work and take a photograph nicely. For binaries the fused image there are several method[5-7] Otsu method are chosen because this method are global method and effective for this type of image. The concept of small area removal is taken from [8]. However, based on biological research results, the human visual system is very sensitive to colours. To utilize this ability, some researchers map three individual monochrome multispectral images to the respective channels of an RGB image to produce a false colour fused image. In many cases, this technique is applied in combination with another image fusion procedure. Such a technique is

sometimes called colour composite fusion. We present a new technique to fuse a colour visual image with a corresponding IR image for a CWD application.

III. PROPOSED METHOD

In this technique for CWD we consider two types of image – a visual image and an IR image. Visual image is nothing but an RGB image which has three main colour components Red, Green and Blue.

.For this we consider IR image as second input. It basically depends on high thermal emissivity of the body. Basically the infrared radiation emitted by the body is absorbed by clothing and then re-emitted by it, is sensed by the infrared sensors. Due to difference in thermal emissivity we can realize the hidden object but since the background is almost black this image cannot help in CWD alone. The fusion algorithm consists of several steps which will be explained in detail in the following. Since these two input images are taken from two different image sensing devices so they are of different size. So we first resize these two types of images because the image fusion and other operations are not possible if the sizes are not same .Then perform the addition operation between visual and IR (visual + IR) images to get the combined image. But the resultant image does not give enough information. Then we complement the IR image to remove the background darkness. IR image lies the intensity between 0 to 255 intensity thus complement means subtracting all matrix component from 255 and we get complemented form or reverse form of the IR image. Then add visual image and complemented IR and get a resultant image. Then we convert IR image into HSV colour model because components of IR image are all correlated with the amount of light hitting the object, and therefore with each other, image descriptions in terms of those components make object discrimination difficult. After converting HSV model the image is now three components. Now we can use fusion technique because two images have the same dimension with same size and we use DWT fusion technique between HSV colour image and combined image. Then this fused image converted into gray scale image. Now we use Otsu's local thresholding technique for binarizing fused gray scale image.Then Extract the weapon portion by calculating all connected area component and remove too small component and also too large component according to the area values. To show the weapon in the actual RGB visual image we multiply the weapon's binary images with three dimensional RGB image. Basically the element wise multiplication is performed between two matrices. Now contour detection is used to detect edges of weapon from the weapon binary image and we use canny edge detector for detecting the edges. Then this binarizes contour image is divided into three components and multiply as before and we get contour with visual RGB image where we can detect the concealed weapon under the person's clothes very clearly.

IV. RESULT AND ANALYSIS

Take two images in the same pose visual RGB image and IR image which are shown in **figure 1** and **figure 2**.Resize these two types of image because image fusion and addition are not able to perform if the sizes are not same.

Figure 1: RGB image

Figure 2: IR image

Combine basically add visual image and IR image and the result is shown in **figure 3**. Actually we want to detect the hiding details from **figure 3** but image from **figure 3** is hazy, so we do not get enough information from **figure3.** Complement the IR image which is use full in the next operation and this complement image is shown in **figure 4.** IR image lies the intensity between 0 to 255 intensity thus complement means subtracting all matrix component from 255 and we get complemented form or reverse form of the IR image. Then add visual image and complemented IR image which is shown in **figure 5**.

Figure 3: Combined image

Figure 4: Complemented IR

Figure 5: Combined1 image

In this steps fusion is not possible due to dimension mismatch. We do these steps because in this step difference between hiding details and man are recognizable. Then we convert IR image into HSV colour model and it is shown in **figure6** because components of IR image are all correlated with the amount of light hitting the object, and therefore with each other, image descriptions in terms of those components make object discrimination difficult. Descriptions in terms of hue/lightness/saturation are often more relevant. After converting HSV model the image is now three components. Now we can use fusion technique because two images have the same dimension with same size. Then we use DWT fusion technique between HSV colour image and combined image is shown in **figure 7.** The discrete wavelet transform DWT is a spatial frequency decomposition that provides a flexible multi resolution analysis of an image. In wavelet transformation due to sampling, the image size is halved in both spatial directions at each level of decomposition process thus leading to a multi1resolution signal representation. The advantages of image fusion over visual comparison of multi-modality are: (a) the fusion technique is useful to correct for variability in orientation, position and dimension; (b) it allows precise anatomic1physiologic correlation; and (c) it permits regional quantisation. Many image processing like denoising, contrast enhancement, edge detection, segmentation, texture analysis and compression can be easily and successfully performed in the wavelet domain. Wavelet techniques thus provide a powerful set of tools for image enhancement and analysis together with a common framework for various fusion tasks. Applying fusion technique image sharpness and contrast enhanced. Then this fused image converted into gray scale image is shown in **figure 8**.

Figure 6: HSV image

Figure 7: Fused image

Figure 8: Fused gray image

This steps is required for the next step in which we use a binarization technique. There are several binarization techniques among them Otsu, Bernsen, savala , th-mean, niblack and iterative partitioning as a framework method are showing good result for this type of image. Here we use Otsu method which is a global Thresholding method i.e threshold value are calculated locally and get the result, no extra threshold value is added here. Extract this weapon portion by calculating all connected area component then remove too small component according to the area values. This only weapon portion binary image is shown in **figure 9**. Let us we want to show the weapon in the actual RGB visual image. The weapon binary images are stored into three different components because we want multiply it with three dimensional RGB image. Multiply individual element to element between two matrixes. In this step we detect weapon with visual RGB image is shown in **figure 10.**

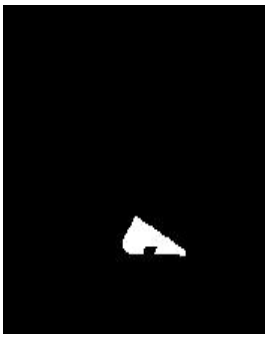


Figure 9: Weapon in binary image

Figure 10: Weapon in visual image

Contour detection is used to detect edges of weapon from the weapon binary image. Edge detection refers to the process of identifying and locating sharp discontinuities in an image. The discontinuities are abrupt changes in pixel intensity which characterize boundaries of objects in a scene. There is an extremely large number of edge detection operators available, each designed to be sensitive to certain types of edges. Here we use canny edge detection techniques. The Canny edge detection algorithm is known to many as the optimal edge detector. Canny's edge detection algorithm is computationally more expensive compared to Sobel, Prewitt and Robert's operator. However, the Canny's edge detection algorithm performs better than all these operators under almost all scenarios. This contour detection of concealed weapon is shown in **figure 11**.Then this binarizes contour image are divided into three component and multiply as before and get contour with visual RGB image which is shown in **figure 12** where we can see the concealed weapon
under person clothes easily.

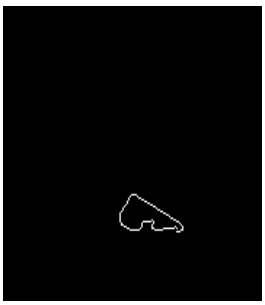


Figure 11: Contour of the Weapon image

Figure 12: Contour with Visual Image

V. CONCLUSION

In this paper we discuss a colour image fusion technique for CWD where we fuse a visual RGB image and IR image. We can able to detect the weapon concealed under person's clothes and bags. But infrared radiation can be used to show the image of a concealed weapon only when the clothing is tight, thin, and stationary. For normally loose clothing, the emitted infrared radiation will be spread over a larger clothing area, thus decreasing the ability to image a weapon.

VI. REFRENCES

[1] Yu-Wen Chang ; Michael Johnson. : Portable Concealed Weapon Detection Using Millimeter Wave FMCW Radar Imaging. Federal funds provided by the U.S. Department of Justice August 30, 2001.

[2] Z. Xue, R. S. Blum, and Y. Li. : Fusion of Visual and IR Images for Concealed Weapon Detection1.U. S.Army Research Office under grant number DAAD19-00-1-0431, pp 1198-1205.

[3] Zhiyun Xue, Rick S. Blum. : Concealed Weapon Detection Using Color Image Fusion. ISIF, pp-622- 627,2003.

[4] Sudipta Roy,Prof. Samir K. Bandyopadhyay, "*Contour Detection of Human Knee*", International Journal of Computer Science Engineering and Technology (IJCSET) ,September 2011 , Vol 1, Issue 8,pp. 484-487.

[5] Otsu, N.: A threshold selection method from gray-level histogram. IEEE Trans. Syst. Man Cybern. 9, 62–66(1979)

[6] Niblack,W.: An Introduction to Digital Image Processing. pp. 115–116. Prentice Hall, Eaglewood Cliffs (1986)

[7] Sauvola, J., Pietikainen, M.: Adaptive document image binarization. Pattern Recogn. 33(2), 225–236 (2000)

[8] Sudipta Roy and Prof. Samir K. Bandyopadhyay. Visual Image Based Hand Recognitions. Asian JournalOf Computer Science And Information Technolog(AJCSIT)y1:4 (2011), pp.106 – 110.

To remove noise in homogenous areas from degraded document images using Wiener filter algorithm

Er.Anita Rana[1], Dr.V.K.Banga[2]

M-Tech Scholar, Department of Electronics & Communication Engg

Amritsar collage of Engineering &Technology, Amritsar

Principle, Amritsar collage of Engineering &Technology, Amritsar

Abstract

Most offline handwriting recognition approaches proceed by segmenting characters into smaller pieces which are recognized separately. The recognition result of a word is then the composition of the individually recognized parts. Inspired by results in cognitive psychology, researchers have begun to focus on holistic word recognition approaches. Here we present a holistic word recognition approach for degraded documents, which is motivated by the fact that for severely degraded documents a segmentation of words into characters will produce very poor results. The quality of the original documents does not allow us to recognize them with high accuracy - our goal here is to produce transcriptions that will allow successful retrieval of images, which has been shown to be feasible even in such noisy environments. We believe that this is the first systematic approach to recognizing words in historical manuscripts with extensive experiments. Our experiment is to clear the degraded documents using filter approach. We will use wiener filter for removing noise partials from different images using wiener filter algorithm. We will also implement this design using GUI (Graphical User Interface) for selecting different images from self created data-base.

Index Terms— Degraded images, noise, de noising, wiener filter

Wiener filter

The Wiener filter is a linear filter for filtering images degraded by additive noise and blurring. Calculation of the Wiener filter requires the assumption that the signal and noise processes are second-order stationary. Wiener filters are often applied in the frequency domain. An image is often corrupted by noise in its acquition and transmission. Image de-noising is used to remove the additive noise while retaining as possible as possible the important signal features. In the recent years there has been a fair amount of research on wavelet thresholding and threshold selection for signal de-noising, because wavelet provides an appropriate basis for separating noisy signal from the image signal. The motivation is that as the wavelet transform is good at energy compaction, the small coefficient is more likely due to noise and large coefficient due to important signal features. These small coefficients can be thresholded without affecting the significant features of the image.

Degraded Images

Degradations in document images result from poor quality of paper, the printing process, ink blot and fading, document aging, extraneous marks, noise from scanning, etc. The goal of document restoration is to remove some of these artifacts and recover an image that is close to what one would obtain under ideal printing and imaging conditions. The ability to restore a degraded document image to its ideal condition would be highly useful in a variety of fields such as document recognition, search and retrieval, historic document analysis, law enforcement, etc. The emergence of large collections of scanned books in digital libraries has introduced an imminent need for such restorations that will aid their recognition or ability to search. Images with certain known noise models can be restored using traditional image restoration techniques such as Median filtering, Weiner filtering, etc. .

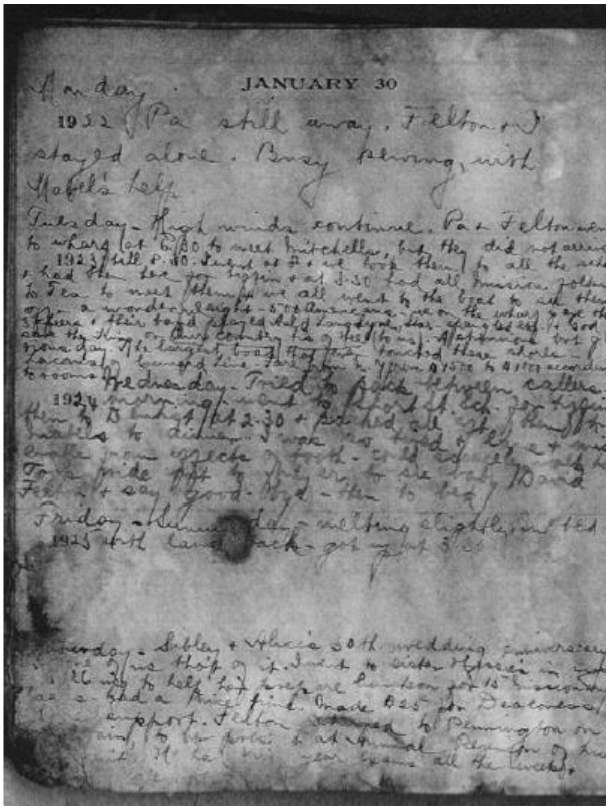


Figure 1: Degraded document

Figure 2: Degraded document

However, in prac-tice, degradations arising from phenomena such as document aging or ink bleeding cannot be described using popular image noise models. Document processing algorithms improve upon the generic methods by incorporating document specific degradationmodels and text specific content models. Approaches that deal with highly degraded documents take a more focused approach by modeling specific types of degradations. For instance, ink-bleeding or backside reflection is one of the main reasons for degradation of historic handwritten documents. In this paper, we approach document restoration in a different way, and useful setting. We consider the problem of restoration of a degraded 'collection of documents' such as those from a single book. Such a collection of documents,arising from the same source, is often highly homogeneous in the script, font and other typesetting parameters. The availability of such a uniform collection of documents for learning allows us to:

• To reduce the noise in homogenous areas.

• To implement wiener filter algorithm for removing the blurry effect from degraded images.

• Evaluating various parameters for studying percentage of improvement.

• To calculate execution time for taking output for our final code.

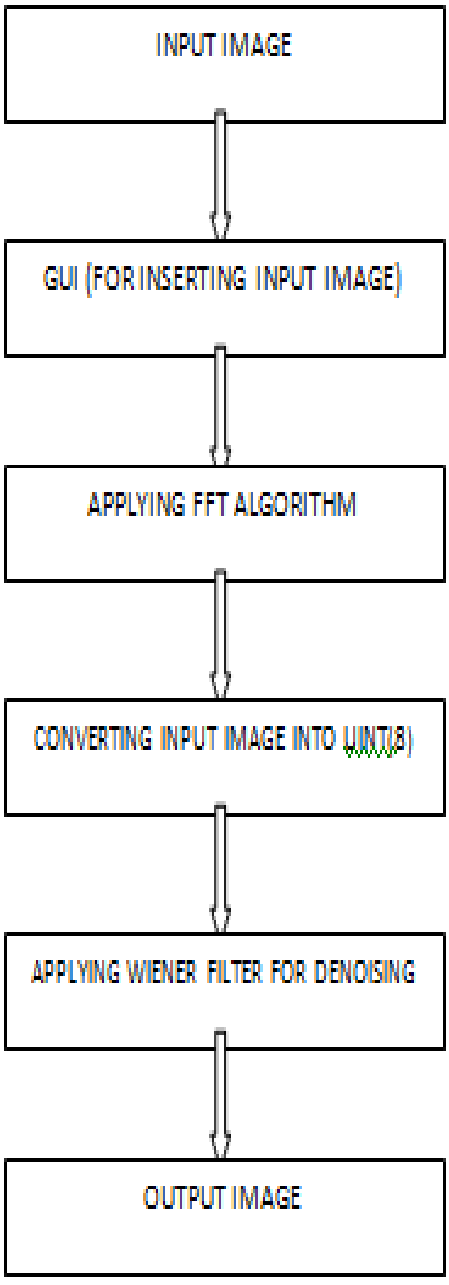
Related work

The work related to our work done so far is as, Niranjan Damera-Venkata, Thomas D. Kite, Wilson S. Geisler,Brian L. Evans and Alan C. Bovik [1] proposed model a for degraded image as an original image that has been subject to linear frequency distortion and additive noise. he develop a distortion measure of the effect of frequency distortion, and a noise quality measure of the effect of additive noise. Mohammed M. Siddeq Dr. Sadar Pirkhider Yaba [2] et. al. stated an algorithm for image de-nosing based on two level discrete wavelet transform and Wiener filter. At first The DWT transform noisy image into sub-bands, consist of low-frequency and high-frequencies and then estimate noise power for each of the sub-band. The noise power is computed through two important computations, compute square of variance for each sub-band then compute the mean of the variance. Srinivasa G. Narasimhan and Shree K. Nayar [3] et. al. stated that the images of outdoor scenes captured in bad weather often suffer from poor contrast. Under bad weather conditions, the light reaching a camera is severely scattered by the atmosphere and the resulting decay in contrast varies across the scene and is exponential in the depths of scene points. Deepak, Vikas Mittal [4]

designed speech recognition system using cross-correlation and FIR Wiener Filter. The algorithm is designed to ask users to record the words three times. The first and second recorded words are different words which will be used as the input signals. The third recorded word is the same word as one of the first two recorded words. The recorded signals corresponding to these words are then used by the program based on cross-correlation and FIR Wiener Filter to perform speech recognition. Bolan Su, Shijian Lu, and Chew Lim Tan [5] et. al. concluded that Segmentation of text from badly degraded document images in a very challenging task due to the high inter/intravariation between the document background and the foreground text of different document images. He proposes a novel document image binarization technique that addresses these issues by using adaptive image contrast. The adaptive image contrast is a combination of the local image contrast and the local image gradient that is tolerant to text and background variation which are caused by different types of document degradations.

The proposed methodology for efficient filtering of historical and degraded document images is illustrated in Fig. 3. It consists of many different steps. At the first step, at the run time GUI will execute and preprocessing based on Wiener filtering is applied. At the next step, several binarization results are combined in order to produce a binary (b/w) image taking into account the agreement in the majority of binarization methodologies.

Flow chart



At the next step, the edge information of the grey level image is combined with the binary result of the previous step. From all edge pixels, only those are selected that probably belong to text areas according to a criterion, number of pixels in output image and input image is calculated. Smoothing algorithm is then applied in order to fill text areas in the edge map. Finally, different parameters are calculated using different formulas.

Evaluation Measures

I Number of pixels in input and output images ,is used to calculate the total number of pixels original and restored image .By using matlab command 'n=nnz(x)' return the number of non-zero elements in matrix x.

II Size of I/O image. By calculating the row and column pixels, it used to find the total size of original and restored image. .

III MSE is **Mean Square Error**, f (i,j) is pixel value of output image, F(i,j) is pixel value of input image. Given by Formula:

$$MSE = \frac{\sum[f(i,j)-F(i,j)]^2}{N^2}$$

Or

MSE=((no_pixels_in_output_imageno_pixels_in_input_image).^2)./((Size_Of_Image).^2)

IV The **PSNR (peak signal to noise ratio)** is used to measure the quality of Restored image compared to the original image. Larger is the value, better will be the quality of image. It is calculated using equation as follow: , where MSE defined in 2 refers to mean square error.

PSNR= 20log10(255 / MSE) ……..(1)

The quality of the image is higher if the PSNR value of the image is high. Since PSNR is inversely proportional to MSE value of the image, the higher the PSNR value is, the lower the MSE value will be. Therefore the better the image quality is the lower the MSE value will be.

V Time calculation :- To use MATLAB command CLOCK to calculate time for our code to be executed, CLOCK is inbuilt command to show the real time, we use this command twice to calculate time consuming parameter.

Results and Discussion

In proposed algorithm, are used to provide more clearity than in previous work. In this, results of all the intermediate steps of the proposed methods are highlighted. Implementation is done on MATLAB Experimental results of intermediate steps show the efficiency of the proposed approach. Results includes following steps:Figure 3: Degraded document

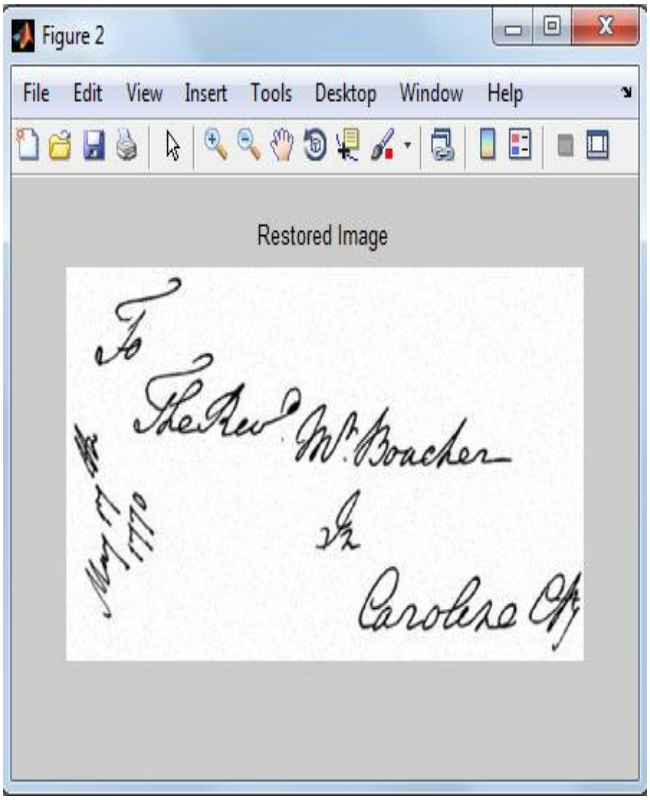


Figure 4: Restored image

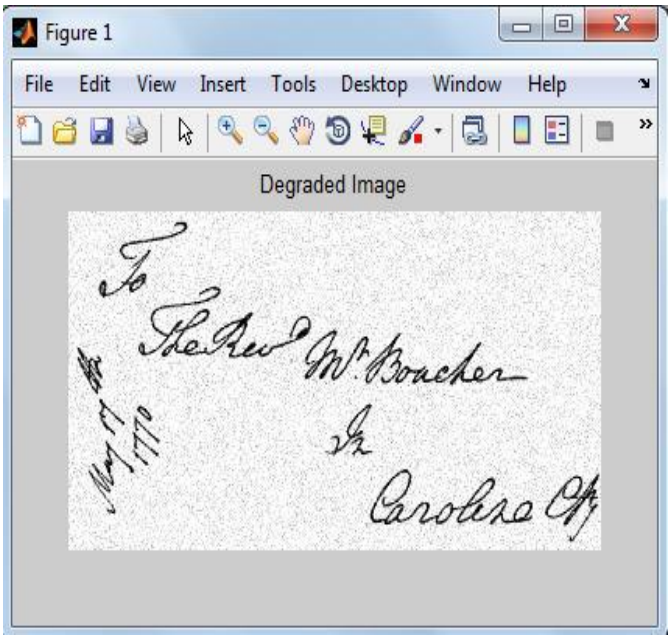


Figure 4.

S.NO.	NO.OF PIXELS OF I/P IMAGES	NO. OF PIXELS OF O/P IMAGES	SIZE OF I/O IMAGES	MSE	PSNR
1	528721	560153	565820	0.0031	49.1715
2	1283804	1317755	1320370	0.0066117	55.8623
3	318176	332435	332478	0.0018	51.4189
4	476790	501494	502095	0.0024	50.2258
5	650976	673892	674866	0.0012	53.4470

Table 1: Evaluation parameters

Conclusion

This paper work is based on removing noise from degraded images (handwritten documents). Our implemented algorithm is Wiener Filter Algorithm. This method includes histogram equalization and de bluring. This paper develops a system which is used to clear the degraded documents. We formulate number of parameters for our output and input images. We used to reduce the noise in homogenous areas, implement wiener filter algorithm for removing the blurry effect from degraded images, Evaluating various parameters for studying percentage of improvement and calculate execution time for taking our final output from our code. We reduce the amount of computation by not including other filters to our algorithm from which the execution time for our code gets very small.

FUTURE SCOPE

For developing an image technique that will become efficient for clearing degraded images, blur images and other noisy images. In this paper we took number of images for our research work, we calculate MSE, PSNR and Time to implement our design parameters. One can use some other technique to implement same design with reduced time. Someone can also calculate some other parameters and can improve GUI design.

REFERENCES:-

[1] Niranjan Damera-Venkata, Student Member, IEEE, Thomas D. Kite, Wilson S. Geisler, Brian L. Evans, Senior Member, IEEE, and Alan C. Bovik, Fellow, IEEE in APRIL 2000, " Image Quality Assessment Based on a Degradation Model" in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 9, NO. 4.

[2] Nikolas P. Galatsanos, Member, IEEE, Vladimir Z. Mesarovic´, Rafael Molina, and Aggelos K. Katsaggelos, Fellow, IEEE in OCTOBER 2000, " Hierarchical Bayesian Image Restoration from Partially Known Blurs" in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 9, NO. 10.

[3] Srinivasa G. Narasimhan and Shree K. Nayar in JUNE , " Contrast Restoration of Weather Degraded Images" in IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 25, NO. 6.

[4] B. Gatos, I. Pratikakis and S.J. Perantonis in 2008 , " Efficient Binarization of Historical and Degraded Document Images" in The Eighth IAPR Workshop on Document Analysis Systems.

[5] Taeg Sang ChoC. Lawrence Zitnick, Neel Joshi, Sing Bing Kang and Richard Szeliski, in APRIL 2012 , " Image Restoration by Matching Gradient Distributions" in IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 34, NO. 4.

[6] Oke Alice, Omidiora Elijah, Fakolujo Olaosebikan, Falohun Adeleye, Olabiyisi ,in AUGUST 2012," Effect of Modified Wiener Algorithm on Noise Models" in International Journal of Engineering and Technology Volume 2 No. 8.

[7] G. NAGENDRA, V.SRIDHAR, M.PRAMEELAMMA and M.ZUBAIR in SEPTEMBER 2012 , " FINGERPRINT IMAGE ENHANCEMENT USING FILTERING TECHNIQUES" in International Journal of Computer Science Engineering (IJCSE).

[8] Deepak and Vikas Mittal in MAY 2013 , " Speech Recognition using FIR Wiener Filter" in International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 5.

[9] Bolan Su, Shijian Lu, and Chew Lim Tan in APRIL 2013 , " Robust Document Image Binarization Technique for Degraded Document Images" in IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 4.

Use of Image Processing Techniques in Medical Field

BhawnaRana[1], Nitika Kapoor[2], Harish Kundra[3]
[1]M.tech Student , RIEIT, Railmajra

bhawnarana24@gmail.com
[2] Assistant Professor, RIEIT, Railmajra.
Er.nitikakapoor@gmail.com
[3]Associate Professor, RIEIT, Railmajra.
hodcseit@rayatbahra.com

Abstract—The processed images find their application in the field of Medical Science and can be beneficial for doctors in identification of diseases stages from monitoring point of view. In today's health care, imaging plays an important role throughout the entire clinical process from diagnostics and treatment planning to surgical procedures. The areas of application of digital image processing are so varied thatsome of organization is desirable in attempting to capture the breath of this field. One of the simplest way to develop a basic understanding of the extent of digital image processing application is to categorized image according to their source for example visual, x-ray and so on. Today, there is almost no area of technical endeavour that is not impacted in some way by digital image processing.

Keywords— Medical imaging, X-rays, Endoscopy, CT scan, digitizer, Stereo endoscope, Image Analyzer.

I. INTRODUCTION

Digital Image Processing succeeds in being an accessible but rigorous first course in the generation and manipulation of medical images.Digital image processing is a very vast in medical filed.Even applications in medical imaging cover a very wide spectrum of activities. In contrast, this paper focuses on image processing and its application related to the medical imaging and its related challenges.Even applications in medical imaging cover a very wide spectrum of activities. In contrast, this paper focuses on image processing and its application related to the medical imaging and its related challenges. With CT scanner, body's internal parts can be identified without causes any discomfort or pain to the patient. MRI picks up a signal from the body's magnetic particles spinning to its magnetic tune and with the help of its powerful computer, converts scanner data into revealing pictures of internal organs. Processing techniques developed for analysing remote sensing data may be modified to analysing the output of medical imaging system to get best advantage to analyse symptoms of the patients with ease.

II. DIGITAL IMAGE PROCESSING FOR MEDICAL APPLICATIONS REQUIREMENTS.

Digital image processing for medical applications required interfacing analog output of sensors such as microscopes,endoscopes, ultrasound etc, to digitizers and in turn to digital image processing system.

- Color correction image.
- Manipulating of colors within an image.
- Contour detection.
- Display of image line profile.
- Restoration of image.
- Smoothing of image.
- Registration of multiple image and mosaicing.
- Generation of negative images.
- Zooming of images.
- Pseudo coloring.
- Point to point measurements.
- Getting relief effect.
- Removal of artifacts from the image.

III. IMAGE PROCESSING SYSTEM FOR THE MEDICAL APPLICATIONS.

The medical applications and refinements continue to bring significant new diagnostic resources to health professionals and the general public they serve. Many successful companies and products today are direct offspring of digital imaging technology. Among medical applications derived from this technology are computed tomography (CAT) Scanning, diagnostic radiography, endoscopy, brain or cardiac angiography and ultrasound.

A. Endoscopy

Endoscopy means that looking inside the body for the medical reasons by using the instrument called endoscope. Endoscope used to examine the interior of a hollow or a cavity of the body. Unlike most of the other medical imaging devices the endoscope are directly inserted in the body.Each endoscope has two fiber bundles therefore one is used to illuminate the inner structure of object and other is used to collect the reflected light from that area. The endoscope is tubular optical instruments which is inspected or view the body cavities.

For a wider field of view andbetter imagequality,atelescopesystemisaddedintheinternalpartoftheendoscope.Technologicaladvancesincomputersandsemiconductorchipshavebroughtaboutlotofchangesinhealthcareduringthelastdecade endoscopy.Thesevideoendoscopesusexenonarclampsaslightsource.ColorImagingisachievedbyincorporatingRGBfiltersbetween XenonLampSupplyandtheproximalendofttheendoscope. The other approach to the generationofcolorimageistodividetheavailablecellsontheCCDamongthethreeprimarycolorsbymeansoffilters.Threeimagesonefore achcolorarethenproducedsimultaneously by the CCD.

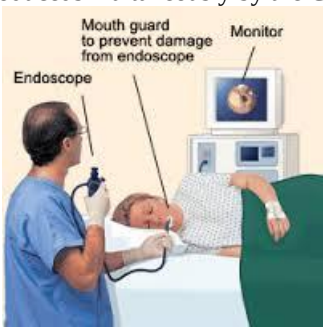


Fig 1.Endoscopy of human body by using the endoscope.

Endoscopic picture areconvertedtodigitalimagesbyusingCCDcamerasandassociatedimagedigitizercircuitsintoaPC/AT.Therecordedimagescanbeimageprocessed for better quality.

1) *Level-1 Stereo endoscope:*The twocameras are mounted on a single laproscope. Images from the cameras are transmitted alternately to a video monitor.Few types of display techniques are used to realize stereo images from two-dimensional images recorded from the above cameras. As the cameras transmits images at 60 -120 cycles per second a three-dimensional, real time image is perceived. The images are transmitted at a high frequency; the effect is that of seeing different images simultaneously.

B. X-Rays Imaging

X-rays are among the oldestsources of electromagnetic radiation used for imaging. The best use of x-rays is medical diagnostics, but x-rays are also used extensively in industry and other areas, like astronomy.X-ray for medical and industrial imaging are generated using an x-ray tube, which is vacuum tube with a cathode and anode. The cathode is heated and causing free electrons to be released. These electrons flow at high speed to positively charged anode.When the electrons strike with a nucleus, that energy is released in the form of x-ray radiation. The energy penetrating power of x-ray is controlled by a voltage applied across the anode. The x-ray simply generated by placing the patient between an x-ray source and film sensitive to x-ray energy.The intensity of x-ray is modified by absorption as they pass through the patient and the resulting energy falling on the film develops it much in the same way that light develops photographic film. Another use of x-ray in medical imaging is computerized axial to mography (CAT). Due to their resolution and 3-d capabilities, CAT scans revolutionized medicine from the moment they first become available. The technique is just similar for the industrial use.In digital radiography, digital image are obtained by one of two methods: by digitizing x-ray film and by having the x-ray that pass through the patient fall directly onto devices such as a phosphor screen that covert x-ray to light.

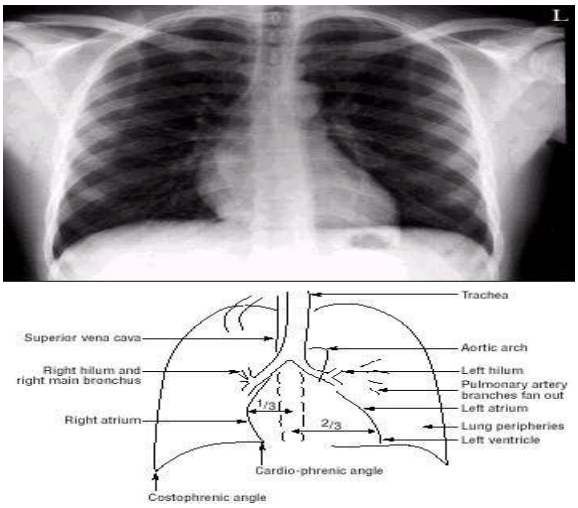


Fig 2. X-Ray of human body.

C. Computer tomography (CT)

Computerised AxialTomographyorcomputertransmissiontomographyorcomputertomographyisamethodofformingimagesfromX-rays.MeasurementsaretakenfromX-raystransmittedthroughthebody.These contain information of the body in the path of the X-ray beam. By using multiple directionsscanningofthebody,multiple datacan becollected.Animageofacross-sectionofthebodyisproducedbymeasuringthetotalattenuationalongrowsandcolumnsofamatrixandthencomputingtheattenuationofthematrixelementsattheintersectionsoftherowsandcolumns.Theinformationobtainedfromthesecomputationscanbepresentedinresultingtwo-dimensional picture.Thepatientliesinatubethroughthecenterofthegantry or theX-rays arepassingthroughthepatientandarepartiallyabsorbed.

Thedetectorresponseisdirectlyrelatedtothenumberofphotonsimpingingonitandhencetothetissuedensity.
The computer sensesthepositionoftheX-raytubeandsamplestheoutputofthedetectoralongadiameterlineopposite totheX-raytube and thecalculation isbasedondataobtainedfromacompletescanmadebythecomputer. Theseimagesarealsostoredintocomputer for image processing.CT has become an important tool in medical imaging to supplement x-raysand medical ultrasonography. It

hasbeen most recently used for preventive medicine or screening for disease, for example a full-motion heart scanning of patients with high risk of heart disease and CT colonography for patients with a high risk of colon cancer.
X-ray computed tomography (x-ray CT) is a technology that uses computer processed x-rays to produce tomography images(virtual 'slices') of specific areas of the scanned object that allow user tosee inside without cutting the body parts.

D. Ultrasonic imaging system

Ultrasonography is a technique by whichultrasonic energy is used to detect the state of the internal body organs. Bursts of ultrasonic energy are transmitted from a piezo-electric or magnetostrictive transducer through the skin and into the internal anatomy.When this energy strikes an interface between two tissues of different acoustical impedance, reflections (echoes) are returned to the transducer.When this energy strikes an interface between two tissues of different acoustical impedance, reflections (echoes) are returned to the transducer.The transducer converts these reflections to an electric signal proportional to the depth of the interface,which is amplified and displayed on an oscilloscope. An image of the interior structure is constructed based on the total wave travelling time,the average sound speed and the energy intensity of the reflected waves. The echoes from the patient body surface are collected by the receiver circuit. Proper depth gain compensation (DGC) is given by DGC circuit. The received signals are converted into digital signals and stored in memory. The scan converter control receives signals of transducer position and TV synchronous pulses. It generates X & Y address information and feeds to the digital memory.The stored digital image signals are processed and given to digital-to-analog converter. Then they are fed to the TV monitor.These signals are converted to digital form using frame grabber and can be stored onto PC/AT disk. Wherever the images lack in contrast and brightness, Image Processing techniques may be used to get full details from Ultrasound images. Figure 3 shows Ultrasound Imaging System.

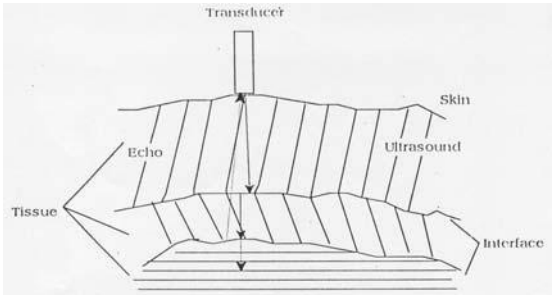


Fig. 3 Ultrasound imaging system

E. Magnetic resonance imaging (MRI)

Superconducingmagnets are used in MRI systems to provide strong uniform, steady magnetic fields. The superconducting magnetic coils are cooled to liquid helium temperature and can produce very highmagnetic fields. Hence the signal to noise ratio of the received signals and image quality are better than the conventional magnets used in the MRI systems.

Different gradient coil system produce a time varying, controlled spatial non-uniform magnetic fields in different directions. The patient is kept in this gradient field space. There are also transmitter and receiving RF coils surrounding the site on which the image is to be constructed. There is a superposition of a linear magnetic field gradient on to the uniform magnetic field applied to the patient. When this superposition takes place, the resonance frequencies of the processing nuclei will depend on the positions along the direction of the magnetic field gradient.This produces a one-dimensional projections of the structure of the three dimensional object. By taking a series of these projections at different gradient orientations using X, Y and Z gradient coils a two or three-dimensional image can be obtained. The slice of the image depends upon the gradient magnetic field.The gradient magnetic field is controlled by computer and that field can be positioned in three time invariant planes (X, Y and Z). The transmitter provides the RF signal pulses. The received nuclear magnetic resonance signal is picked up by the receiver coil and is fed into the receiver for signal processing.By two-dimensional Fourier Transformation, the images are constructed by the computer and analyzed using image processing techniques.

1) Level-1 Multispectral tissue classification of magnetic Resonance imaging (MRI):

- *MRI data*consists of multiple channels of independent but geometrically registered medically significant data, it analogous to multispectral remote sensing data.
- *Multispectral* analysis of proton MR images may provide tissue characteristic information encoded therein.
- *Using* well-established methods for computer processing of multispectral images, tissue characterization signatures are sought; using supervised or unsupervised classification methods.

F. Digital image processing for ophthalmology

The image processing techniques described including morphological filters for pre-processing fundus images, filters for edge detection. Fundus images of the retina are color image of the eye taken by specially designed digital cameras. Ophthalmologists rely on fundus images to diagnose various diseases that affect the eye, such as diabetic retinopathy and retinopathy of prematurity.

- To analyse retina, optic nerve, pigment epithelium and choroid in the ocular fundus.
- Colorslides have a resolution of 4000 x 3000 pixels.
- Fluorescein Angiograms have a resolution of 1800 x 1350 pixels.

- Common standard digital cameras have resolution of 512 x 480, which may be sufficient for obtaining relevant information of blood vessels etc. (Present day technology: 2048 x 2048 element resolution cameras).
- 8-bit resolution (indicative of contrast) is sufficient for most of the Opthalmology images.

G. Fundus image analyzers

Many diseases of the human visual system and of the whole body can have a dramatic impact on the 3-dimensional geometry of the ocular fundus. Glaucoma is probably the most important disease in this category. It increases the cupping of the optic nerve head at an early stage of the disease, in many cases before a reliable diagnosis can be made and visual field losses occur. The early diagnosis of glaucoma is a major issue in general public health care. Quantitative assessment of fundus geometry is expected to be helpful for this purpose

The ocular fundus consists of several layers of highly transparent tissue, each having individual physical properties, reflectivity, absorption and scatter. 2-dimensional geometry normally specifies sub-structures such as the vessel pattern or the area of pallor delineated by contrast or color variations. It is less important how deep they are located within the fundus. Depth is commonly associated with the topography of the interior limiting surface of compact retina and optic disc tissue.

A system for ocular fundus analysis consists of two parts, the image acquisition and the analysis software. The image is normally obtained using a telecentric fundus camera (Ex. Ziess-30 degree fundus camera). The image is captured onto a slide film. The film is scanned using a slide film scanner and transcribed to a Personal Computer. Alternatively the image can be directly acquired from the camera by interfacing it to the personal computer using a frame grabber card. Fundu image analyser (FIA) is the optic disc analysis software develop at NRSA. The present version operates on 2-D image only and does not support depth/volume calculations.

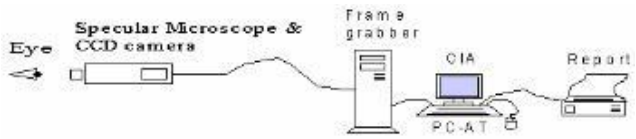


Fig 4. Show the fundu image analyzer.

H. Indocyanine green (Icg)image

- ICG anhiography is basically similar to that of fluorescein angiography.
- Differencencs are:
  - ❖ Spectral characteristics and,
  - ❖ Permeability from choroidal capillaries.
- Sodium fluorescein dye used in fluorescein angiography has a maximum absorption at 485nmand peak emission at 520nm.
  - ❖ The largest portion of excitation and emission energy of this visible light is absorbed by the retinal pigment epithelium and macular xanthopyll.
  - ❖ As a result, it is difficult to obtain sufficient fluorescence from the deeper layers of choroidal vessels.
- In blood, about 20% to 40% of injected sodium fluorescein remains unbound to serum albumin. This unbound fluorescein leaks rapidly from the highly fenestrated choriocapillaries into the choroidal anatomy. Because of this, details of the choroidal vascular pattern are obscured. For these two reasons, fluorescein angiography cannot provide useful information on choroidal circulation.
- In ICG angiography, the maximum absorption and peak fluorescence of Indocyanine dye is in the spectrum at 805nm and 835nm respectively. This near infrared light can penetrate the retinal pigment epithelium much more effectively than visible light, allowing uninterrupted examination of the choroidal vascular network. In addition, since approximately 98% of ICG dye in blood is bound to serum proteins, it leaks very slowly from the choroidal capillaries.

IV. ADVANTAGES OF DIGITAL PROCESSING FOR MEDICAL APPLICATIONS

- Digital data will not change when it is reproduced any number of times and retains the originality of the data.
- Offers a power tool to physicians by easing the search for re-preventative images.
- Displaying images immediately after acquiring.
- Enhancement of images to make them easier for the Physician to interpret.
- Quantifying changes over time;
- Providing a set of images for teaching to demonstrate examples of diseases or features in any image;
- Quick comparison of images.

V. ADVANCED DIGITAL IMAGE PROCESSING TECHNIQUES

- Neural network based image processing.
- Statistical approach for texture analysis.
- Segmentation in color and B/W images.
- Expert system based Image Processing.
- Application of object oriented programming techniques in Image Processing environments.
- Shape in machine vision.
- Multispectral classification techniques.
- Auto focussing techniques for MRI images.
- Thresholding technique for finding contours of objects.
- Sequential segmentation technique to find out thin vessels in medical images and hair line cracks in NDT.
- Fractal method for texture classification.
- Data compression techniques using fractals

and Descrete Cosine Transformers.

VI. Conclusions

During the next year, proufound changes are expected in computer and communication technologies that will offer the medical imaging system industry a challenge to develop advanced telemedicine applications of high performance. Medical industry, vendors , and specialists need to agree on a universal Medical imaging system industry a challenge to develop advanced telemedicine applications meteorology and medical imaging, images comprise the vast majority of acquired, processed and archived data. The medical imaging field in particular, has grow substantially in recent years, and has generated additional interest in methods and tools for the management, analysis and communication of medical image data.Recently proposals regarding the design of IDB system and the management of image data are influenced by the object oriented approach. This approach offers a framework with which different type of entities for example different kinds of image data and operation for example image processing functions, image access mechanisms etc, maybe uniformly represented as objects.

VII. REFERENCES

[1] R. C. Gonzalez woods and Addison Wesley, digital image processing 3nd ed.

[2] Anil K. Jain, Prentice-Hall: Fundamentals of Digital Image Processing .

[3] Geoff Dougherty: Digital image processing for medical applications.

[4] Introduction to science of medical imaging edited by Bryan.

[5] Digital image wrapping, George wolberg, IEEE computer Society press 1999.

[6] Digital image processing- chellappa, 2nded, IEEE computer society press, 1992.

[7] Biomedical instrumentation- M. Arumugam, Anuradha Agencies, polishers kumbaknam 19992..

A Performance evaluation of Carrier to Noise ratio for SSB Signal in Radio over Optical Fiber System

Akhil Bhatia[1], Sonu Kumar[2]
[1]ECE Department, ACET, Amritsar, Punjab, India
akhil.ece@acetedu.in@gmail.com
[2]ECE Department, JIET, Jind,Haryana,India
sonu37346@gmail.com

Abstract: The optical and wireless communication systems convergence will activate the potential capacity of photonic technology for providing the expected growth in interactive video, voice communication and data traffic services that are cost effective and a green communication service. The last decade growth of the broadband internet projects the number of active users will grow to over 2 billion globally by the end of 2014. Enabling the abandoned capacity of photonic signal processing is the promising solution for seamless transportation of the future consumer traffic demand. One emerging technology applicable in high capacity, broadband millimeter-wave access systems is Radio over Fiber also called Fiber To The Air (FTTA). In this paper, Optical SSB signal is specifically selected as it has tolerance for power degradation due to dispersion effects over a length of fiber and CNR (carrier to noise ratio) performance is evaluated in terms of phase noise from RF oscillator Linewidth and laser linewidth. Signal degradation is studied for various lengths of fibers in the presence of fiber chromatic dispersion

Keywords: RoF, CNR, MZM, OSSB, Power degradation.

I. INTRODUCTION

The Indian telecommunication industry is one of the world's fastest growing industries, with 653.92 million telephone (landlines and mobile) subscribers and 617.53 million mobile phone connections as on May 2010[1]. It stands the second largest telecommunication network in the world in terms of number of wireless connections after China. As the fastest growing telecommunications industry in the world, it is projected that India will have 1.159 billion mobile subscribers by 2013[1]. To meet the explosive demands of high-capacity and broadband wireless access, modern cell-based wire-less networks have trends, projecting continuous increase in the number of cells and utilization of higher frequency bands which leads to a large amount of base stations (BSs) to be deployed; therefore, cost-effective BS development is a key to success in the market [2]. In order to reduce the system cost, radio over fiber (RoF) technology has been proposed. RoF systems transmit an optically modulated radio frequency (RF) signal from a central station (CS) to a base station (BS) via an

optical fiber. The RF signal recovered using a photo detector (PD) at the BS arrives at a mobile station (MS) through a wireless channel. This architecture provides a cost-effective system since any RF oscillator is not required at the BS [3], and [4]. However, the performance of RoF systems depends on the method used to generate the optically modulated RF signal, power degradation due to fiber chromatic dispersion, nonlinearity due to an optical power level, and phase noises from a laser and an RF oscillator. Several techniques have been found for the optical generation of mm-waves wireless signals, including optical self-heterodyning, up- and down conversion, and external modulation[5], and [6]. The external modulation generates mm-wave optical double sideband (DSB) by using an external optical modulator. It is attractive because of the simplicity, and it can offer the most cost-effective base station (BS) without adding any active millimeter wave components to it. However, optical DSB signal suffers a severe fiber dispersion effect in an optical fiber link, resulting in the fading [7]. This problem has been solved in various ways; via either optical filtering of one of the sideband or single sideband modulation, and via compensation of the dispersion using either a fiber Bragg grating (FBG) or optical phase conjugator (OPC) . So, Optical Single Side Band (OSSB) modulation scheme is an effective way to eliminate the dispersion effects in RoF system. Here, we investigate the CNR (carrier to noise ratio) penalty due to fiber chromatic dispersion and phase noises from an RF oscillator and laser linewidth using an Optical Single Side Band (OSSB) signal. For the analysis of the CNR penalty, the autocorrelation and the PSD (power spectral density) function of a received photocurrent at photo detector (PD) are evaluated [8]. The bandwidth of an electrical filter is dealt in the CNR penalty since the phase noises result in an increase of the required bandwidth and the increased bandwidth causes an additional CNR penalty. It is shown that the phase noise from the RF oscillator is the dominant parameter in a short optical distance.

II. ROF SYSTEM MODEL

Generally, RoF systems transmit an optically modulated radio

frequency (RF) signal from a central station (CS) to a base station (BS) via an optical fiber and the photocurrent

wireless channel which is shown in Fig.1. An OSSB signal at base station (BS) is generated by using a Mach Zehender Modulator and a phase shifter. An RF signal from an oscillator is split by a power splitter and a 90◦ phase shifter.

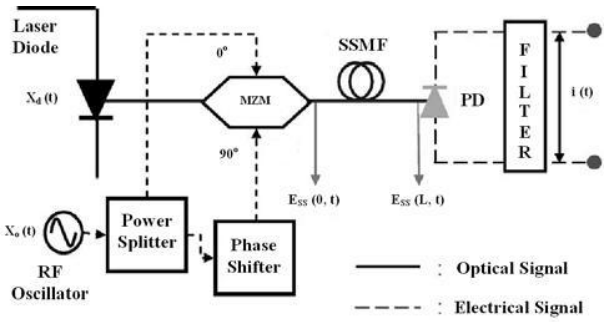


Fig.1. RoF system signal model

First, the optical signals from the optical source (laser diode) and the RF oscillator are modeled as follows:

$$x_d(t) = A^d \exp j\,(w_d t + \Phi_d(t)) \quad \text{.....} \quad (1)$$

$$x_o(t) = V_o .Cos\,(w_o t + \Phi_o(t)) \quad \text{.....} \quad (2)$$

Where A^c and V_o define amplitudes from the laser diode and the RF oscillator, ω_d and ω_o define angular frequencies of the signals from the LD and the RF oscillator, and $\Phi_d(t)$ and $\Phi_o(t)$ are phase-noise processes.

After optically modulating $x_o(t)$ by $x_d(t)$ with a Dual Electrode MZM, the output signal is represented as

$$E_{ss}(0, t) = \frac{L_{MZM} \cdot x_d(t)}{\sqrt{2}} \exp j\left(\gamma\pi + \frac{\pi}{V_\pi} \cdot \frac{x_o(t)}{\sqrt{2}}\right) + \exp j\left(\frac{\pi}{V_\pi} \cdot \frac{x_o(t)}{\sqrt{2}}\right) \quad \text{...} \quad (3)$$

$$E_{ss}(0, t) = \frac{A^d .L_{MZM}}{\sqrt{2}} \exp j\,(\gamma\pi + w_d t + \Phi_d(t)) + \alpha\pi \cos\,(w_o t + \Phi_o(t)) + \exp j\,(w_d t + \Phi_d(t) + \alpha\pi \cos\,(w_o t + \Phi_o(t) + \theta)) \quad .(4)$$

where ˜$x_o(t)$ denotes the phase-shift version of $x_o(t)$, γ(= Vdc/$V\pi$) and α(= V_o/ $\sqrt{2}V\pi$) define a normalized dc and ac value, $V\pi$ is the switching voltage of the DE MZM, L_{MZM} is the insertion loss of the DE MZM, and θ is the phase shift by the phase shifter. The output signal can be the OSSB or the ODSB signal by controlling the phase shifter. Since the ODSB signal suffers from fiber chromatic dispersion severely and requires double bandwidth than that of the OSSB signals. Due to that reasons, the OSSB signal will be generated. For generating the OSSB signal, θ and γ are set to π/2 and 1/2, respectively. By using (4) and the OSSB signal becomes

corresponding to the transmitted RF signal is extracted by the filter and this signal arrives at a mobile station (MS) through a

$$E_{SS}(0, t) = \frac{A^d .L_{MZM}}{\sqrt{2}} \exp j\left(\frac{\pi}{2} + w_d t + \Phi_d(t)\right) + \alpha\pi \cos(w_o t + \Phi_o(t)) + \exp j\,(w_d t + \Phi_d(t)) \quad \text{.... (5)}$$

$$E_{SS}(0, t) \cong A^d .L_{MZM} J_0(\alpha\pi) \exp j\left(w_d t + \Phi_d(t) + \frac{\pi}{4}\right) - \sqrt{2}\, J_1(\alpha\pi) \exp j\,(w_o t + \Phi_o(t)) \quad \text{.... (6)}$$

After the transmission of L_{fiber} in km standard single mode fiber (SSMF), the signal at the end of the SSMF becomes

$$E_{SS}(L, t) \cong A^d .L_{MZM} .L_{add} .10^{\frac{\alpha_{fiber} L_{fiber}}{20}} J_0(\alpha\pi) \exp j\left(w_d t + \Phi_d(t - \tau_0) - \varphi_1 + \frac{\pi}{4}\right) - \frac{\sqrt{2}\, J_1(\alpha\pi)}{J_0(\alpha\pi)} \exp j\,(w_d t + \Phi_d(t - \tau) + w_o t + \Phi_o(t - \tau) - \Phi_2) \quad \text{... (7)}$$

III. CNR PENALTY EVALUATION

To evaluate the CNR and the CNR penalty, we utilize the autocorrelation function and the PSD of the photocurrent [8]. By using a square-law model, the photocurrent $i(t)$ can be found from (7) as follows:

$$i(t) \cong \eta \left| E_{SS}(L, t) \right|^2 \quad \text{.... (8)}$$

$$i(t) \cong \eta \left| A^d \right|^2 B + 2\alpha_1 \cos\,(\Phi_d(t - \tau) - \Phi_d(t - \tau) + w_o t + \Phi_o(t - \tau) - \Phi_o + \Phi_{21}) \quad \text{..... (9)}$$

Where

$$A_1 = A_d .L_{MZM} .L_{add} .10^{\frac{\alpha_{fiber} L_{fiber}}{20}} J_0(\alpha\pi)$$

$$\alpha_1 = \frac{\sqrt{2} J_1(\alpha\pi)}{J_0(\alpha\pi)}$$

$$B = 1 + \alpha_1^2$$

where η defines the responsivity of the PD and $|.|^2$ is the square-law detection. From (9), the autocorrelation function $R_I(\tau)$ is obtained as

$$R_1(\tau) = \langle i(t).i(t + \tau) \rangle \quad \text{..... (10)}$$

. The PSD function $S_I(f)$ can be written as

$S_1(f) = \langle F\ R_1(\tau) \rangle$ ..... (11)

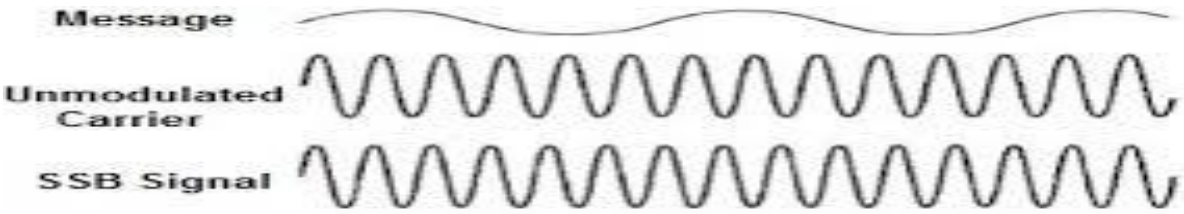


Figure 2. Simple Signal

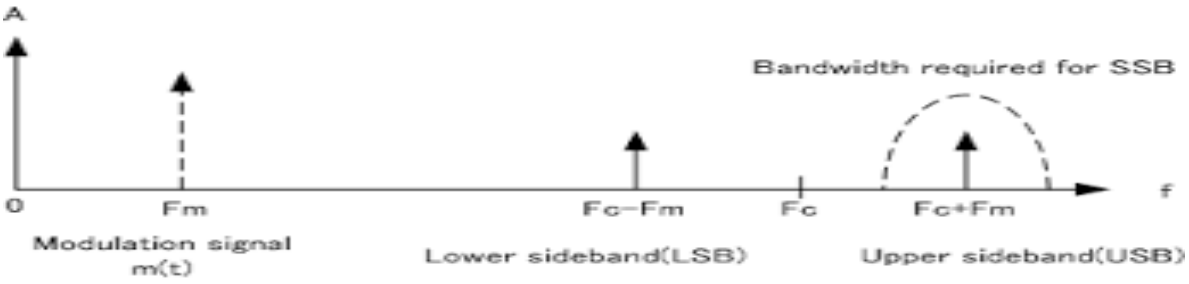


Figure 3. Simple Modulated Signal

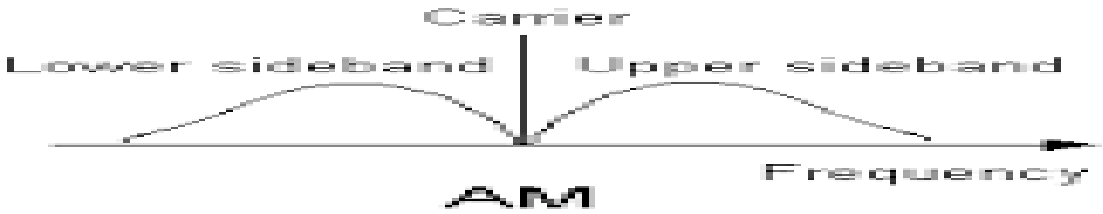


Figure 4. Simple Amplitude Amplification

$$S_1(f) = R_1(\tau) \int_{-\infty}^{\infty} R_1(\tau)\, d\tau * \exp(-j\tau w) \quad \ldots. (12)$$

In equation (13), the first term represents a dc component, second and third is the broadening effects due to the fiber dispersion and the linewidths of the RF oscillator.

$$\frac{S(f)}{\eta^2 A^4} = B^2 \delta(f) + \frac{2\gamma_o \alpha_1^2 .\exp(-2\gamma_t |\tau|).\cos[2\pi(f-f_o)\tau]}{\gamma_o^2 + 2\pi(f-f_o)]^2} + \frac{4\alpha_1^2 .\exp(-2\gamma_t |\tau|)}{(2\gamma_t)^2 + [2\pi(f-f_o)]^2} \quad \ldots (13)$$

$$.\{\gamma_t .\exp(-2\gamma_t |\tau|) - \gamma_t \cos[2\pi(f-f_o)\tau] - \frac{4\pi\gamma_d(\gamma_d+\gamma_o)(f-f_o)}{\gamma_o^2 + 2\pi(f-f_o)]^2} .\sin[2\pi(f-f_o)\tau]\} + P(f+f_o)$$

Where

$$P(f+f_o) = \frac{2\gamma_o \alpha_1^2 .\exp(-2\gamma_t |\tau|).\cos[2\pi(f+f_o)\tau]}{\gamma_o^2 + 2\pi(f+f_o)]^2} + \frac{4\alpha_1^2 .\exp(-2\gamma_t |\tau|}{(2\gamma_t)^2 + [2\pi(f+f_o)]^2}$$

$$.\{\gamma_t .\exp(-2\gamma_t |\tau|) - \gamma_t \cos[2\pi(f+f_o)\tau] - \frac{4\pi\gamma_d(\gamma_d+\gamma_o)(f+f_o)}{\gamma_o^2 + 2\pi(f+f_o)]^2} .\sin[2\pi(f+f_o)\tau]\}$$

Now the received RF carrier Power P_I is approximately represented as follows

$$P_1 = 2 \int_{f_o - \frac{B_o}{2}}^{f_o + \frac{B_o}{2}} PSD(f) df \ldots.. (14)$$

And by using (14), we find ratio p between the total carrier power and the required power as follows:

$$p = \frac{P_1}{P_t}$$

$$p \cong \frac{2}{\pi} \exp(-2\gamma_t |\tau|) \tan^{-1} \frac{\pi .B}{2\gamma_o} \quad \ldots. (15)$$

The CNR penalty induced by the differential delay from the fiber chromatic dispersion and the linewidths from the laser and the RF oscillator is found as

$$CNR \cong \frac{P_1}{2B_o .\frac{N_o}{2}}$$

$$CNR \cong \frac{2\eta^2 A_1^{d4} \alpha_1^2 p}{N_o .\frac{\gamma_o}{\pi} \tan\frac{\pi . p \exp(-2\gamma_t |\tau|)}{2}} \quad \ldots. (16)$$

IV. RESULT AND DISCUSSION

Now, we investigate the CNR penalty due to the differential delay, and the filter type. If CNR_0 is defined as a reference CNR, the CNR penalty CNR is represented as

$$CNR = 10 \log_{10} \frac{(CNR_o)}{(CNR)}$$

$$CNR = 10 \log_{10} \frac{p_0 .\gamma_o \tan\frac{\pi p.}{2} \exp(2\gamma_t |\tau|)}{p.\gamma_{oo} \tan\frac{\pi p_0 .}{2} \exp(2\gamma_{oo} |\tau|)} \quad \ldots (17)$$

For calculating the CNR_o, we set p_0 to 0.5 as a half-power bandwidth filter, γ_{oo} to π, which means a 1 -Hz linewidth of the RF oscillator, and zero laser linewidth. The CNR penalty CNR depends on p, the linewidths, and the differential delay. Firstly, we investigate the effect of p and γ_o on the CNR penalty for a 10-km fiber, 30-GHz RF carrier, fiber dispersion parameter D (= 17 ps/nm.km), and 1550-nm.

Table 1 the Simulation Parameters for CNR penalty as a function of the RF oscillator linewidth and percentage of received power

Parameters	**Value**
Fiber dispersion	17 ps/nm-km
Optical transmission distance	10 km
RF carrier frequency	30 GHz
Wavelength of LD	1550 nm
Half power bandwidth filter	0.5
RF oscillator linewidth	0.1 to 20 Hz
Percentage of received power	0.1 to 0.99

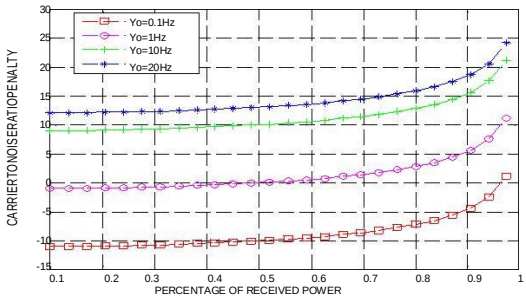


Fig.5. CNR as a function of the RF oscillator linewidth and percentage of received powe

The First result sketched in Fig.2 with simulation parameters in Table 1represents the CNR penalty as a function of the RF oscillator linewidth and percentage of received power is. The linewidth of the RF oscillator has been swept from 0.1 to 20 Hz and the CNR penalty of the RF oscillator due to the increment of the phase noise from 0.1 to 20 Hz is around 23 dB. Also the effect of γ_o is linearly proportional to CNR and Fig. 2. The linear proportion means that CNR increases 10 dB, which is equivalent to ten times the increment of γ_o.

CNR also increases as *p* becomes large since the increment of the noise power is greater than that of the received signal power as the bandwidth increases. For example, the CNR penalty of p = 0.99 is 12.2 dB as compared to p = 0.1[9]. Thus, the minimum required power to detect the signal should be carefully considered before we consider the filter bandwidth.

Table 2 the Simulation Parameters for CNR penalty as a function of the laser linewidth and length of fiber

Parameters	**Value**
Fiber dispersion	17 ps/nm-km
Optical transmission distance	1 km to 40 km
RF carrier frequency	30 GHz
Wavelength of LD	1550 nm
Half power bandwidth filter	0.5
Laser linewidth	10 to 624 MHz
Percentage of received power	0.5

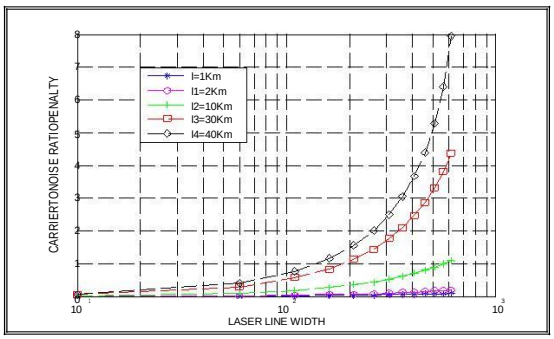


Fig.6. CNR as a function of the laser line width and fiber transmission distance.

Now, The Second result CNR is sketched in Fig. 3 with simulation parameters in Table 2. represents the function of the laser line width and fiber transmission distance. It is found that CNR exponentially increases as the laser linewidth (Y_d). It is notice that CNR penalty due to laser linewidth from 10 to 624 MHz are 0.22, 1.2, 4.9, and 8 dB.in 2, 10, 30, and 40 km SSMFs. Further, it is found that CNR penalty increases around 8 dB with respect to fiber length from 1km to 40 km. So, the RoF system relatively suffers from CNR for a long transmission, such as 40 km, while CNR is almost not
changed (=0.22 dB) even for the FP laser in the short-transmission case (=2 km). It is confirmed that the FP laser can be used in a practical microcell boundary because the radius of the microcell is from 0.2 to 1 km.
The CNR penalty due to the laser linewidth increases dramatically over a specific distance. Therefore, the laser linewidth should be selected carefully in a long -haul transmission since the large differential delay and large laser linewidth cause a serious CNR penalty. For a short distance, the phase noise from the RF oscillator is the dominant factor of the CNR penalty. For consideration, the CNR penalty due to RF oscillator linewidth from 0.1 to 20 Hz is around 23 dB in any case, while the CNR penalties due to the laser linewidth for 624 MHz are 0.22, 1.2, 4.9 and 8m dB in 2- , 10-, 30 - and 40-km SSMFs. This means that we can employ a cheap laser such as the FP laser in the RoF system in picocell, microcell and macrocell without a severe CNR penalty.

V. CONCLUSION

We have shown that the CNR Penalty has been investigated due to the phase noise from RF oscillator as well as laser for various line widths over different lengths of fiber. It is evident that the CNR penalty increases as the length of the fiber increases following the exponentially increment. We also conclude that the bandwidth of an electrical filter at the receiver should be carefully chosen after considering minimum required signal power ratio *p*.

REFERENCES

[1] http://en.wikipedia.org/wiki/Communications_in_India.

[2] Y. Kim *et al.*, "Beyond 3G: Vision, requirements, and enabling technologies," *IEEE Commun. Mag.*, vol. 41, no. 3, pp. 120–124, 2003.

[3] A. Alphones, "Double-spread radio-over-fiber system for next-generation Wireless technologies," *OSA J. Opt. Netw.*, vol. 8, no. 2, pp. 225–234, Feb. 2009.

[4] T. Koonen, "Fiber to the Home/Fiber to the Premises: What, Where, and When?," Proceedings of the IEEE, Vol. 94, No. 5, May 2006.

[5] P. Kaur, and R.S.Kaler, "Radio over Fiber Networks," Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007) RIMT-IET, Mandi Gobindgarh, March 23, 2007.

[6] N. Mohamed, S.M. Idrus, and A.B. Mohammad, "Review on System Architectures for the Millimeter-Wave Generation Techniques for RoF Communication Link," IEEE International RF and Microwave Conference Proceedings, December 2-4, 2008.

[7] N. Pleros, K. Vyrsokinos, K. Tsagkaris, and N. D. Tselikas, "A 60 GHz Radio-Over-Fiber Network Architecture for Seamless Communication With High Mobility," Journal of Lightwave Technology, Vol. 27, No. 12, June 15, 2009.

[8] H. K. Dass, Advanced Engineering Mathematics, 1st Edition**,** S. Chand, 2009.

The Ubiquitous DBMS and Mobile Database

Divya sharma[1](div2711@gmail.com)
ACET,Amritsar
Sapna Kumari [2] (guptasana@rediff.com)
Assistant Professor, BBKDAV College for women,Amritsar

ABSTRACT

Advancement in mobile computing technologies has prompted strong needs for database systems that can be used in small devices such as sensors, cellular phones, PDAs, car navigators, and Ultra Mobile PCs (UMPCs).We term the database systems that are customizable for small computing devices as *Ubiquitous Database Management Systems* (*UDBMSs*). In this paper, we review the requirements of the UDBMS and then include lightweight DBMSs selective convergence, flash-optimized storage systems, data synchronization, support of unstructured/ semi structured data, complex database operations, self management, and security. Then we review existing systems and research prototypes. We review the functionality of UDBMSs including the footprint size, support of standard SQL, transaction management, concurrency control, recovery, indexing, and access control.

Keywords:
databse ,security,synchronization,Structured data.

1. Introduction

The growing popularity of mobile technologies and advancement in computing power have prompted strong needs for database systems that can be used in small computing devices such as sensors, smart cards, cellular phones, PDAs, car navigators, and Ultra Mobile PCs (UMPCs). These small devices with mobility and embedded processors are called *ubiquitous devices.* As the ubiquitous devices get computationally powerful and the bandwidth of the wireless network rapidly expands, we can use them to perform tasks anytime and anywhere often downloading a variety of data from servers and uploading sensor data to servers. This kind of computing environment is commonly called the *ubiquitous environment*.

New storage devices suitable for ubiquitous devices such as flash memory and MEMS (Micro-Electro-Mechanical Systems)-based storage devices have been developed. As the capacity of the storage devices is getting bigger and bigger, we can easily store and manage a huge amount of data in a ubiquitous device. This trend prompted strong needs for the database systems that can be used in ubiquitous devices.

The primary *storage* of ubiquitous devices is flash memory. Flash memory is non-volatile and has many advantages over the disk. Since the capacity of flash memory is increasing and the cost decreasing, flash memory will be widely used also in PCs and servers. Another type of storage media for ubiquitous devices is MEMS-based storage devices . A MEMS-based storage device is a secondary storage device and also has many
advantages over the disk. Currently, there are some prototypes of MEMS-based storage devices but no products are available yet.
Ubiquitous devices usually have a limited storage capacity. Hence, users store bulk of data in the server and download the necessary parts to the ubiquitous devices. In this environment, when the data are modified in the ubiquitous device, the data need to be
transmitted back and stored at the server to maintain consistency of data between them. This issue is called *data synchronization*.

The data types that need to be supported in ubiquitous devices include text data, web pages, XML data, spatial data, multimedia data, and sensor/stream data. E-mail clients, word processors, and spreadsheet applications manage text data. Web browsers manage web pages and XML data. Car navigation systems manage spatial data. Image viewers, MP3's, and movie players
manage multimedia data such as JPEG, MP3, and AVI files. A sensor transmits the data sensed to the server as a stream.
To support the ubiquitous environment, the UDBMS needs to be able to be deployed to different types of ubiquitous devices and to be able to support various applications. In addition, the UDBMS should support new types of storage devices, different types of data, data synchronization, self-management, and security.

2. REQUIREMENTS OF THE UDBMS

In this paper, we consider mobile and embedded DBMSs as UDBMSs. Based on
existing systems, we identify important requirements for the UDBMS as follows:

- **Lightweight DBMSs**

Table 1 shows a summary of typical specifications of ubiquitous devices. As shown in Table 1,ubiquitous devices have lower computing power than PCs or servers.

Ubiquitous Devices	CPU Clocks	Main Memory Sizes	Storage Sizes
Sensors	7 MHz	0.5 ~ 8 KBytes	8 ~ 128 KBytes
Smartcards	14 MHz	4 KBytes	128 KBytes
Cell Phones	300 MHz	64 MBytes	128 MBytes
PDAs	624 MHz	128 MBytes	256 MBytes
Car Navigators	1 GHz	256 MBytes	16 GBytes
UMPCs	1.3 GHz	1 GBytes	80 GBytes

Table 1.

Using a low-clock CPU, small memory, and small storage, a UDBMS needs to support the functionalities required by applications with acceptable performance.Furthermore, since ubiquitous devices have limited power sources such as batteries, a UDBMS needs to
support the functionalities with low power
consumption. Thus, it is important to design and implement a UDBMS as simple as possible considering the performance of devices.

➢ **Selective Convergence**

To support the lightweight DBMS requirement, it is important to selectively compose the modules of a UDBMS depending on the applications and the device
type. In order to emphasize the capacity that selects only necessary modules, we call this property "*selective convergence*". For low performance devices such as sensors and smartcards, users would want only simple and basic functionalities. In contrast, for high performance devices such as PDAs and UMPCs, users would want advanced functionalities such as data synchronization.
For example, if a user wants to run a GIS application in his PDA, the user would want spatial functionalities.

➢ **New Storage Devices**

For ubiquitous devices, non-volatile memories (e.g., flash, EEPROM, and FeRAM) and very small secondary storage devices (e.g., MEMS) have many advantages over the disk.
Flash memory is a representative non-volatile memory.Compared with the disk, flash memory has attractive features such as small size, better shock resistance, lower power consumption, fast access time, and no mechanical seek and rotational latency.Besides, there is an erase operation, which does not exist in the disk. In order to update existing data in a page, an erase operation should be performed first on the entire block to which the page belongs. The erase time is about ten times slower than the write time, and the number of erase operations is limited to 100,000 ~ 1,000,000 times.

A MEMS-based storage device is a very small non-volatile secondary storage. The size is as small as 1cm2,and the average access time is ten times faster than that of the disk with lower power consumption. The MEMS device is composed of a media sled and a probe tip array. The *media sled* is a square plate on which data are recorded, and the *probe tip array* is a set of heads.
The MEMS device reads and writes data by moving the media sled in the direction of both X and Y axes. By selecting and activating a portion of the heads simultaneously, users can access multiple data sectors in parallel.

- **Unstructured and Semi-structured Data**

Various types of unstructured/semi-structured data such as text, multimedia, XML, spatial, stream, and sensor data are widely used in database applications.Those unstructured/semi-structured data are important not only in servers but also in ubiquitous devices. Examples are lyrics

data in MP3 players, map data in car navigators, and multimedia data in PDAs. Thus, efficient management and search of unstructured/semistructured data will also be required of the UDBMS.

- **Security**

Since ubiquitous devices often contain personal data such as banking and healthcare data, a UDBMS needs to ensure the data security by providing access control policies.

3. Existing systems

In this section, we survey representative research prototypes and commercial products of the UDBMS and compare their functionalities.

3.1 Representative Systems

Some research groups and commercial DBMS vendors have developed UDBMSs. Table 2 shows the research prototypes and commercial products we surveyed.

Commercial products include IBM DB2 Everyplace,Oracle 10g Lite, Oracle Berkeley DB, and Microsoft SQL Server CE. Oracle Berkeley DB has been developed by University of California, Berkeley, but its
license has moved to Oracle corp.

Research Prototypes	**Commercial Products**
TinyDB, PicoDBMS, Odysseus/Mobile	IBM DB2 Everyplace, Oracle 10g Lite, Oracle Berkeley DB, MS SQL Server CE

Table 2.

Odysseus/Mobile. TinyDB has been developed at University of California, Berkeley. Pico DBMS has been developed at University of Versailles and INRIA. Odysseus/Mobile is the ubiquitous version of the Odysseus DBMS that has been continually evolving for the last 19 years at KAIST. Odysseus DBMS is tightly coupled with information retrieval (IR) and spatial database functionalities.

Odysseus/Mobile supports all the functionalities of the Odysseus DBMS and additionally supports selective convergence, data synchronization, and the flash optimized storage system (ongoing) for ubiquitous devices. Odysseus/Mobile supports selective
convergence through the architecture that allows users to choose necessary modules at compile time.

Existing UDBMSs can be categorized by target devices in which the DBMS is deployed. Table 3 shows the summary. In Table 3, it seems that sensors, smartcards, and high performance devices are different enough to justify different DBMSs.

However, we expect that the difference will become less obvious as device technology evolves, and UDBMSs that support the requirements will be needed for all those devices. For example, even in sensors, complex operations such as data mining will be needed to detect and filter out outliers in sensed data.

Target Devices	**UDBMSs**	
Extremely Small Devices with Low Computing Power	Sensors	Tiny DB
	Smartcards	PicoDBMS
Small Devices with High Computing Power	Cell Phones, PDAs, Car Navigators, and UMPCs	IBM DB2 Everyplace, Oracle 10g Lite, Oracle Berkeley DB, MS SQL Server CE, Odysseus/Mobile

Table 3.

4. Data Synchronization

In a mobile environment, data synchronization is a very important issue. However, research on data synchronization between the UDBMS and the server has been rare. Representative synchronization modules are the sync server of IBM DB2 Everyplace [IBM06], the mobile server of Oracle 10 [Ora06], and the active sync of Microsoft SQL Server CE. Commercial synchronization solutions consist of client databases on ubiquitous devices, a synchronization server, and a server database. The synchronization server controls the consistency of replicated data in the client and server databases.
Main issues on data synchronization are (1) efficiently maintaining data synchronization between a huge number of ubiquitous devices and the server, (2) resolving conflicts when there are different versions of the same data among ubiquitous devices and the server,(3) recovering from crash and restarting data synchronization when system failure occurs during data synchronization.

4.1 Unstructured/Semi-structured Data

Research on managing unstructured/semi-structured data has been active in the context of server DBMSs and will be also important in the context of UDBMSs.

There are two approaches to support unstructured/semi structured data. One is the loose coupling approach, and the other is the tight coupling approach. Commercial vendors use the loose coupling approach. In the loosely-coupled architecture, the functionality of managing the data is implemented using the DBMS API on top of the DBMS engine. Thus, the loosely coupled
architecture incurs overhead caused by the
high-level (typically, SQL-level) API calls between the unstructured/semi-structured data management module and the DBMS engine. In contrast to commercial vendors, the Odysseus DBMS uses the tight coupling
approach. In the tightly coupled architecture, the functionality of managing unstructured/semi-structured data is integrated into the DBMS engine. The tight coupling architecture eliminates the overhead caused by the high-level API calls—obtaining high performance.
Since ubiquitous devices (including PDAs and UMPCs) lack computing power to run a fully-fledged DBMS that supports unstructured/semi-structured data, research on developing a lightweight version of the unstructured/semi-structured data management module considering the specification and performance of the ubiquitous devices needs to be conducted.

5. Mobile Database

A mobile database is a database that can be connected to by a mobile computing device over a mobile network. The client and server have wireless connections. A cache s maintained to hold frequent data and transactions so that they are not lost due to connection failure. A database is a structured way to organize information. This could be a list of contacts, price information or distance travelled. The use of laptops, mobile and PDAs is increasing and likely to increase in the future .with more and more applications residing in the mobile systems.

While those same analysts can't tell us exactly which applications will be the most popular, it is clear that a large percentage will require the use of a database of some sort. Many applications such as databases would require the ability to download information from an information repository and operate on this information even when out of range or disconnected.

5.1 Need for Mobile Database

a) Mobile users must be able to work without a wireless connection due to poor or even non-existent connections.

b) Applications must provide significant interactivity.

c) Applications must be able to access local device/vehicle hardware, such as printers, bar code, scanner or GPS. units (for mapping or Automatic vehicle Location systems).

d) Bandwidth must be conserved (a common requirement on wireless networks that charge per megabyte or data transferred).

e) Users don't require access to truly live data, only recently modified data.

If your application meets any of those requirements, the chances are good that you will be required to build a mobile database application with synchronization.

5.2 Mobile database system architecture

For any mobile architecture, things to beconsidered are:
1)Users are not attached to a fixedgeographical location.
2) Mobile computing devices: low-power,low-cost, portable.
3)Wireless networks
4)Mobile computing constraints

- **Three parties**

Mobile databases typically involve three parties: fixed hosts, mobile units, and base stations.
Fixed hosts perform the transaction and data management functions with the help of database servers.
Mobile units are portable computers that move around a geographical region that includes the cellular network (or "cells") that these units use to communicate to base stations.

Base stations

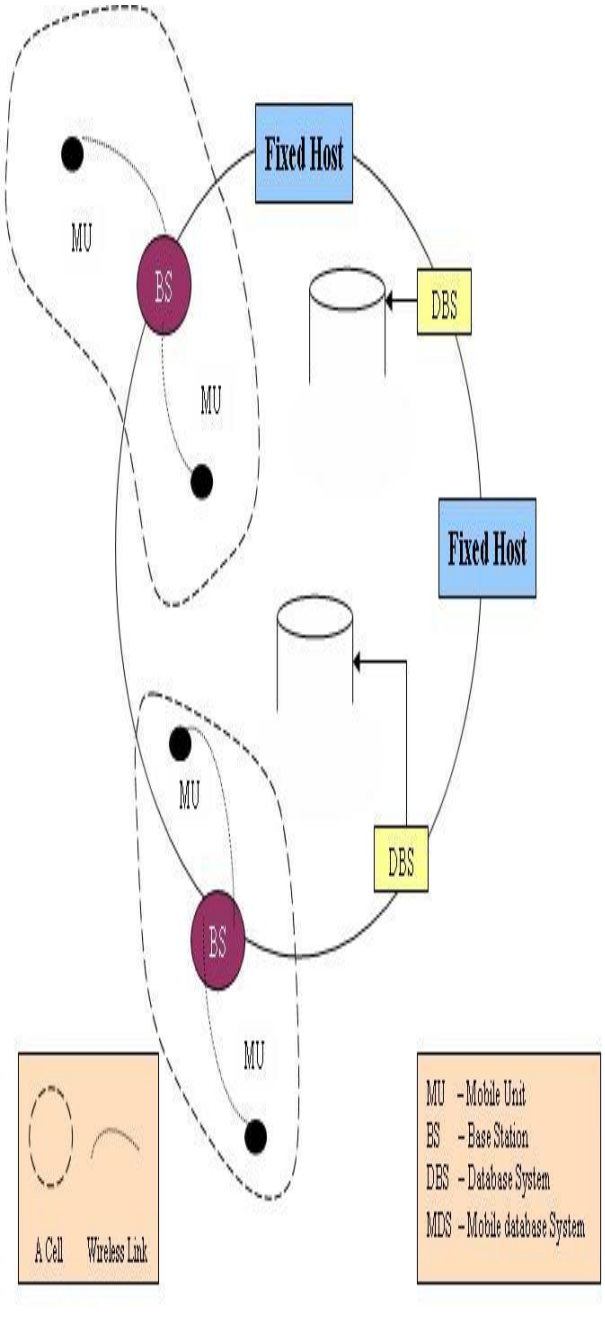
Are two-way radios, installations in fixed locations, that pass communications with the mobile units to and from the fixed hosts. They are typically low-power devices such as mobile phones, portable phones, or wireless routers. When a mobile unit leaves a cell serviced by a particular base station, that station transparently transfers the responsibility for the mobile unit's transaction and data support to whichever base station covers the mobile unit's new
locations.

Products

Sybase Inc.'s SQL Anywhere dominates the mobile-database field, with about 68 percent
of the mobile database market. IBM's DB2
Everyplace is a relational database and enterprise synchronization server thatextends enterprise applications to mobile devices. Microsoft SQL Server Compact and Oracle9i Lite are similar mobile databases.Products from lesser-known vendors, such as SQL Base from Gupta Technologies.

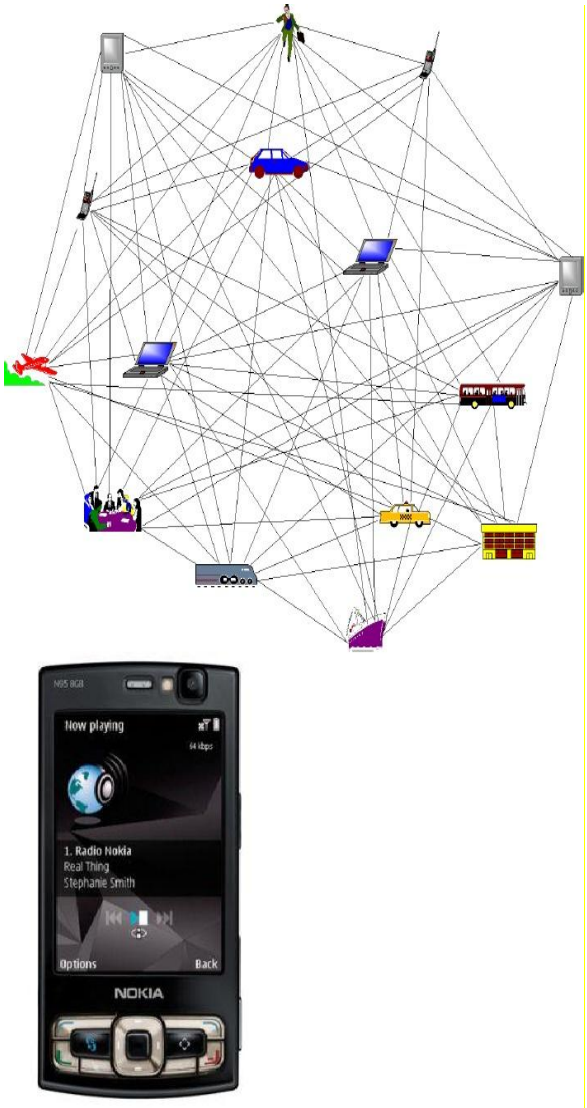
Sybase's SQL Anywhere

SQL Anywhere offers enterprise-caliber databases that scale from 64-bit servers with thousands of users down to small handheld devices. SQL Anywhere's data exchange technologies extend information in corporate applications and enterprise systems to databases running in mission-critical frontline environments. Design and management tools within SQL Anywhere enable developers to implement and deploy frontline applications and equi padministrators to easily manage and support location.



6. Mobile database Systems

- **Fully Connected Information Space**



- Each node of the information space has some communication capability.
- Some node can process information.
- Some node can communicate through voice channel.
- Some node can do both Can be created and maintained by integrating legacy database systems, and wired and wireless systems (PCS, Cellular system, and GSM).

7. Advanced Mobile Phone Service (AMPS)

AMPS was the first cellular system, which was developed during the 1970s by Bell Lab. From 1974 to 1978, a large scale AMPS trial was conducted in Chicago. Commercial AMPS service has been available since 1983.It is based on frequency division multiple access (FDMA), AMP was designed as a high capacity system based on a frequency reuse scheme. A total of 50 MHz in the 824-849 MHz and 869-894 MHz bands is allocated for AMPS. This spectrum is divided into 832 full-duplex channels using 1664 discrete frequencies, that is, 832 downlinks and 832 uplinks. In AMPS, the typical frequency reuse plan employs either a 12-group frequency cluster using omnidirectional antennas or a 7-group cluster using three sectors per base stations. Thus, there are about 50 channels per cell.

8. Mobile Security

With the rise in popularity of smart phones has come an increasing need to secure them. Since their introduction mobile phones have becoming increasingly smaller, more powerful with increasing storage capacity and have remained expensive items. With the rise of their popularity so has the need to secure the devices from theft, as well as traditional threats that effect computers such as malware and the need to back and protect the data on the devices. Although viruses are a key concern, the actual number of viruses targeting mobile phones in the wild has not been widespread.

9. Database Security

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. Traditionally databases have been protected from external connections by firewalls or routers on the network perimeter with the database environment existing on the internal network opposed to being located with in a demilitarized zone. Additional network security devices that detect and alert on malicious database protocol traffic include network intrusion detection systems along with host-based intrusion detection systems. Database security is more critical as networks have become more open. Databases provide many layers and types of information security, typically specified inthe data dictionary,
including:

- Access control
- Auditing
- Authentication
- Encryption
- Integrity controls

REFERENCES

1Arasu, A. et al., "STREAM: The Stanford Stream Data Manager," *IEEE Data Eng. Bull.*, 26(1), pp. 19-26, 2003.

2.Anciaux, N., Bouganim, L., and Pucheral, P.,"Future Trends in Secure Chip Data Management," *IEEE Data Eng. Bull.*, 30(3)

3Anciaux, N., Bouganim, L., Pucheral, P., and Valduriez, P., "DiSC: Benchmarking SecureChip DBMS," *IEEE TKDE*, 20(10), pp. 1363-1377, 2008.

4.Amer-Yahia, S., Case, P., Rolleke, T.,Shanmugasundaram, J., and Weikum, G.,"Report on the DB/IR Panel at SIGMOD 2005,"*SIGMOD Record*, 34(4), pp. 71-74, 2005.

5. Barbara, D., and Imielinski, T.Sleepers and Workaholics: CachingStrategies in Mobile Environments.Proc. ACM SIGMOD Conf.,Minneapolis, May, 1994.

6.Chrysanthis, P. K., TransactionProcessing in Mobile ComputingEnvironment, in IEEE .& Advances in Parallel and DistributedSystems, October 1993.

7. Dhawan, C. Mobile Computing.McGraw-Hill, 1997.

A New Robust And Secure Approach To SVD-3Level DWT Video Watermarking For Frame Dropiing And Some Other Attacks

Ms. Dipti Malhotra
HOD Dept. of MCA
A.C.E.T. Amritsar

Manmeet Kaur
Asst. Professor Dept. of MCA
A.C.E.T. Amritsar

***Abstract*— Digital watermarking is used to protect digital content such as images, audio and videos that have been tampered maliciously. Digital media has disadvantage of being prone to easy illegal copying methods such as tampering, piracy, fraud and counterfeiting. Digital video watermarking is a new and merging area of research to exploit different ways in order to prohibit illegal replication and exploitation of digital contents. In this paper, to maintain the quality of video and to ensure the ownership we propose a new SVD-3 Level DWT watermarking embedding technique. Singular value decomposition (SVD) is an important transform technique in robust digital watermarking .We apply the 3 level DWT and SVD on selected frames and embed the watermark into randomly selected frames with the help of secret key to authenticate the video by considering the video quality, robustness and video imperceptibility.**

Index Terms - Digital Video Watermarking, Secret Key, Scaling Factor, 3 Level DWT SVD Algorithm.

I. INTRODUCTION

In the past several years a rapid growth in multimedia (audios, videos, images) and illegal transfer of this multimedia content over the internet are becoming important issues in digital era. This leads the development of new technologies providing security to this multimedia content. Digital watermarking is used to protect this sensitive information using different watermarking technologies. Video watermarking is relatively a new technique in multimedia technology. [1] Video watermarking is the process in which watermark is embedded in a video sequence by using a secret key. The amount of information that can be embedded in the video sequence is called payload. The extraction is performed at the other end using the same secret key as shown in Fig: 1**.** The embedded watermark should be robust against variety of attacks such as Subtractive attacks, Distortive attacks, Additive attacks, Filtering, Cropping, Compression, Rotation and Scaling attacks, so that video can be protected from illegal copying and provide security against several other attacks that only performed on videos such as frame dropping, frame swapping and frame averaging [2].The two types of watermark can be used such as visible watermark and invisible watermark. We can add the watermarks either in the whole frames of video or in certain frames depending upon the requirement [3].

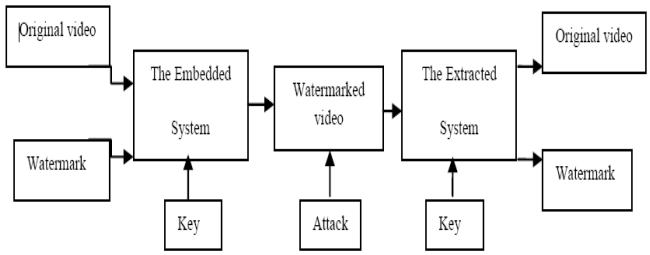


Fig. 1. A General Video Watermarking Process

[4] Video watermarking is very different from image watermarking, even though some techniques can be viewed as an extension to it. [1] [4] video watermarking is mainly used in two domains: spatial domain, frequency domain. The first category is spatial domain watermarking in which watermark is embedded in frames by directly modifying the pixel values of that frame[4]. In second category [4] Frequency domain watermarking techniques, first coefficients of transformed video frames are modified and then transformations are applied and at last the inverse process is applied to get the watermarked video. Discrete Fourier transforms (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) [5, 6, and 7] and the Singular Value Decomposition (SVD) [8, 9] is common transforms for watermarking. Watermarking is mostly used in frequency domain because of human visual system is more sensitive to low frequency coefficients and less sensitive to high frequency coefficients. [10] Depending upon the various applications, video watermarking is used in fingerprinting, copyright protection, video authentication, copy control and broadcast monitoring .Apart from these applications video watermarking systems has some properties including effectiveness, data payload, blind or informed detection, false positive rate, capacity, robustness, perceptual transparency, security, cost, sensitivity, and scalability [2].

The rest of the paper is organized as section 2 describes Related work. Section 3 describes Proposed Architecture. Section 4 describes Proposed Algorithm.Section 5 defines Experimental Results. Section 6 demonstrates conclusion.

II. RELATED WORK

A. DWT: [11] [14] It divides an image into two sections such as in lower resolutions as well as in higher resolutions. Lower resolution means LL components and higher resolution means horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low frequency part is further divided into two sections of high and low frequencies. This process is repeated number of times to compute multiple scale wavelet decomposition. [12] Proposed a method in which 3D DWT is applied using perceptual mask and embedding is performed by weighing the mark through the defined mask and then the Inverse 3D DWT (IDWT) is performed.

- Advantages: More accurate model because its properties similar to HVS and more robust to noise addition.
- Disadvantages: Higher frequencies change the quality of image.

B. SVD: It is a mathematical tool which decomposes a matrix into two orthogonal matrices and one diagonal matrix consisting of the singular values of the matrix [13]. The SVD mathematical technique provides an elegant way for extracting algebraic features from an image and improves watermark robustness and resistance against many kinds of attacks [14] [15]. SVD is a useful method to separate the system into a set of linearly independent components. A digital Image X of size MxN can be represented by its SVD as follows:

$$X = USV^T$$

$$U = [U_1, U_{22} \ldots . U_m]$$

$$V = [V_1, V_{22} \ldots . V_n]$$

$$S = \begin{bmatrix} \sigma_1 & & \\ & 0 & \\ & & \sigma_2 \end{bmatrix} \quad (2)$$

SVD is more applicable in watermarking because of following reasons:

- SVD is able to efficiently represent the intrinsic algebraic properties of an image, where singular values correspond to the brightness of the image.
- Singular values have good stability, which means a small perturbation added to an image will not significantly change the corresponding singular values.[18]

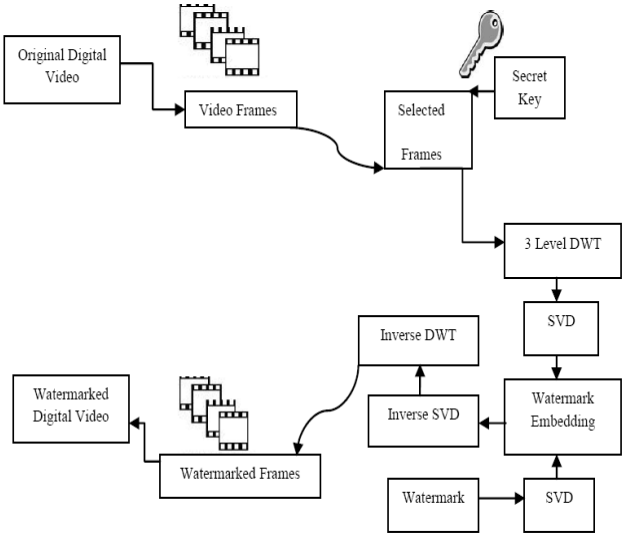


Fig. 2. Procedure of watermark embedding

III. PROPOSED ARCHITECTURE

The proposed method effectively hides the secret data into video using existing video watermarking techniques. Fig: 2 give a complete overview of data flow in proposed algorithm. This method uses some frames of video to hide the secret data. The frames selected to hide secret data are random frames and not sequential frames. Hence each frame that contains the secret data can be identified using secret key, a 10 digit number provided by user. The selection of frames is done by using several functions that are made up from secret key. So, watermark is embedded in whole video and not in some parts of video. We also set up a passkey identifier to give only four trials to the user and if the user inserts more than 4 wrong keys then it means he/she is trying to find out the watermarked frames by trying random keys. If four wrong entries are made by user then the video will be damaged leaving no data behind.

IV. PROPOSED ALGORITHM

In this section, we have discussed some motivating factors in the design of our approach to video watermarking. We have used DWT and SVD for developing the algorithm. Among various tools, SVD and DWT are more reliable in digital watermarking. Due to the fact of localization in both spatial and frequency domain, wavelet transform is the most preferable transform among all other transforms. After converting the video into frames, we have applied 3 levels DWT on selected frames. In the next stage, the SVD is applied to selected sub-bands and embed the same original watermark by modifying the singular values. Embedded watermark in middle frequencies increases the robustness to variety of attacks. The procedure of embedding a digital watermark into the original video is depicted in Fig: 2. After that, inverse SVD and inverse DWT is applied in order to reconstruct the

watermarked digital video. After getting the watermarked video the extraction process is performed at other end in order to check the extracted watermark resembles with original one or not.

A. Watermark embedding algorithm

- Apply DWT to the selected frames repeatedly up to the third level.
- Perform SVD transform on approximation and all the detail parts in third level of wavelet transform, $f_Q = U_Q S_Q V^T$ Where Q ∈ {LL3, LH3, HL3, HH3}.

$$f_Q = U_Q S_Q V^T \quad (1)$$

- Perform SVD transform on watermark,

$$W = U_W S_W V^T{}_W \quad (2)$$

- In general, embedded watermark at this stage. Modify the singular values of approximation and all the detail parts with the singular values of the watermark as:

$$\gamma_Q^* = \gamma_Q + \alpha_Q \gamma_W \quad (3)$$

- Here, is scale factor of combined transform, which value is 0.04.
- Take inverse combined transform and reconstruct the watermarked video.

B. Watermark extraction algorithm

- Apply DWT to selected watermarked frames repeatedly up to the third level.
- Apply SVD transformation on approximation and all details parts up to the third level of wavelet transform, Where Q ∈ {LL3, LH3, HL3, and HH3} and get the combined transform coefficient γ_Q^*
- Extract singular values of watermark from approximation and all detail parts.

$$\gamma_{W^*}^Q = \frac{\gamma_Q^* - \gamma_Q}{\alpha_Q} \quad (4)$$

- Extract the watermark from video frames.

$$W_Q^* = U_W S_Q^* V_W^T \quad (5)$$

- After detecting all estimates of watermark, sum up all these estimates and normalized $\overline{W_Q^*}$ between [0, 1].
- Reproduced the watermark,

$$W_Q^* = \sum_{i=1}^{Q} w_Q^* \quad (6)$$

V. EXPERIMENTAL RESULTS

The main focus of this algorithm is its dynamic and key dependent frame selection technique [3]. We have implemented and experiment it using MATLAB (matrix laboratory) which is a multi-paradigm numerical computing environment and fourth-generation programming language. The experimental results are as below which show original frames and corresponding watermarked frames. We test the proposed watermarking algorithm with different variations using colored host video clips. Each video clip is partitioned into different number of frames. We employed "Rhinos" video sequence in AVI format where total number of frames we calculated is 114 and selected 10 random frames to embed watermark such as "logo1.png" of size (128 × 128) in that frames as shown in Fig: 4. The 10 random original frames are shown in Fig: 3 and their corresponding watermarked frames are shown in Fig: 5. Watermarked Video quality was estimated by SSIM, PSNR, BER and MSE.

Fig. 3. Original Frames

Fig. 4. Watermark Image

Video	Frame no.	SSIM	PSNR	BER	MSE
Rhinos	6	0.99	52.70	0.01	0.12
	13	0.99	53.20	0.01	0.12
	24	0.99	53.31	0.01	0.12
	42	0.99	52.77	0.01	0.12
	46	0.99	52.35	0.01	0.12
	61	0.99	52.63	0.01	0.12
	70	0.99	52.97	0.01	0.12
	88	0.99	53.92	0.01	0.12
	94	0.99	53.44	0.01	0.12
	106	0.99	53.16	0.01	0.12

Fig. 5. Watermarked Frames

TABLE I. CALCULATED VALUES OF SSIM,PSNR,BER AND MSE OF WATERMARKED VIDEO

We then tested the robustness and quality of watermarked video using a scaling factor 0.04 and different performance evaluation metrics. For each frame we have calculated the SSIM, PSNR, MSE and BER as shown in above Table I.

A. To check the imperceptibility of watermarked video:

The PSNR is a quality metric used to determine the degradation in the embedded image with respect to the host image or also defined as ratio between maximum power of a signal and power of distorted signal [16]. It is most easily defined via the mean squared error (MSE) as:

$$PSNR = 10log_{10}\frac{L*L}{MSE}$$

The MSE [16] defined it as average squared difference between a reference image and a distorted image. It is calculated as:

$$MSE = \frac{1}{XY}\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j) - e(i,j))^2$$

The BER [16] defined it as the ratio that describes how many bits received in error over the number of the total bits received. It is often expressed as percentage and calculated by comparing bit values of embedded image and cover image.

$$BER = P/(H * W)$$

The SSIM is a method for measuring the similarity between two images. SSIM is designed to improve on traditional methods like peak signal to noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human eye perception. It is calculated by formula given below:

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}$$

The value calculated shows that propose DWT-SVD based video watermarking algorithm is imperceptible. The calculated PSNR value is 53.05db which shows quality of watermarked video appear visually identical to the original one and there is no degradation in visual quality. The value calculated for SSIM is 0.99 which shows the structural similarity between original video and watermarked video.

In order to check the quality of extracted watermark, the normalized Cross-correlation (NC) value between the original watermark and extracted watermark is calculated for different frames using scaling factor 0.04, which is defined as:

$$NC = \frac{\sum_{i=0}^{M1}\sum_{j=0}^{M2}[W(i,j)W'(i,j)]}{\sum_{i=0}^{M1}\sum_{j=0}^{M2}[W(i,j)]^2}$$

Where W and W` represent the original image and extracted watermark image, respectively. The watermark extraction using scaling factor 0.04 is shown in Fig: 6 which show that correlation value of extracted watermark is near to 1 and extracted watermark is same as original one. The values of PSNR, MSE, SSIM and BER for 10 random frames are calculated as shown in Fig: 6, Fig: 7, Fig: 8 and Fig: 9.Also the correlation coefficient of extracted watermark is shown in Fig: 10.

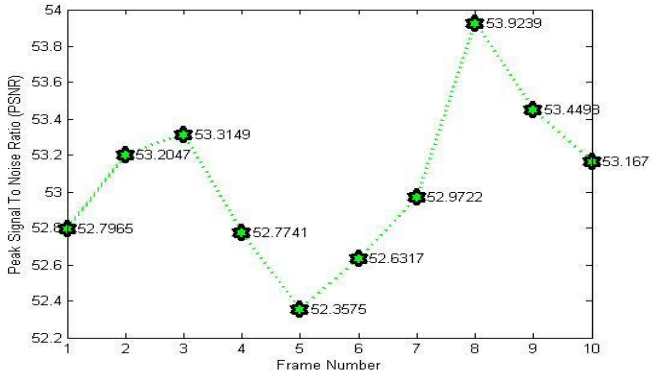


Fig. 6. PSNR values of watermarked video for 10 frames

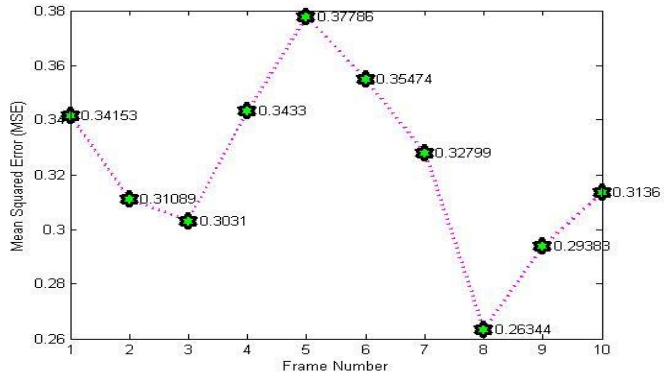


Fig. 7. MSE values of watermarked video for 10 frames

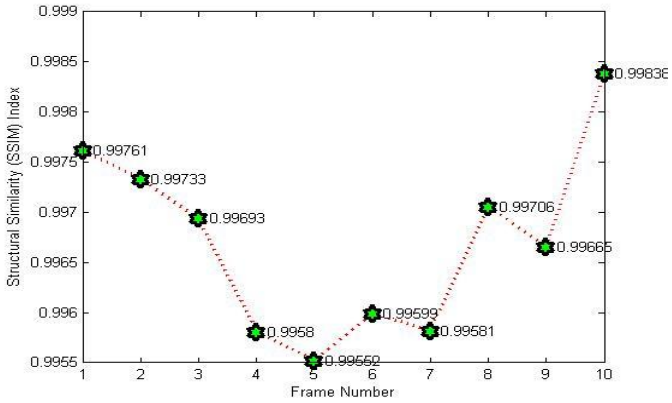


Fig. 8. SSIM values of watermarked video for 10 frames

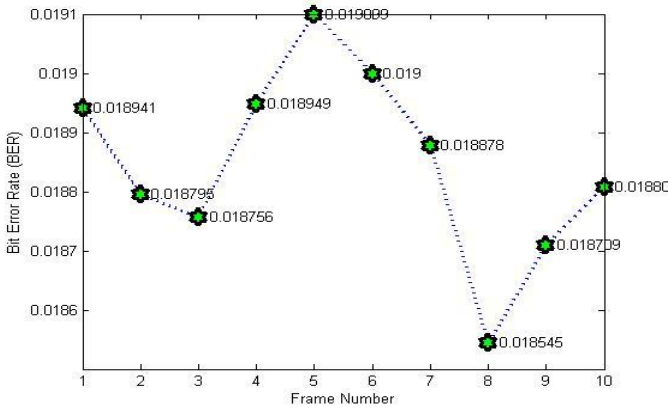


Fig. 9. BER values of watermarked video for 10 frames

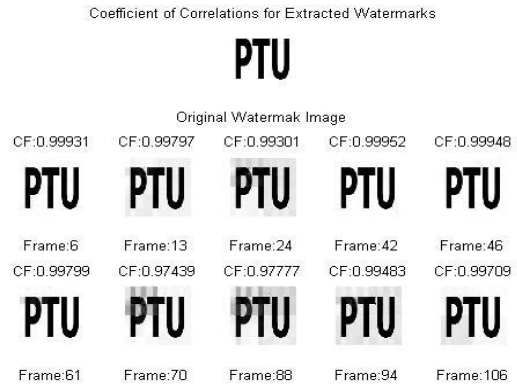


Fig. 10. Corelation coefficient of extracted watermark with scaling factor 0.04

B. Choice of appropppriate scaling factor:

It is actually a hard step for choosing the suitable scaling factor.Usually, the scaling factor is chosen to be a scalar value. In most of literature the scaling factor is chosen between 0 and 1[17].Table II shows the SSIM, PSNR, MSE ,BER of the watermarked video and the correlation coefficient (NC) of the extracted watermark for several scaling factors. From this table, the higher scaling factor is, the worse the robustness and invisibility of watermark will be.

TABLE II. AVERAGE VALUES OF SSIM,PSNR,BER AND MSE FOR WATERMARKED VIDEO AND EXTRACTED WATERMARK USING VARIOUS SCALING FACTORS

Different parameters of watermarked video and Normalized Cross-Correlation values for extracted watermark						
Video	**Scale factor .**	**SSIM**	**PSNR**	**BER**	**MSE**	**NC**
Rhinos	0.9	0.9151	38.557	0.02	9.08	0.92
	0.5	0.9539	40.509	0.02	5.80	0.95
	0.1	0.9960	50.122	0.19	0.63	0.98
	0.04	0.9992	53.05	0.01	0.12	0.99

C. To check the robustnessof extracted watermark:

To check the quality of extracted watermark we applied several attacks on 10 random frames in which the watermark is inserted. The attacks applied are Gaussian attacks, speckle attacks, salt& pepper attacks, scaling attacks, blur, Gaussian filtering and circular filtering. The calculated normalization correlation coefficient for different attacks is shown in Table III.

TABLE III. CORELATION COEFFICIENT VALUE UNDER VARIOUS ATTACKS.

Attacks	**Correlation Coefficient**
Gaussian Noise (mean=0, var=0.001)	0.97
Speckle Noise (mean= 0,var=0.001)	0.97
Salt & pepper (d=0.01)	1

Scaling [256 256]	0.95
Blur	1
Circular filtering(radius=5)	1
Gaussian filtering [5 5], σ =0.l	1

VI. CONCLUSION

The proposed algorithm is more secure than the conventional algorithms due to the use of an encryption key for the selection of the random frames to be watermarked. And at time of extraction process same encryption key is needed and if key is wrong then nobody can find the watermarked frames. The values of correlation factor between the extracted watermark and original watermark after these various attacks is closer to 1 or almost one which shows that proposed method is robust to various attacks. The calculated values of parameters show the high imperceptibility of the algorithm. Also the algorithm is simple blind algorithm, more secure and highly robust against frame dropping because of random frames & other manipulations.

ACKNOWLEDGMENT

This is to express my sincere gratitude to Dr. Satvir Singh, Associate Professor, Department of Electronic & Communication Engineering, SBS State Technical Campus, Ferozepur (Punjab), India, for sparking in me the enthusiasm and initiative to discover and learn. I am truly thankful to him for guiding me through the entire paper and being as a motivator in this learning curve.

REFERENCES

[1] Jayamalar, T and Radha, V, "Survey on digital video watermarking techniques and attacks on watermarks," *International Journal of Engineering Science and Technology*, vol. 2, Pp. 6963-6967, 2010.

[2] Potdar, Vidyasagar M and Han, Song and Chang, Elizabeth, "A survey of digital image watermarking techniques," *Industrial Informatics*, 2005.

[3] Madia, Jigar and Dave, Kapil and Sampat, Vivek and Toprani, Parag, "Video Watermarking using Dynamic Frame Selection".

[4] Doerr, Gwena and Dugelay, Jean-Luc, "A guide tour of video watermarking*," Signal processing: Image communication, Elsevier*, vol. 18, Pp.263-282,2003.

[5] Tay P, Havlicek JP. "Image watermarking using wavelets", Pp. 258–261, 2002.

[6] Kundur D, Hatzinakos D., "Digital watermarking using multi-resolution wavelet decomposition".*Int Conf Acoust Speech Signal Proc*, Pp. 2969–72, 1998.

[7] Wu C, Zhu W-P Swamy MNS. , "A watermark embedding scheme in wavelet transform domain". *In: IEEE Region 10 Conference Proceedings: Analog and Digital Techniques in Electrical Engineering*, vol. A, Pp.279–82, 2004.

[8] Loukhaoukha K, " Chouinard J-Y, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification." *In: IEEE.* Pp .177–82, 2009.

[9] Gorodetski V, Popyack L, Samoilov V, Skormin V. "SVD based approach to transparent embedding data into digital images," *In: Proc. International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS'01).* 2001.

[10] Lu, Gaoyan and Zhang, Yongping and Liang, Fengmei and Zheng, Dechun,"Survey of Video Watermarking**"** *Video Engineering*,vol.21, Pp .009,2012

[11] Sinha, Sanjana and Bardhan, Prajnat and Pramanick, Swarnali and Jagatramka, Ankul and Kole, Dipak K and Chakraborty, Aruna," Digital video watermarking using discrete wavelet transform and principal component analysis," *International Journal of Wisdom Based Computing*,vol.1, Pp 7--12, 2011.

[12] Campisi, Patrizio and Neri, Alessandro," Video watermarking in the 3D-DWT domain using perceptual masking*," IEEE*, vol.1, Pp.I--997, 2005.

[13] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T. Wu, Y.-C. Hsu, "On svd-based watermarking algorithm*," Applied Mathematics and Computation* Pp 54–57, 2007.

[14] Preda, Radu O and Vizireanu, Dragos N," A robust digital watermarking scheme for video copyright protection in the wavelet domain," *Measurement , Elsevier*,vol. 43, Pp 1720—1726,2010.

[15] Rastegar, Saeed and Namazi, Fateme and Yaghmaie, Khashayar and Aliabadian, Amir," Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform,"*AEU-International Journal of Electronics and Communications*, vol. 65, Pp 658—663,2011.

[16] A. K. Singh, N. Sharma, M. Dave, A. Mohan, "A novel technique for digital image watermarking in spatial domain," *in: Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, IEEE*, pp. 497–501, 2012.

[17] Mohammad, Ahmad A and Alhaj, Ali and Shaltaf, Sameer, "An improved SVD-based watermarking scheme for protecting rightful ownership," *Signal Processing Elsevier*, vol. 88, Pp 2158—2180,2008.

[18] Rajab, Lama and Al-Khatib, Tahani and Al-Haj, Ali, "Hybrid DWT-SVD video watermarking," *Innovations in Information Technology, 2008. IIT 2008. International Conference on, IEEE*, , Pp 588--592,2008.

A REVIEW ON UNDERWATER WIRELESS SENSOR NETWORKS

Er.AnudeepKaur
M.Tech Research
Scholar
Amritsar College of Engg. & Technology

Dr. Tanupreet Singh
Professor and Head of Department
Of Electronics and Communication
A.C.E.T. Amritsar

ABSTRACT:-**In this paper, an overview of various underwater wireless sensor networks has been discussed. Moreover the survey has been done on the work of the various researchers. Underwater wireless sensor networks (UWSNs) have pulled in a quickly developing interest from researchers amid the last few years. Because of the points of interest of simple deployment, self-management, and no necessity for infrastructure, UWSNs can be connected to an extensive variety of aspects, for example naval surveillance, earthquake and tsunami forewarning, atmosphere and sea observation, and water pollution tracking. UWSNs have different characteristics for eseatransmission, and high error rate since acoustic signals are utilized for communications, instead of radio signals. It has been concluded from the survey that none of the technique is very much efficient for UWSN. So the paper has been concluded with a future scope to overcome this issue.**

KEYWORDS:- Underwater Wireless Sensor Networks, VBF, HH-VBF

1.INTRODUCTION

On the earth, 71% of the surface is secured with seas; this massive region contains bounteous assets and different animals. In any case contrasted and the terrestrial environment, one knows simply not very many about the nature's turf. As more individuals turn their center to the seas, there has been developing enthusiasm toward inquires about of this field. Nonetheless, the seas environment is so eccentric and risky that a large portion of the submerged ranges are the place individuals can't reach by and by. Individuals spontaneously think about the sensor systems which have been broadly utilized within nature. The sensor systems have been quickly connected in seas, which are precisely the underwater wireless sensor systems (Uwsns).

Underwater wireless sensor systems (Uwsns) have pulled in a quickly developing enthusiasm from specialists amid the last few years. Because of the advantages of easy deployment, self-management, and no need for infrastructure, Uwsns can be connected to an extensive variety of perspectives, for example, as naval surveillance, earthquake and tsunami forewarning, climate and ocean observation, and water pollution tracking. In these applications, every node needs to work together with others in sensing occasions of enthusiasm by exchanging obtained information. To make the information gathered from sensor nodesmeaningful, the positions of related nodes are oftenrequired. As of late, different nodelocalization algorithms for Uwsns have been proposed.

Not the same as terrestrial sensor systems, UWSNs have unique attributes, for example, high propagation delay, restricted transfer speed, and high error rate since acoustic signs are utilized for communications, instead of radio signs [1, 2]. Hence, their communication protocols for UWSNs should be developed to take into account these characteristics. In UWSNs, flooding-based routing protocols are favored because of their capacity of lessening the routing overhead as far as no need of way setup and support. Additionally, these routing protocols can expand the packet delivery ratio by permitting different duplicates of a packet to achieve the sink along diverse ways.

1.1 Challenges of underwater wireless sensor networks

The design of underwater wireless sensor networks may be confronted by many challenges like:

- Available bandwidth is extremely limited.
- Underwater channel is severely impaired, particularly because of multi-path and fading.
- Propagation delay in underwater is five orders of magnitude higher than in radiofrequency (RF) terrestrial channels, and extremely variable.
- High bit error rates and temporary losses of connectivity (shadow zones) can beaccomplished, because of the extreme qualities of the underwater channel.
- Battery power is constrained and typically batteries cannot be energized, also because solarenergy cannot be misused.

- Underwater sensors are prone to failures because of fouling and corrosion.

2.UNDERWATER SENSOR NETWORK ARCHITECTURE

UWSN architectures can be classified in several ways. One classification discriminates between static, semi-mobile,and mobile architectures,another popular UWSN classification method is to divide UWSNs into two-dimensional(cover ocean floor) and three-dimensional (includes depth as a dimension),UWSN can also be single-hop, multi-hop,or hybrid (single-hop individual sensors, multi-hop clusters) [1]. Architectures can be grouped into short-term, time-criticalapplications, and long-term, non-time-critical applications.RF, optical, and acoustic wave based architectures areanother way to look at the available UWSNs[2].

Fig. 1 shows the most common UWSN architecture. The individual nodeshas been anchored at the ocean floor. They areusually smaller in size, battery operated, and they mostly transmit data via acoustic modems. The cluster heads are alsoanchored to the ocean floor. In addition to having acoustic modems. Cluster heads are equipped with acoustictransceivers,namely a *vertical* and a *horizontal* transceiver[1]. The horizontal transceiver is used by the cluster head oruw-sink to communicate with the sensor nodes in order to[3]: i) send commands and configuration data to the sensors. This communication will happening between underwater sink or cluster head to sensors. ii) collect monitored data. This communication will happening between sensors to cluster head or sink. Cluster heads communicate via horizontal acoustic modes with all other individual nodes within the cluster. The data transfer from node to cluster head can be single-hop (each node communicated to the cluster head directly) or multi-hop. In case of multi-hop paths, as in terrestrial sensor networks [6], the data produced by a source sensor is relayed by intermediate sensors until it reaches the uw-sink. This results in energy savings and increased network capacity but increases the complexity of the routing functionality as well.The vertical transreceiver is used by the uw-sinks to relay data to a *surface station[1]*. Vertical transceivers must be long range transceivers for deep water applications as the ocean can be as deep as 10 km. The surface station is equipped with an acoustic transceiver that is able to handle multiple parallel communications with the deployed uw-sinks. Finally base or suRface station will send the sensed data to on-shore base station via RF signal[3].

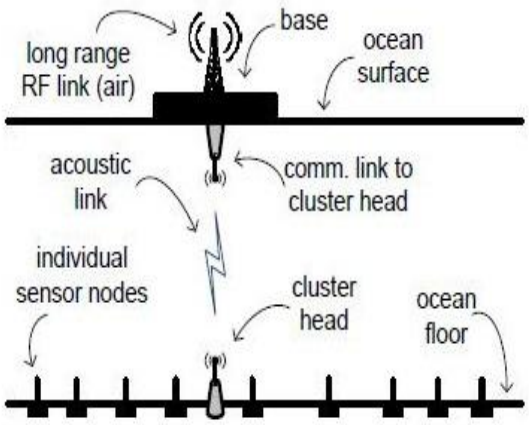


Fig1. 2D architecture of underwater sensor network [1]

Unlike TWSNs, the hardware of the cluster head node is dissimilar from all other nodes, as it has additionalfunctionalities such as a direct communication link with the ocean surface. Hence, a TWSN's cluster headswitching feature (which increases the overall network lifetime by efficiently distributing the power consumptionamong nodes) cannot be utilized inUWSNs. Also, the cluster head is potentially the most security-vulnerablecomponent in UWSNs military applications, because it is a single point of failure node [1].

Fig. 2 shows an alternative 3D UWSN architecture.Three dimensional underwater networks are used to detect andobserve phenomena that cannot be adequately observed by means of ocean bottom sensor node,i.e.,to performcooperative sampling of 3D ocean environment[1].

In 3D architecture,sensor node float at different depth in order to observe the given phenomenon. In this architectureeach sensor is anchored to the ocean bottom and equiped with a floating buoy that can inflate by a pump.The buoypushes the sensor towards the ocean surface. The depth of sensor then can be regulated by adjusting the length of wirethat connect the sensor to the anchor, by means of an electronically controlled engine that reside on sensor[4]. 3D architecture can have all nodes directly communicate to the surface base or can have only cluster headscommunicate directly to the base. In the former case, all nodes are of the same type, but communication might be moreenergy intensive than that of the cluster head approach. The cluster head approach requires only the cluster head tocarry a long-range communicationmodem. On the other hand, the clustered approach is vulnerable to single point of failure[1]. Military applications areextremely sensitive to single point of failure hardware components.

In 3D architecture ,sensor node float at different depth in order to observe the given phenomenon. In this architectureevery sensor is anchored to the ocean bottom and equiped with a floating buoy that can inflated by a pump.The buoypushes the sensor towards the ocean surface. The depth of sensor then can be regulated by adjusting the length of wirethat connect the sensor to the anchor,by means of an electronically controlled engine that reside on sensor.[4]3D architecture can have all nodes directly communicate to the surface base or can have only cluster headscommunicate directly to the base. In the former case, all nodes are of the same type, but communication might be moreenergy intensive than that of the cluster head approach. The cluster head approach requires only the cluster head tocarry a long-range communication modem. On the other hand, the clustered approach is vulnerable to single point offailure[1]. Military applications are extremely sensitive to single point of failure hardware components.

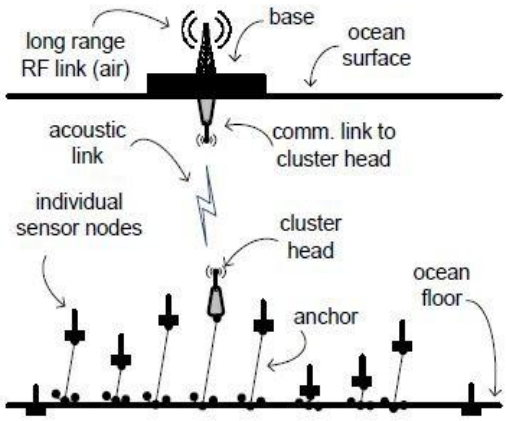


Fig 2: 3D architecture of underwater sensor network [1]

3.UNDERWATER IMAGE ENHANCEMENT TECHNIQUES

3.1 VBF

VBF is a location-based routing approach for UWSNs [5]. In this protocol, state information of the sensor nodes is not required since only a small number of nodes are involved during packet forwarding. Data packets are forwarded along redundant and interleaved paths from the source to the sink, which helps handling the problem of packet losses and node failures. It is assumed that every node previously knows its location, and each packet carries the location of all the nodes involved including the source, forwarding nodes, and final destination [6]. The forwarding path is specified by the routing vector from the sender to the target. As soon as a packet is received, the node computes its relative position with respect to the forwarder. Recursively, all the nodes receiving the packet compute their positions. If a node determines that it is close enough to the routing vector, it puts its own computed position in the packet and continues forwarding the packet; else, it simply discards the packet. In this way, all the packet forwarders in the sensor network form a "routing pipe", the sensor nodes in this pipe are eligible for packet forwarding, and those which are not close to the routing vector do not forward. Fig. 3 illustrates the basic idea of VBF.

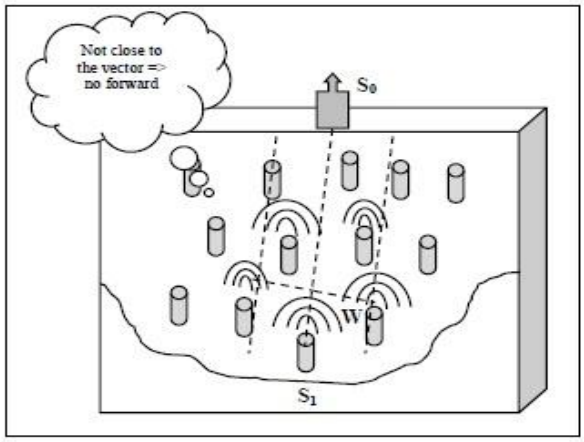


Fig 3.VBF routing protocol for UWSNs. [6]

VBF has many essential drawbacks. First, using a virtual routing pipe from source to destination can affect the routing efficiency of the network with different node densities. In some spaces, if node deployment is sparser or become sparse due to some node movement, then it is possible that very few or even no node will lie within that virtual pipe, which is responsible for the data forwarding; even it is possible that some paths may exist outside the pipe. Eventually, this will result in small data deliveries in sparse spaces. Second, VBF is very sensitive about the routing pipe radius threshold, and this threshold can affect the routing performance significantly; such feature may not be desirable in the real protocol developments. Furthermore, some nodes along the routing pipe are used again and again in order to forward the data packets from sources to the sink, which can exhaust their battery power.

3.2 Robustness Improved Location-Based Routing for Underwater Sensor Networks (HH-VBF)

The need to overcome two problems encountered by the VBF, i.e., small data delivery ratio in sparse networks, and sensitivity to the routing pipe's radius, the HH-VBF (hop-by-hop VBF) is proposed by Nicolaou et al. [7]. HH-VBF forms the routing pipe in a hop-by-hop method, enhancing the packet delivery ratio significantly. Although it is based on the same concept of routing vector as VBF, instead of using a single virtual pipe from the source to the sink, it defines a different virtual pipe around the per-hop vector from each forwarder to the sink. In this protocol, each

node can adaptively make packet forwarding decisions based on its current location [6]. This design can directly bring the following two benefits: First, since each node has its own routing pipe, the maximum pipe radius is the transmission range. Second, in sparse networks, HH-VBF can find a data delivery path even so the number of eligible nodes may be small, as long as there exists one in the network.

In HH-VBF, the routing virtual pipe is redefined to be a per-hop virtual pipe, instead of a unique pipe from the source to the sink [7]. When some areas of the network are not occupied with nodes, for example there exist "voids" in the network, even a self-adaptation algorithm may not be able to route the packets. In such a case, a forwarder is unable to reach any node other than the previous hop. Although simulation results show that HH-VBF considerably produces better results for packet delivery ratio, but still it has an inherent problem of routing pipe radius threshold, which can affect its performance. Moreover, due to its hop-by-hop nature, HH-VBF is not able to add a feedback mechanism to detect and avoid voids in the network and energy efficiency is still low compared to VBF[7].

3.3 VBVA Routing Protocol

Xie et al. [8] introduce a Vector-Based Void Avoidance (VBVA) routing protocol, which extends the VBF routing protocol to handle the routing void problem in UWSNs. VBVA assumes two mechanisms, vector-shift and back-pressure. The vector-shift mechanism is used to route data packets along the boundary of a void. The back-pressure mechanism routes data packets backward to bypass a concave void. VBVA handles the routing void problem on demand and thus does not need to know network topology and void information in advance. Hence, it is very robust to cope with mobile voids in mobile networks. Simulation results in [8] show that VBVA can handle both concave and convex voids effectively and efficiently in mobile underwater sensor networks only when these voids are inside the forwarding pipe, while the voids outside the forwarding pipe is not solved by VBVA.

3.4 ES-VBF

To solve the energy problem in UWSN, Bo et al.[9] put forward an energy-aware routing algorithm, called Energy-Saving Vector-Based Protocol (ES-VBF). The main purpose of this routing protocol is saving energy. ES-VBF takes both residual energy and localization-based information into consideration while calculating the desirableness factor as in (3), which allows nodes to weigh the benefit for forwarding packets. The ES-VBF algorithm modifies the calculation of the desirableness factor of (1) for VBF protocol to be calculated if the node residual energy is smaller than 60% of initial energy.

3.5 L1-ABF PROTOCOL

The angle-based flooding approach is used in this proposed routing protocol. This routing mechanism is not based on sensor node location information and has been designed for delay and power efficient multi-layer communication in underwater acoustic networks. In this routing mechanism, there is no need for a sender node to know its own location or the location of the final destination (Sink) before transmitting the data packets. Anchor nodes flood the sensed data towards the surface sinks via the upper layer nodes. The forwarder node will define the flooding zone by using the initial angle $\Theta = 90 \pm 10K$. Here, K is a variable and has a finite set of values, K, (1, 2…..8). After defining the flooding zone, the node will send Hello Packets (HP) within the defined zone and wait for the Hello Reply (HR). If there is no HR received, the node will increase the value of K in the initial angle, to increase its flooding zone until the basic condition is met ($0 < \Theta < \pi$). Here, it assumes that after the completion of one round by using the different values of the variable k and the node did not receive any Hello Reply, the nodes can send data packets directly to the sink nodes on the maximum power. Here, it is important to note that nodes can use random values of the variable K to increase the size of the flooding zone. The randomness of the K value is more helpful to control the End-to-End delays as well as the power consumption of the nodes. The selection of the random values for K depends on the movement of the nodes.

4. RELATED WORK

R. Rachman et al. [10] has indicated systems reproduction. System Simulator (Ns2) that has been utilized was NS 2.30. For this situation, there were 6 hubs where there was one hub as principle or focal hub. Two hubs would be set moving haphazardly movement from the source hub while three hubs would be set static. This recreation measure the vitality utilization in examination with the information parcel. There were a few parameters that they utilized within their case, comprised of Bit rate, Delay, Frequency, and so on. They gave the general situation to setup of the submerged environment for their reenactments. R.zandi et al. [11] proposed an Autonomous Underwater Vehicle (AUV) based restriction calculation that utilized four directional acoustic shafts with settled edges on AUV to telecast messages occasionally. These messages contained current position of AUV and ID of the transmitter bar. The latent sensors got these messages and discovered two of them issued by diverse progressive shafts in one side of AUV way that they put on the middle lines (most noteworthy force segment) of these two distinctive

transmitter bars. These two messages were utilized to gauge the sensors position. Significant focal point of this technique was being noiseless that prompt vitality effectiveness and no need time synchronization among sensor hubs. Execution of the proposed confinement system was assessed by reenactments, utilizing MATLAB. Reenactment results demonstrated that limitation precision and effectively of the proposed system by picking ideal estimation of parameters, for example, transmission interim, shaft width and fulfilling scope state of all sent sensor hubs was high. J.iqbal et al. [12] has expected to address such sort of vulnerabilities and nearly inspect even minor varieties happening in sign lessening in instances of circular and tube shaped spreading. These varieties had been tended to by utilizing a scientific displaying procedure as `gradient Estimation Vector'. It was the system for efficiently changing parameters in a model to focus the impacts of such changes. Inclination Estimation Vectors really portrayed the sign weakening all the more decisively alongside the varieties and vulnerabilities included. M. Waldmeyer et al. [13] displayed a multi-stage AUV-supported restriction plan for Uwsns. The proposed strategy consolidated the adaptability and restriction exactness of an AUV-supported confinement, the vitality proficiency of "quiet limitation" and enhanced confinement scope with k-stage limitation focused around sensor hubs. They assessed the execution of the proposed plan as far as the confinement scope, exactness and correspondence expenses utilizing reproductions. They demonstrated that while enhanced execution with various stages was exchanged off with higher correspondence costs as a rule, the last can be minimized while keeping up great execution with a proper decision of the acoustic correspondence range. C. Keyu et al. [14] exhibited the improvement of MAC conventions in Uwsns, this paper reviews the current state-of-the-craftsmanship MAC conventions for Uwsns. In the early improvement, the execution as far as postponement and throughput of the Uwsns had been the real concern of the MAC layer convention outline. Later, the outline of vitality productive MAC conventions turned into another exploration center on the grounds that sensor hubs were for the most part fueled by batteries which were more averse to be revived. In this paper, they initially depicted the submerged acoustic environment and the difficulties to the MAC conventions plan in Uwsns. They then gave a relative investigation of a few sorts of MAC conventions as indicated by present existing various usage. Besides, open exploration issues would be abridged. Assuredly, this study would motivate more dynamic research around there. K.m. Pouryazdanpanah et al. [15] examined that vitality productivity was a test in submerged remote sensor system. Double sinks vector based sending (DS-VBF) took both leftover vitality and area data into thought as need components to find an enhanced steering way to spare vitality in submerged systems. The adjusted steering convention utilizes double sinks on the water surface which enhances system lifetime. As indicated by arrangement of double sinks, bundle conveyance proportion and the normal end to end deferral were improved. In light of their reenactment brings about examination with VBF, normal end to end postponement diminished more than 80%, remaining vitality expanded 10%, and the addition of bundle gathering proportion was around 70%. A. Tariq et al. [16] proposed a solid model with the name of 3 Hop-Reliability Model (3h-RM), in which each sender hub of each one gathering of three layers would keep up the duplicate of same effective exchanged information parcels without making additional trouble on the systems. Reenactment results demonstrated that 3h-RM could attain better conveyance degrees as contrasted with 2h-ACK unwavering quality model without utilizing any extra assets and designs. Acoustic channel attributes were made a numerous issues like, low transfer speed; long proliferation deferrals and high slip channel rates that can result in to hamper the proficiency of Uwsns. With these obligations, it was exceptionally troublesome errand to outline a steering convention which had the capacity to augment the unwavering quality of these systems. K. Li et al. [17] figured the visit arranging of an information donkey gathering sensor information in Uwsns as a vitality obliged bi-objective advancement issue termed the Underwater Data Muling Problem (UDMP). UDMP had the two clashing targets of minimizing the length of a visit and expanding the quantity of sensors reached, while fulfilling the vitality requirement of the information donkey at all times. They outlined an estimate calculation to comprehend one exceptional instance of this NP-hard issue, which processed a set of Pareto-productive arrangements tending to the tradeoff between the two streamlining targets to make fitting visit arranging. Reenactment results accepted the viability of this calculation. A.davis et al. [18] exhibited an outline of Uwsns, their applications, and their difficulties. They additionally introduced a study of different UWSN architectures presently utilized as a part of conveyed UWSN frameworks. Various applications exploited minimal effort, little estimated, effortlessly configurable and adaptable TWSN hubs to screen, locate, and track different natural phenomena and occasions. The late headway in hardware and sensor scaling down and low-control advances empowered Twsns to expand their compass to submerged applications. Submerged remote sensor systems (Uwsns) can be utilized within a lot of people new applications. Yet, Uwsns advancement was reliant on various mechanical difficulties that need to be succeed.L. Sungwon et al. [19] required another steering convention which considered the attributes of submerged limitation to help bundle transmissions from both confined hubs and unlocalized hubs to the sink. In this paper, they proposed an Underwater Hybrid Routing Protocol (UHRP) which had the half and half gimmicks of flooding-based

directing conventions and touchy specially appointed steering conventions, taking into account our new steering metric. What's more, the extended ring pursuit method was reconsidered to be connected to diminish directing overhead in nature's domain. Q.zhang et al. [20] considered the impact of hub topology on the target following in Uwsns. Firstly, by utilizing the learning of geometry, the impacts of four common topologies on target following focused around Uwsns were broke down qualitatively. The four commonplace topologies incorporated four hubs structure a square, four hubs were in line, four hubs were near one another, and four hubs structure a standard tetrahedron. Besides, to assess the self-assertive topology, the relationship between the back Cramer-Rao lower bound (PCRLB) and hub's position was determined. Thirdly, their target following plan comprised of the ideal topology choice plan by minimizing PCRLB, the ideal combination focus determination conspire by minimizing vitality utilization, and the multi-sensor molecule channel (PF) was outlined. Last, reenactment results demonstrated the adequacy of the proposed plan. H.y.chang et al. [21] gave calculations expanding the vitality productivity of every sensor hub by utilizing the proposed Wake-up/Sleep (Wus) and Valid Measurement Selecting (VMS) plans. An interfacing different model (IMM) channel was connected to the proposed appropriated structural planning keeping in mind the end goal to adapt to a target move. Reenactment results outlined the execution of the proposed following channel. A. Umar et al. [22] proposed an augmentation of IAMCTD (Improved Adaptive Mobility of Courier hubs in Threshold-improved DBR convention for Uwsns) that concentrated on improving system unwavering quality and throughput for basic extent based applications. Their plan maintained a strategic distance from control overhead that was available in IAMCTD for actualizing changes inside and out limit. The development example of dispatch hubs alongside decreasing correspondence trouble on hubs builds throughput too. Furthermore, dependability period was enhanced and hub thickness for every round remained nearly high enhancing the general system unwavering quality. Taking into account the far reaching reenactments utilizing MATLAB, they watched that their plan enhanced the execution as far as throughput and steadiness period. Besides, nearly higher system thickness for every round was kept up and end-to-end postponement is settled all through the system lifetime. S.k. Reddy et al. [23] displayed two non-cryptographic calculations (DS-PADV and DS-RADV) to guarantee information survivability in versatile UWSN. The DS-PADV secured against proactive enemy which traded off of hubs before distinguishing its target. DS-RADV maked the system secure against responsive foe which traded off hubs in the wake of distinguishing the target. They broke down memory overheads and correspondence costs both scientifically and utilizing recreations. In existing plans, sensors stay static between visits from the sink, while in their plan sensors could move between progressive visits from the sink. They demonstrated that their methodologies performed better than known plans regarding correspondence overheads.

5. CONCLUSION AND FUTURE SCOPE

Underwater Wireless Sensor Networks (UWSNs) have an important role in different applications, such as offshore exploration and ocean monitoring. The networks consist of a considerably large number of sensor nodes deployed at different depths. Many routing protocols have been proposed in order to discover an efficient route between the sources and the sink. In this paper, an overview of various underwater wireless sensor networks has been discussed. Moreover the survey has been done on the work of the various researchers. It has been concluded from the survey that none of the technique is very much efficient for UWSN. So the paper has been concluded with a future scope to overcome this issue.

In near future,wwe will use comprehensive to reduce the amount of data going to be transmitted to suitable comprehensivetechniques

REFERENCES

[1] Kavar, Jaydip M., and K. H. Wandra. "Survey paper on Underwater Wireless Sensor Network."

[2] Ian F. Akyildiz, Dario Pompili, TommasoMelodia, State of the Art in Protocol Research for Underwater Acoustic

[3] Sensor Networks, WUWNet06, September 25, 2006, Los Angeles, California, USA

[4] J.H. Cui,J.Kong,M.Gerla, and S.Zhou,The building mobile underwater wireless networks applications,IEEE network,vol. 20,no. 3,pp.12-2006 Almirdevis,hwachang-"underwater wireless sensor network-ieee 2012".

[5] P. Xie, J.-H. Cui, and L Lao, "VBF: Vector-based Forwarding Protocol for Underwater Sensor Networks," International conference on networking (IFIP networking), , pp. 1- .

[6] Ibrahim, Dina M., Tarek E. Eltobely, Mahmoud M. Fahmy, and Elsayed A. Sallam. "Enhancing the Vector-Based Forwarding Routing Protocol for Underwater Wireless Sensor Networks: A Clustering Approach." In ICWMC 2014, The Tenth International Conference on Wireless and Mobile Communications, pp. 98-104. 2014.

[7] N. Nicolaou, A. See, P. Xie, J.-H. Cui, and D. Maggiorini, "Improving the Robustness of Location-

based Routing for Underwater Sensor Networks," Proc Of the OCEANS' , Europe, June , pp. 1- .
[8] P. Xie, Z. Zhou, Z. Peng, J.-H. Cui, and Z. Shi, "Void Avoidance in Three-dimentional Mobile Underwater Sensor Networks," Proc of the th international conference of wireless algorithms, system, and applications (WASA 2009), USA, August , pp. 305- . 314
[9] W. Bo, L. Yong-mei, and J. Zhigang, "ES-VBF: An Energy Saving Routing Protocol," Proc. of the 2012 International Conference on Information Technology and Software Engineering, 2012, pp. 87- .
[10] Rachman, Reza, EkaPurwaLaksana, DarmaSetiawan Putra, and RiriFitri Sari. "Energy Consumption at the Node in Underwater Wireless Sensor Network (UWSNs)." In Computer Modeling and Simulation (EMS), 2012 Sixth UKSim/AMSS European Symposium on, pp. 418-423. IEEE, 2012.
[11] Zandi, Rahman, Mahmoud Kamarei, and HadiAmiri. "Underwater acoustic sensor network localization using four directional beams." In Electrical Engineering (ICEE), 2013 21st Iranian Conference on, pp. 1-6. IEEE, 2013.
[12] Iqbal, Junaid, Faheem Ahmed, Muhammad Ishaque, and M. Hassan Nasir. "Gradient Estimation Vector Modeling of signal attenuation in Underwater Wireless Sensor Networks." In Applied Sciences and Technology (IBCAST), 2012 9th International Bhurban Conference on, pp. 144-147. IEEE, 2012.
[13] Waldmeyer, Marc, H. Tan, and Winston Khoon Guan Seah. "Multi-stage AUV-aided localization for underwater wireless sensor networks." In Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on, pp. 908-913. IEEE, 2011.
[14] Chen, Keyu, Maode Ma, En Cheng, Fei Yuan, and Wei Su. "A Survey on MAC Protocols for Underwater Wireless Sensor Networks." 1-15.
[15] Pouryazdanpanah, K. Maryam, MohammadfazelAnjomshoa, S. Ahmad Salehi, Amir Afroozeh, and G. MarjanMoshfegh. "DS-VBF: Dual sink vector-based routing protocol for underwater wireless sensor network." In Control and System Graduate Research Colloquium (ICSGRC), 2014 IEEE 5th, pp. 227-232. IEEE, 2014.
[16] Ali, Tariq, Low Tang Jung, and Ibrahima Faye. "Three hops reliability model for Underwater Wireless Sensor Network." In Computer and Information Sciences (ICCOINS), 2014 International Conference on, pp. 1-6. IEEE, 2014.
[17] Li, Ke, Chien-Chung Shen, and Guaning Chen. "Energy-constrained bi-objective data muling in underwater wireless sensor networks." In Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on, pp. 332-341. IEEE, 2010.
[18] Davis, Almir, and Hwa Chang. "Underwater wireless sensor networks." In Oceans, 2012, pp. 1-5. IEEE, 2012.
[19] Lee, Sungwon, and Dongkyun Kim. "Underwater hybrid routing protocol for UWSNs." In Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on, pp. 472-475. IEEE, 2013.
[20] Zhang, Qiang, Meiqin Liu, Senlin Zhang, and Huayan Chen. "Node topology effect on target tracking based on underwater wireless sensor networks." In Information Fusion (FUSION), 2014 17th International Conference on, pp. 1-8. IEEE, 2014.
[21] Yu, Chang Ho, JeongCheor Lee, Jae Weon Choi, Myeong-Kwan Park, and Dong Joong Kang. "Energy efficient distributed interacting multiple model filter in UWSNs." In Control, Automation and Systems (ICCAS), 2012 12th International Conference on, pp. 1093-1098. IEEE, 2012.
[22] Umar, A., M. A. Hasnat, M. Behzad, I. Baseer, Z. A. Khan, U. Qasim, and N. Javaid. "On Enhancing Network Reliability and Throughput for Critical-range based Applications in UWSNs." Procedia Computer Science 34 (2014): 196-203.
[23] Reddy, SasiKiran VL, SushmitaRuj, and AmiyaNayak. "Distributed data survivability schemes in mobile Unattended Wireless Sensor Networks." In Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 979-984. IEEE, 2012.

Modification of surface using Powder Metallurgy electrode in electrical discharge machining with current innovative techniques: A review

Pahulpreet Singh, Vikas Kumar*, Paramjit Singh, Gaurav Tejpal, Sukhdeep Singh
Department of Mechanical Engineering,
Amritsar College of Engineering and Technology, Amritsar, Punjab, India
*C.T. Institute of Engineering and Technology, Shahpur campus, Jalandhar, Punjab, India
vikas_cadcam@rediffmail.com, er_pannu266@yahoo.com, gaurav_tejpal@acetedu.in, pahulpreet09@gmail.com

***Abstract*—Electrical discharge machining (EDM) is a non-conventional machining process widely used for manufacturing complex geometry or hard to cut materials e.g. (super alloys, ceramics, and composites). These materials are very difficult-to-machine with other conventional machining processes. Many researchers have showed a significant amount of research interests in EDM process due to its wide application in defense, automotive, aerospace, and manufacturing of tool and dies and tremendous role in the progress of least cost products with more trustworthy quality assurance. In electrical discharge machining process use of powder metallurgy electrode instead of other electrode materials like (copper, mild steel and graphite etc.) has emerged an alternative tooling option with a view to impart improved surface properties of work piece material. The main intention of this paper is to presents the scenario of modification of surface properties of work piece by using powder metallurgy electrode and in sighting current innovative techniques used in EDM process.**

***Index Terms*—Electrical Discharge Machining (EDM), Powder Metallurgy (PM), Innovative techniques.**

I. INTRODUCTION

All Last five decades technology of EDM process has played an essential role in manufacturing industries and became crucial in manufacturing applications such as die and mold making, micro-machining, machining of composite ceramics and prototyping, etc. The phenomena of Electrical discharge or spark machining in EDM process takes place over a very short period of time in a very narrow space (10-100μm) known as inter electrode gap between electrode and work piece, which is filled with dielectric liquid involving melting and evaporation of the tool electrode as well as work piece material. Earlier in 1770, Joseph Priestly an English scientist discovered the erosive effect of electrical discharges. In 1930s, attempts were made for the first time to machine metals and diamonds with electrical discharge.

A Disintegrator was developed by V.E. Matulaitis and H.V. Harding [1] of Elox US to remove the broken taps from expensive Work piece materials e.g. (high speed steel and cemented carbide) through Erosion process which was caused by arc discharges occurring in inter electrode gap connected to a DC power supply. Short mechanical contacts initiated the arc discharges like welding arcs which was interrupted by retraction using vibration of the tool electrode. An equipment was developed by AEG [2] capable of eroding diamond using the heat generated by arc discharges occurring at high frequencies in the inter electrode gap. These processes are not very promising due to low precision resulted due to overheating of the machining area and defined as "Arc-Machining", On the other hand "Spark Machining", works precisely because the work piece is protected from excessive heat attacks. This feature of spark machining is clearly apparent from its shop floor application. However, from the physical point of view it is difficult to distinguish between arc machining and spark machining. In 1943, soviet scientists B. R. Lazarenko and N. I. Lazarenko [3] reversed the effect of metal removal from electric circuit breakers and optimized this phenomenon for material removal purposes. In 1950s, relaxation type generators (resistance–capacitance charging condensers to store and define discharge energy) were used. It became possible to make a simple servo control circuit to automatically find and hold a given gap between electrodes (Tool & work piece) and moreover to control pulse times through these circuits. In 1980s, Computerized Numerical Control (CNC) machines came into the picture and the efficiency of EDM process is further enhanced. In the last two decades, researchers have carried out a lot of research work to enhance the productivity of EDM process.

II. MECHANISM OF EDM PROCESS

The mechanism of erosion of material from work piece mainly conversion of electrical energy into thermal energy through a series of sparks occurring into inter electrode gap between tool electrode and work piece immersed in a dielectric fluid [4]. Generation of plasma channel between the cathode and anode is done by the thermal energy [5] at a temperature in the range of 8000 to 12,000 °C [6] or as high as 20,000 °C [7] resulting in a significant amount of heating and melting of material at the surfaces of work piece and tool electrode shown in figure no:1. The plasma channel breaks down when the pulsating DC supply is turned [8] resulting in rapid cooling

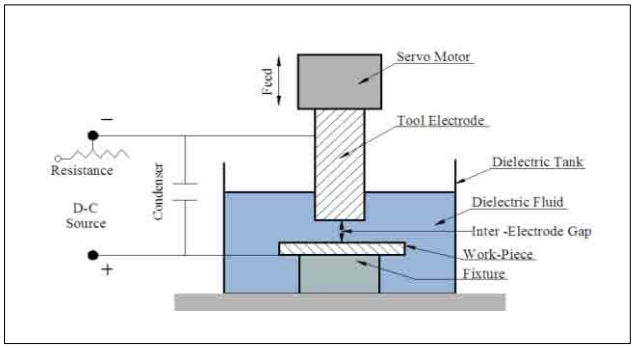


Fig. 1. Schematic diagram of sinking EDM process.

allowing the circulating dielectric fluid to flush the molten material from the inter electrode gap in the form of debris The range of volume of material removed per discharge is typically lie between 10_6 to 10_4 mm3 and the material removal rate (MRR) is usually between 2 and 400 mm3/min [9] since the shape of the tool electrode defines the area in which the spark erosion will occur.

III.MODIFICATION OF SURFACE BY POWDER METALLURGY ELECTRODE

The Earlier, in EDM process, mechanically formed tool electrodes materials e.g. copper, brass, mild steel, graphite, chromium, tungsten, steel, copper-tungsten and copper chromium alloys were used by researchers. Powder metallurgy electrode is an alternative tooling method which is more economical and faster to manufacture and also to reduce the cost of electrode made by conventional method which may cost around 100 times more than a simple square electrode. In powder metallurgy, a large number of EDM tool electrodes can be manufactured from a single die and punch assembly. This may results in an overall reduction of cost for mass production of EDM electrodes. Powder metallurgy is a viable alternative method to produce tool electrode in which the desirable properties of different materials can be combined. The electrodes made by using powder metallurgy technology from special powders have been used to modify EDM surfaces in recent years, to improve wear and corrosion resistance. Many researchers are continuously trying to improve the properties of surface by EDM process using powder metallurgy tool electrode. Surface deposition by EDM in a liquid dielectric using PM compact tool electrode was reported by Gangadhar e.t. al. [10]. Results showed that deposition of tungsten carbide on flank and rake of a HSS toll using PM electrode containing 40%WC and 60% Fe (zinc sterate as lubricant) with reverse polarity and kerosene as dielectric resulted in low variation in cutting forces. Soni and Chakraverti [11] investigated that migration of appreciable amount of elements from the tool electrode to work piece and vice versa. Moreover, surface got alloyed in the re-solidified layer causing a change in chemical composition and significant increase in surface hardness of the work piece during electro-discharge machining of high carbon high chromium die steel (hardened) with rotating copper-tungsten tool electrode. Samual et al. [12] Reported that EDMing of hardened steel (BS 970817M40, 53Rc) work material of Cu electrode made through PM and paraffin as dielectric. A new method of surface modification by EDM process was described by Wang et al. [13]. Tsai et al. [14] Investigated the blending of copper powders containing resin with chromium powders to form tool electrode by using an ordinary EDM machine tool and kerosene fluid, a hard ceramic layer can be created on the work piece surface with a Ti or other compressed powder electrode in a certain condition. It was reported that a compact TiC ceramic layer can be created on the surface of the metal work piece. The small area EDM process using a copper–tungsten electrode on AISI 1045 carbon steel was investigated by Lee et .al [15] It was reported that the values of the MRR, SR increase for higher values of pulse current. Ferreira [16] investigated copper-tungsten electrodes with negative polarity. It was reported that copper-tungsten electrodes with negative polarity was suitable for the planetary EDM surface micro finishing of die steel (AISI H13) with good geometry accuracy and sharp details. Chen et. al [17] investigated machining characteristics and surface modifications affect on low-carbon steel (S15C) with semi-sintered electrodes. Results showed that the composition of the semi-sintered electrodes was transferred onto the machined surface efficiently and effectively during the EDM process and that the process is feasible and can easily form a modified layer on the machined surface. Samuel et. al [18] investigated the comparison of the performance of powder metallurgy (P/M) tool electrodes with conventional electrodes (using straight polarity and not in machining conditions favouring surface modification).it was reported that P/M electrodes were found to be more sensitive to changes in pulse current and pulse duration and their impact on output parameters such as material removal rate and electrode wear was found to be different as compared to conventional electrodes. Li. et al [19] proposed that the densification electrodes could be improved by the addition of nickel. It was also found that under certain processing and operating conditions, P/M electrodes could cause net material addition instead of material removal. Wang et al. [20] suggested the application of “electrical discharge coating (EDC)” method for surface repairing and strengthening of cutting tools and moulds. Experiments were conducted by author on carbon steel with titanium powder compact electrodes using negative polarity of the tool and a machining time of 18min. It was found that low values of discharge current (2–10A) and low pulse duration (2–12_s) gave a concentration of titanium carbide as high as 51% and more than three times increase in hardness. Maximum value of micro-hardness was achieved at 2.2A discharge current and 2_s pulse duration. Moro et al. [21] reported that working life of the die by three to seven times can be improved by using Ti powder compact electrodes. Gangadhar et al. [22] investigated mild steel by using bronze compacts P/M electrode having 90% copper and 10% tin in reverse polarity. Author studied the work surface using electron microscopy and X-ray diffraction analysis and found that surface topography was modified by the process. The major phase present in the surface was Cu3Sn while other phases such as Cu6Sn5 and CuSn were also

present. Results concluded the possibility to alter the metallurgical and physico-chemical nature of the surface by suitable changes in the ingredients and compositions of the powder compact. Shunmugam et al. [23] used tungsten carbide powder compact electrodes containing 40% WC and 60% Fe to improve the wear resistance of mild steel work material. Energy dispersive analysis of the surface confirmed the transfer of tungsten carbide to the machined surface. Other than WC and W2C phases, iron carbide was also present in the deposited layer in the form of FeC, (Fe3C) H and Fe3C phases. Mohri et al. [24] modified the surface of carbon steel and aluminum work pieces using composite electrodes of copper, aluminum, tungsten carbide and titanium in hydrocarbon oil. It was reported that electrode material was found in the work piece surface layer and the characteristics of the surface layer changed remarkably. These surfaces had less cracks and higher corrosion and wear resistance. Tsunekawa et al.[25] studied by modifying surface of aluminum using powder compact electrodes having 64% Ti and 36% Al. Author fined put dendritic precipitates of titanium carbide on the machined surface. The electrode was connected to negative polarity and kerosene was used as the working fluid. The average diameter and alloyed depth of discharge craters increased with increase in pulse width, the other important factor being the discharge current. It was found that the forming pressure of the powder metallurgy electrodes did not affect material transfer. Kruth et al. [26] succeeded in depositing aluminum on steel and TiC on aluminum using Al and Ti–Al green compact electrodes respectively with a traditional EDM machine. Experiments were conducted by using porous electrodes with negative polarity favouring high tool wear. In a, Pantelis et al. [27] machined 0.4% carbon steel with a tool electrode containing 70% Fe and 30% WC using both positive and negative polarity in comparative analysis of the two polarities. The work surfaces were subjected to optical metallography, SEM, EDS, X-ray diffraction analysis, surface roughness measurements and micro-hardness testing. White layer was found along the surface of machined specimens for all the pulse energies tested, regardless of the polarity used. Tungsten rich zones were found in the alloyed white layer with negative polarity, but high pulse energies during machining resulted in extensive cracking and surface defects. Simao et al. [28] attempted a statistical analysis using L8 fractional factorial Taguchi design. Author conducted surface modification of H13 hot work tool steel by WC/cobalt electrodes and identified the effect of key operating factors. The alloyed/modified layer had relatively few micro-cracks, an average thickness of 30_m and surface hardness of 1319 HK, up from 640 HK. Open gap voltage was shown to have little effect on work piece micro-hardness. Patowari et al. [29] designed same experimental for machining C-40 grade steel with WC/Cu powder metallurgy electrodes. Results showed the presence of both WC and Copper in the work piece surface. The deposition was achieved in only 3 min and significant factors were highlighted. Surface examination on SEM revealed relatively few micro-cracks and an increase in hardness from 200–220HV to 1200–1632HV was reported. To compare the effect of different dielectric media on surface modification, Bai et al. [30] modified properties of surface of super-alloy Haynes 230 with Al–Mo composite electrode using distilled water and kerosene. Each sample was machined for 6 min. Distilled water gave higher hardness whereas kerosene gave better surface finish, finer surface morphology, thicker alloyed layer and slower oxidation rate. The best *R*a value of surface roughness obtained was 2.62_m. Current density at the negative electrode was higher than the positive electrode. It was concluded that surface alloying effect was better in kerosene as compared to distilled water. Tsai et al [31] reported transfer of copper and chromium particles from copper–chromium sintered electrodes under negative polarity.

From the available literature, it can be inferred that EDM has the potential of becoming a useful and cheap alternative process for surface modification. Powder metallurgy electrodes offer a convenient way of achieving selective surface alloying. PM manufactured electrodes have proved to be best alternative method of electrode manufacturing due to ease of production and control of properties.

IV. Innovative Techniques in EDM

A. Coloring of Titanium alloy using EDM process

By using WEDM process, a new method of coloring titanium alloys was proposed by Minami et al. [32]. WEDM normally uses deionized water, so, due to electrolysis there is a formation of an oxide layer over the surface of anode work piece. It is recognized that the coloring of stainless steel and the surface of titanium alloy is done by anodic oxidation, occurred by the interference of light in the oxide film formed by electrolysis. During the process of cutting finish on the WEDMed surface, the surface is given an arbitrary colour as shown in Figure 2.

Oxide layer thickness determines the colour, so, by varying the open voltage or by controlling the wire-electrode's feed rate the colour can be changed. On products of titanium, fine and multicolored pattern can be drawn in sinking EDM by using a simple electrode controlled by an NC system [33].

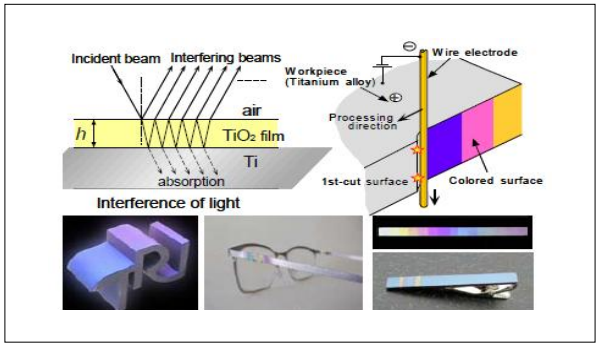


Fig. 2. Schematic of coloring of titanium alloy using EDM process [32].

B. EDM of non-conducting material

It has been supposed that EDM can machine only electrically conductive materials. However, EDM can also

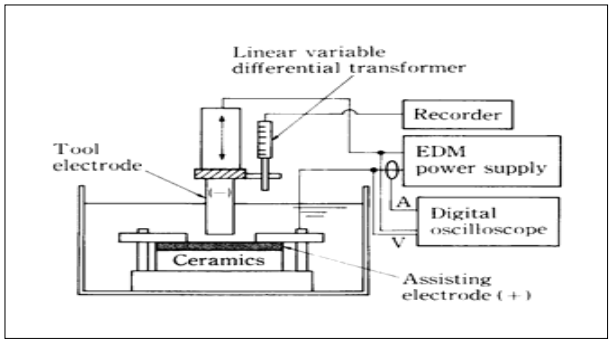


Fig. 3. Schematic of EDM for insulating ceramics with an assisting electrode method [36-38].

machine diamond by introducing the coating of graphite on it. Diamond should be heated in a pyrolitic atmosphere comprised with a carbon compound or in a non oxidizing flame, until it reaches the temperature of conversion to graphite. The discharge spot's temperature should be greater than the conversion temperature of diamond-graphite's conversion temperature when there is the occurrence of discharge between the coating of graphite and the tool electrode, as the newly formed graphite-coating is done on the bottom of the crater, then there is repetition of this same process [34, 35]. Fukuzawa et al. [36-38] discovered a way by which nonconductive ceramics are EDMed totally. As shown in Figure 3, for machining, a metal plate/ mesh is placed over the ceramics. Initially, in between the metal plate and tool electrode, there is production of discharge. There is erosion of metal plate and thermal decomposition of working oil and deposition of pyrolitic carbon on the positive polarized work-piece. As, in die sinking the carbon is deposited on tool electrode by the above mentioned phenomenon. Further, electrically conductive carbon layer covers the ceramics surface after the erosion of metal. Hence, till discharge maintains the carbon deposition, there is continued occurrence of discharge on the ceramics. 3D shapes of materials such as Si3N4, ZrO2, SiC, Al2O3, AlN, glass, old ceramics, and diamond are machined by EDM process with this method. As shown in Figure 4, WEDM facilitates the machining of a chair-shaped product of Si3N4 [38]. Taniguchi et al. [39] machine diamond and alumina ceramics by using micro wave. Work pieces of these materials were placed in the gap between a pair of needle electrodes and the axis of these electrodes was oriented parallel to the electric field of the micro wave standing in a micro wave tube. Dielectric heating inside the material melts the alumina ceramic, whereas the discharge column developed between the surface of diamond and the tip of the needle electrode generates the heat flux which evaporates the diamond as the dielectric hysteresis loss of diamond was insignificant. The high electric resistivity of the silicon single crystal generates a large voltage drop which is one of the difficulties produced during the process of EDM slicing of silicon wafers [40- 42]. One of these authors also stated that this large voltage drop is also produced by the high contact resistance at the point of contact in between the silicon wafer and metal electric feeder. In general, when two smooth surfaced plates are made to be in contact with each other, the area of real contact is very small, and as in this small area density of concentrated electric current is very high which signifies the voltage drop. Hence, there would be enormous drop in voltage when interface is developed between metal and high-electric-resistivity material, while voltage drop due to interface by the contact of two different metals is ignorable when it is compared with the voltage drop in the discharge channel. Thus it is concluded that to improve the machining rate, formation of a low electric resistivity layer over the silicon wafer service is done. The contact resistance is caused by the small area of real contact along with the differences in work function between contacting materials due to which the Schottky barrier is created. The effects of the Schottky barrier in metal-silicon contact was eliminated by the process of electroplating the silicon surface with metal like Ni, Al and Sb-Au [42, 43]. This was done to minimize the contact resistance in the EDM of the silicon single crystal and to alter the rectifying contact to an ohmic one.

C. EDM of non-linear holes

To reduce the forming cycle time, it is essential to cool the mold surface in plastic injection molding and aluminum die-casting. Curved surfaces of the mold are provided with proper channels for the passage of coolant. However, mechanical processes such as cutting, grinding, etc. are unable to effectively machine curved holes. Thus, curved holes are effectively machined by performing several novel electrical machining methods [44-47].

Fig. 4. Machining of insulating ceramics by wire EDM (work-piece: Si3N4) [38].

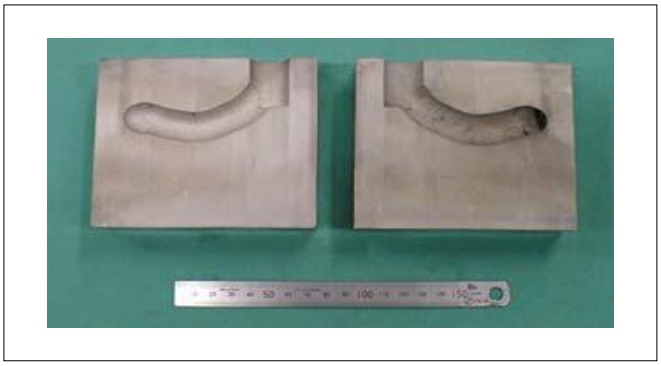


Fig. 5. Curved Tunnel machined by EDM [45].

Hollow space of a straight pipe was introduced by a coil spring made as similar to the curvature of the hole in order to guide the coil. The end of the coil spring is attached with a spherical tool electrode. Initially, both the coil spring and the guide pipe were fed together to a certain depth by machining the work piece. Then the coil spring is allowed to feed alone as the position of the guide pipe is fixed. Goto et al. [45] proposed the curved hole shown in Figure 5. Uchiyama et al. [47] also introduced an electrochemical machining method.

D. Strip EDM

Electrical discharge machining (EDM) is widely used to machine all conductive materials those are hard-to-cut metals. In EDM process material removed not only from work-piece but also from electrode resulting in low productivity. A new method was introduced e.g. strip EDM to in order to overcome these problems. Strip EDM is basically a similar process like wire EDM. In strip EDM a continuously moving brass strip Brass strip (width: 10 mm, thickness: 0.1 mm) is provided as an electrode. The waste or worn strip is removed by winding reel and a new one is supplied continuously shown in figure 6, 7. Hence no tool electrode wear happens during the machining process. The strip EDM method was applied to EDM milling as well as EDM turning shown in figure 6.

Author has used a commercial wire EDM machine (EZ20S, SPM Co., Ltd.). As shown in Fig. 7. The strip electrode can move relatively to the work-piece material, which was set on the Z-column of the machine. The power source generated bipolar pulses that consisted of +140 V and -80 V. The pulse conditions were 12.8 kHz with a duty ratio of 36%. De-ionized water used as a working fluid and a nozzle injected into a machining gap. Problem of corrosion caused by water to work-piece during the EDM process can be prevent by the bipolar pulse due to the low average voltage between the work-piece and the electrode [48].

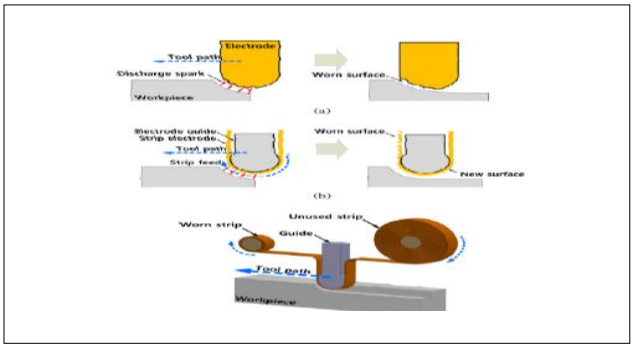


Fig. 6. (a) General EDM (b) Strip EDM (c) the concept of the strip EDM.

E. Two methods are under Strip EDM

- Strip EDM milling
- Strip EDM turning

Figure 8 shows the schematics of the EDM milling in this study. The depth of the cut and machining length were 1 mm and 15 mm, respectively. The material of the block electrode was brass, the same as the strip. Radial depth of the cut was

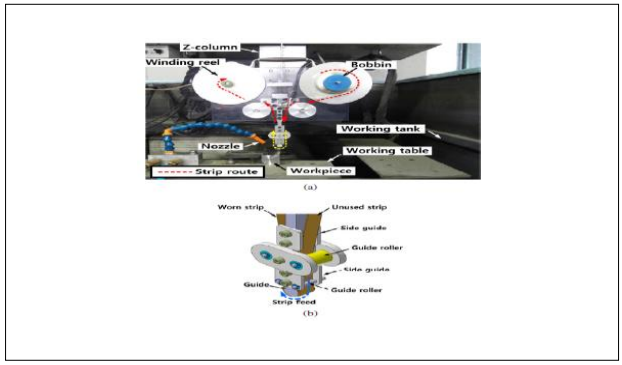


Fig. 7. (a) Strip-EDM system (b) Electrode guide.

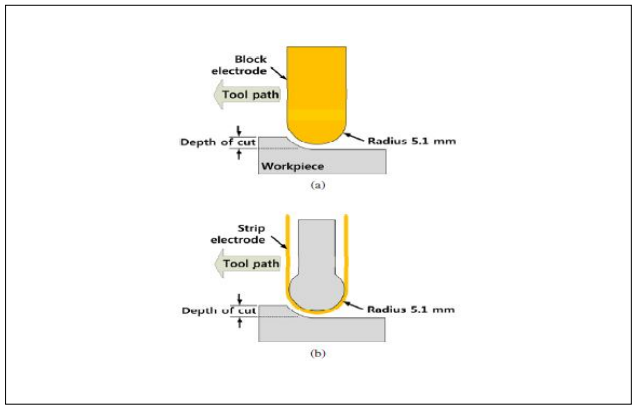


Fig. 8. (a) Normal EDM milling using a block electrode; (b) Strip- EDM milling. Strip EDM turning.

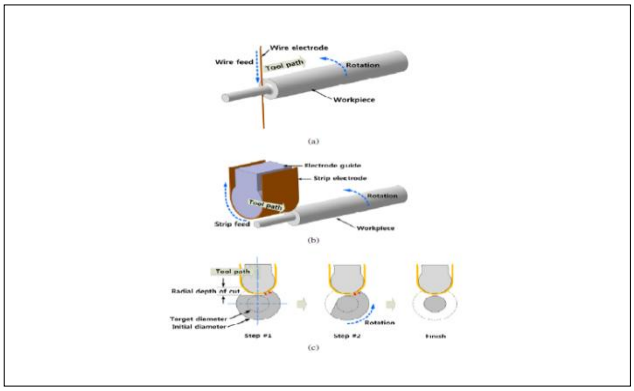


Fig. 9. Strip (a) Wire-EDM turning (b) Strip-EDM turning (c) Steps of strip-EDM turning.

and diameter of round work-piece was 3 mm. The wire electrode moved in the axial direction of the work-piece rod, as shown in Figure 9 (a). In case of strip electrode moved in the radial direction of the rod in the strip-EDM turning process. The strip-EDM turning operation is shown in Figure 9 (b). Strip machining process consisted of two steps, as shown in Figure 9 (c).In the first step, no rotation of work-piece machined by the electrode. Secondly, rotating work-piece is machined when electrode reached the center of the rod. The rotation of the work-piece should at a high speed in wire-EDM turning because this machining method could make a helical shape on low rotation speed [49, 50]. The strip-EDM method

was able to complete the machining with only one revolution. While the work- piece rod rotated at 90 rpm in the wire-EDM turning process.

F. Conclusions

- Powder metallurgy electrodes offer a convenient way of modifying and achieving selective surface alloying. Powder metallurgy tool in EDM process has been used mostly for steel based materials. There are so many composite ceramics need to be investigated through PM tool electrode in EDM process for future work.
- A new method for coloring the surfaces through electrolysis has been mostly used for titanium and stainless steel materials. Coloring of non conductive materials may have significant approach by using this process. This is needed to be investigated for further research work.
- Earlier, EDM process was used to machine conductive materials. But now a day, non-conducting material like diamond can also be machined through EDM process by introducing coating of graphite on the surface of non-conductive material.
- In strip-EDM, no cusp is produced due to flat strip electrode as compare to EDM turning process in which wire electrode is used. Moreover the large area of the strip electrode increases MRR as compare to wire electrode, which is small in diameter.

REFERENCES

[1] M. Kunieda, B. Lauwers, K.P. Rajurkar, B.M. Schumacher, "Advancing EDM through Fundamental Insight into the Process", CIRP Annals – Manufacturing Technology, vol. 54, 2005, pp. 64–87.

[2] M. Kunieda, B. Lauwers, K.P. Rajurkar, B.M. Schumacher "Advancing EDM through Fundamental Insight into the Process", CIRP Annals - Manufacturing Technology, Volume 54, Issue 2, 2005, Pages 64–87

[3] B. R. Lazarenko, "To invert the effect of wear on electric power contacts", Dissertation of the All-Union Institute for Electro Technique in Moscow/CCCP (in Russian), 1943.

[4] [4] H.C. Tsai, B.H. Yan, F.Y. Huang, EDM performance of Cr/Cu based composite electrodes, Int. J. Mach. Tools Manuf. 43 (3) (2003) 245–252.

[5] E.I. Shobert, What happens in EDM, in: E.C. Jameson (Ed.), Electrical Discharge Machining: Tooling, Methods and Applications, Society of Manufacturing Engineers, Dearbern, Michigan, 1983, pp. 3–4.

[6] G. Boothroyd, A.K. Winston, Non-conventional machining processes, in: Fundamentals of Machining and Machine Tools, Marcel Dekker, Inc, New York, 1989, p. 491.

[7] J.A. McGeough, Electro discharge machining, in: Advanced Methods of Machining, Chapman & Hall, London, 1988, p. 130.

[8] S.F. Krar, A.F. Check, Electrical discharge machining, in: Technology of Machine Tools, Glencoe/McGraw-Hill, New York, 1997, p. 800.

[9] S. Kalpajian, S.R. Schmid, Material removal processes: abrasive, chemical, electrical and high-energy beam, in: Manufacturing Processes for Engineering Materials, Prentice Hall, New Jersey, 2003, p. 541.

[10] A. Gangadhar, M. S. Shunmugam and P. K. Philip, Surface modification in electro discharge processing with a powder compact tool electrode, Wear, 143 (1) (1991) 45-55.

[11] J.S. Soni and G. Chakraverti, Experimental investigation on migration of material during edm of die steel (T215 Cr12), Journal of Materials Processing Technology, 56 (1996) 439-451.

[12] M. P. Samuel and P. K. Philip, Power metallurgy tool electrodes for electrical discharge machining, International Journal of Machine Tool and Manufacture, 37 (11) (1997) 1625-1633.

[13] Z. L. Wang, Y. Fang, P. N. Wu, W. S. Zhao and K. Cheng, Surface modification process by electrical discharge machining with a Ti powder green compact electrode, Journal of Material Processing Technology, 129 (1-3) (2002) 139-142.

[14] H. C. Tsai, B. H. Yan and F. Y. Huang, EDM performance of Cr/Cu based composite electrodes, International Journal of Machine Tool and Manufacture, (43) (3) (2003) 245-252.

[15] Hwa-Teng Lee, Fu-Chuan Hsu, Tzu-Yao Tai, Study of surface integrity using the small area EDM process with a copper–tungsten electrode, Materials Science and Engineering A, 364 (2004) 346–356.

[16] Jose Carvalho Ferreira, A study of die helical thread cavity surface finish made by Cu-W electrodes with planetary EDM, International Journal of Advance Manufacturing Technology, 34 (2007) 1120–1132.

[17] Yuan-Feng Chen, Han-Ming Chow, Yan-Cherng Lin and Ching-Tien Lin , Surface modification using semi-sintered electrodes on electrical discharge machining, International Journal of Advanced Manufacturing Technology 36 (5-6) (2008) 490-500.

[18] Samuel, M.P., Philip, P.K., 1997. Powder metallurgy tool electrodes for electrical discharge machining. International Journal of Machine Tools & Manufacture 37 (11) 1625–1633.

[19] Li, L., Wong, Y.S., Fuh, J.Y.H., Lu, L., 2001. EDM performance of TiC/copper based sintered electrodes. Materials and Design 22, 669–678.

[20] Wang, Z.L., Fang, Y., Wu, P.N., Zhao, W.S., Cheng, K., 2002. Surface modification process by electrical discharge machining with a Ti powder green compact electrode. Journal of Materials Processing Technology 129, 139–142.

[21] Moro, T., Goto, A., Mohri, N., Saito, N., Matsukawa, K., Miyake, H., 2001. Surface modification process by electrical discharge machining with TiC semi-sintered electrode. Journal of Japanese Society of Precision Engineering 67 (1), 114–119.

[22] Gangadhar, A., Shunmugam, M.S., Philip, P.K., 1991. Surface modification in electro discharge processing with powder compact tool electrode. Wear 143, 45–55.

[23] Shunmugam,M.S., Philip, P.K., Gangadhar, A., 1994. Improvement of wear resistance by EDM with tungsten carbide powder metallurgy electrode. Wear 171, 1–5.

[24] Mohri, N., Saito, N., Tsunekawa, Y., 1993. Metal surface modification by electrical discharge machining with composite electrodes. Annals of the CIRP 42 (1), 219–222.

[25] Tsunekawa, Y., Okumiya, M., Mohri, N., Takahashi, I., 1994. Surface modification of aluminum by electrical discharge alloying. Materials Science and Engineering A174, 193–198.

[26] Kruth, J.P., Stevens, L., Froyen, L., Lauwers, B., 1995. Study on the white layer of a surface machined by die sinking electro-discharge machining. Annals of the CIRP 44 (1), 169–172.

[27] Pantelis, D.I., Vaxevanidis, N.M., Houndri, A.E., Dumas, P., Jeandin, M., 1998. Investigation into application of electro discharge machining as steel surface modification technique. Surface Engineering 14 (1), 55–61.

[28] Simao, J., Lee, H.G., Aspinwall, D.K., Dewes, R.C., Aspinwall, E.M., 2003. Work piece surface modification using electrical discharge machining. International Journal of Machine Tools & Manufacture 43, 121–128.

[29] Patowari, P.K., Mishra, U.K., Saha, P.,Mishra, P.K., 2006. Surface modification of C-40 steel using WC-Cu P/M green

compact electrodes in EDM. In: Proceedings of the 1st International and 22nd AIMTDR Conference, IIT, Roorkee, India, pp. 875–879.
[30] Bai, Ching-Yuan, Koo, Chun-Hao, 2006. Effects of kerosene or distilled water as dielectric on electrical discharge alloying of super alloy Haynes 230 with Al–Mo composite electrode. Surface & Coatings Technology 200, 4127–4135.
[31] Tsai, H.C., Yan, B.H., Huang, F.Y., 2003. EDM performance of Cr/Cu-based composite electrodes. International Journal of Machine Tools & Manufacture 43, 245–252.
[32] Minami H., Masui K., Tsukahara H., Hagino H., 1998, Coloring Method of Titanium Alloy using EDM Process, Proc. ISEM 12, 503-512.
[33] Minami H., Masui K., Tsukahara H., Hagino H., 2001, Coloring of Titanium Alloy using EDM Process – Drawing with Simple Electrode -, Proc. ISEM 13, 589-599.
[34] Heerschap, M., Levitt, C.M., 1960, Eroding of Hard Crystalline Carbon, United States Patent, 2,939,941.
[35] Van Osenbruggen C., van Ruler J., Schoenmakers T.M., 1977, Method of Finishing a Workpiece of a Non-conducting Material, Particularly Diamond, by Means of Spark Erosion, United States Patent, 4,013,863.
[36] Fukuzawa Y., Katougi H., Mohri N., Furutani K., Tani T., 1998, Machining Properties of Insulating Ceramics with an Electric Discharge Machine, Proc. ISEM 12, 445-453.
[37] Mohri N., Fukuzawa Y., Tani T., Sata T., 2002, Some Considerations to Machining Characteristics of Insulating Ceramics, Annals of the CIRP, 51/1, 161-164.
[38] Tani T., Fukuzawa Y., Mohri N., Saito N., Okada M., 2004, Machining Phenomena in WEDM of Insulating Ceramics, Journal of Materials Processing Technology, Vol. 149, Issues 1-3, 124-128.
[39] Taniguchi N., Nagata T., 1968, Micro-wave Machining, 50th Denki-Kakoh-Kenkyukai, 1, 1-22 (in Japanese).
[40] Uno, Y., Kubota, S., Yokomizo, S., Okada, A., Tanaka, H., 1996, Study on Fine Boring of Single Crystalline Silicon by EDM, J. of JSEME, 30, 65, 9-16 (in Japanese).
[41] Kawada, K., Masaki, K., Sato, T., Masuzawa, T., 1994, Study on Micro-EDM (3rd Report), J. of JSEME, 28, 59, 1-10 (in Japanese).
[42] Luo Y.F., Chen C.G., Tong Z.F., 1992, Slicing Thin Silicon Wafers by Wire EDM Cutting, ISEM 10, 287-294.
[43] Kunieda M., Ojima S., 2000, Improvement of EDM Efficiency of Silicon Single Crystal through Ohmic Contact, Precision Engineering, 24, 185-190.
[44] Fukui M., Kinoshita N., 1989, Developing a Mole Electric Discharge Digging Machining, Annals of the CIRP, 38/1, 203-206.
[45] Goto A., Watanabe K., Takeuchi A., 2002, A Method to Machine a Curved Tunnel with EDM, IJEM, 7, 43-46.
[46] Ishida T., Kogure S., Miyake Y., Takeuchi Y., 2004, Creation of Long Curved Hole by Means of Electrical Discharge Machining Using an In-pipe Movable Mechanism, J. Materials Processing Technology, 149, 157-164.
[47] Uchiyama M., Shibazaki T., 2004, Development of an Electro machining Method for Machining Curved Holes, J. Materials Processing Technology, 149, 453-459.
[48] Chung, D., K., Shin, H., S., Chu, C., N., 2012, "Modeling and Experimental Investigation for Electrolytic Corrosion Prevention in High Frequency Micro EDM Using De-ionized Water," Microsystems Technologies, 18, p. 703.
[49] Imai, T., Suzuki, T., Kwatsu, H., Koto, A., 2010. "Electrical Discharge Machining," Gijutsu- Hyohron Co., Ltd., Tokyo, p. 124.
[50] Song, K. Y., Chung, D. K., Park, M. S., Chu, C. N., "Strip-EDM Turning," 2012, Proceeding of Korean Society for Precision Engineering Autumn Conference, p. 41.

OXIDATION STABILITY OF FUELS DERIVED FROM OILS: A REVIEW

Meetu Singh
Department of Applied Sciences,
Punjab Technical University,
Jalandhar, India.
Email: meet.rajput40@yahoo.com

Amit Sarin
Department of Applied Physics,
Amritsar College of Engineering and
Technology, Amritsar.
Email: amit.sarin@yahoo.com

Neerja
PG Department of Physics and
Electronics, DAV College, Amritsar
Corresponding author:
neerjakalia@yahoo.co.in

Abstract --
Atmospheric Pollution is one of the most concerning problems of modern society. The high energy demand in the industrialized world and pollution problems caused due to widespread use of fossil fuels. This makes it necessary to develop the renewable energy sources of limitless duration and smaller environmental impact than the traditional one. Fuels derived from oils are renewable transportation fuels consisting of fatty acid methyl esters, generally produced by transesterification of vegetable oils and animal fats. Oxidation stability of such fuels is an important issue because fatty acid derivatives are more sensitive to oxidative degradation than mineral fuel. The present paper is an attempt to review the work done so far on the oxidation stability of oil derived fuels under different conditions.

Keywords--
Renewable Energy, Fatty Acid Methyl Esters, Transesterification, Oxidation Stability.

I. Introduction

The state of our environment is deteriorating fast due to variety of reasons and one of the major is widespread use of fossil fuels. The development of renewable energy sources of limitless duration and smaller environmental impact is need of the hour. The progress of fuels derived from oils, also termed as biofuels, can be traced back to early 19th century. In fact, the development of diesel engines and biofuels has simultaneous history of technological advancements and economic struggle. Background interest in such fuels is continuing to increase in the U.S. and throughout the world [1]. India, like most of the developing countries of the world, despite its potential agricultural resources, is still highly dependent on imported crude oil for energy production. With its growing population, India's demand for the energy is 3.5% of world's energy demand and is expected to grow at the rate of 4.8% per annum of its present demand. As the demand of crude oil has increased dramatically and thus, country's cost for the import of crude oil has increased substantially [2]. The most popular fuel synthesized from oils, currently in use is termed as biodiesel. Biodiesel is defined by ASTM as "a fuel comprised of monoalkyl esters of long-chain fatty acids derived from vegetable oils or animal fats, designated B100" [3]. Biodiesel is produced by a chemical process known as transesterification, by which the triglycerides are reacted with alcohols, in the presence of a catalyst, to produce fatty acid alkyl esters. A byproduct of transesterification is glycerine, also known as glycerol. Since the most common alcohol used to produce biodiesel is methanol, another name for biodiesel is fatty acid methyl esters (FAME).Biodiesel is environmentally friendly because of lower hydrocarbon emissions, lower carbon monoxide emissions and reduction of greenhouse gases but there is increase in NO_x in biodiesel emissions. Oil derived fuels can reduce the dependency on foreign oil and helps to lubricate the engine itself, decreasing engine wear. Since, fuels like biodiesel which are synthesized from oils are chemically ester molecules. Thus, there is every possibility that such fuels will be hydrolyzed to alcohol and acid in the presence of air or oxygen. Presence of alcohol will lead to reduction in flash point and presence of acid will increase total acid number. All these make biodiesel relatively unstable on storage and residual products of biodiesel such as insoluble gums, total acids and aldehydes formed from degradation may cause engine problems like filter clogging, injector coking, and corrosion of metal parts. This is why the oxidation stability is an important criterion for such fuels.

II. Oxidation Stability

Mechanism of Oxidation Stability

During the oxidation process, the fatty acid methyl ester usually forms a radical next to double bond. This radical quickly binds with the oxygen in the air, which is a biradical. This forms peroxide radical. The rapid radical destruction cycle begins after that. This peroxide radical immediately creates new radical from the fatty acid methyl ester, which in turn binds with the oxygen in the air. Then the destructive radical auto-oxidation cycle starts [4]. During this process, up to 100 new radicals are created quickly from one single radical, meaning that decomposition occurs at an exponentially rapid rate and results in formation of a series of by-products. These by-products formed during the oxidation process cause the fuel to eventually deteriorate [5,6]. Finally the oil spoils and became rancid very quickly.

Oxidative rancidity begins with an initial chain reaction:

$$RH \rightarrow R^{\bullet}$$

Followed by a propagating reaction that involves unstable peroxides and hydro peroxides:

$$R^{\bullet} + O \rightarrow ROO^{\bullet}$$
$$ROO^{\bullet} + RH \rightarrow R—OOH + R^{\bullet}$$

Followed by the termination reactions resulting in aldehydes, alcohols and carbonic acids:

$$R^{\bullet} + R^{\bullet} \rightarrow R—R$$
$$ROO^{\bullet} + R^{\bullet} \rightarrow R—OO—R$$

Literature Review

The present paper discusses the importance of oxidation stability of biodiesel. Oxidative stability is an important property of biodiesel that is influenced by both FAME chemical composition and by storage and handling conditions.

Knothe has studied the dependence of biodiesel fuel properties like viscosity, heat of combustion, oxidative stability, lubricity, cold flow properties on the structure of fatty acid alkyl ester and thereby, estimated the relative rates of oxidation of saturated and unsaturated methyl esters [7].

Dunn and Knothe studied the oxidation stability of biodiesel in blends with jet fuel by analysis of oil stability index (OSI) [8]. Dunn has also studied the oxidative stability of Soybean oil fatty acid methyl esters by oil stability index [9]. Soybean methyl ester (SME) samples from five separate sources and with varying storage and handling histories were analyzed for OSI at 60 ^{0}C using an oxidative stability instrument. Results proved that OSI may be used to measure relative oxidative stability of SME samples as well as to differentiate between samples from different producers. Polavka et al. studied the oxidation stability of methyl esters derived from rapeseed oil and waste frying oil, both distilled and undistilled, by Differential Thermal Analysis and Rancimat [10].

Sarin et al. studied the influence of metal contaminants on oxidation stability of Jatropha biodiesel and observed that copper has strong catalytic effect and other metals- iron, nickel, manganese and cobalt also had strong negative influence on oxidation stability [11]. Mittelbach et al. investigated the influence of different synthetic and natural antioxidants on the oxidation stability of biodiesel produced from rapeseed oil, sunflower oil, used frying oil, and beef tallow, both distilled and undistilled [12]. He found that the induction periods of methyl esters could be improved significantly with antioxidants. He determined a good correlation between improvement of the oxidation stability and the fatty acid composition. Dunn has also studied the effect of different antioxidants on oxidation stability of biodiesel from soybean oil [13]. Liang et al. have reported that synthetic antioxidants are more effective than natural antioxidants [14].

Long storage stability studies were also carried out on biodiesels synthesized from rapeseed oil, used frying oil, high oleic sunflower oil, high and low erucic Brassica carinata oil [15-17]. Results of study suggested that to obtain a highly stable biodiesel and to avoid oxidation, it is necessary to take especial precaution during the storage such as limiting access to oxygen and exposure to light and moisture.

Park et al. have studied the blending effects of palm, rapeseed and soybean biodiesels on oxidation stability [18]. When soybean biodiesel was blended with palm and rapeseed biodiesels having higher oxidation stability, the oxidation stability of the blended biodiesel was improved.

Other limitations of biodiesel arise at low temperatures. The low temperature flow properties of biodiesel are characterized by cloud point, pour point and cold filter plugging point and these must be considered when operating compression-ignition engines in moderate temperature climate during winter months. The “cloud point” is the temperature at which a sample of the fuel starts to appear cloudy, indicating that wax crystals have begun to form which can clog fuel lines and filters in a vehicle’s fuel system and the “pour point” is the temperature below which the fuel will not flow and “cold filter plugging point” is the temperature at which a fuel causes a filter to plug due to its crystallization [19-21].

III. Conclusions

The review of the work done so far has revealed that it will not be possible to use biodiesel having low oxidation stability and poor physico-chemical properties. Thus, more emphasize should be given on fuels derived from tree borne non-edible oil seeds due to rising food-fuel issues. Large numbers of studies have been devoted to the oxidation stability of different oils.

References

[1] Purohit P., Gaikwad S., Gurav R., Conference proceeding of I-CORT, Institute of Knowledge College of Engineering,(Pune), 2012: Mech 1-5.

[2] Kumar N, Sharma PB, Das LM and Garg SK (2006). A feasibility analysis of community scale biodiesel production in India. SAE Publication No. 2006-28-0031.

[3] Standard specification for biodiesel fuel blend stock (B100) for middle distillate fuels. Report no. D6751-08. ASTM; 2008.

[4] Formo MW, Jungermann E, Noris F and Sonntag NOV. Bailey’s Indust Oil Fat Products, John Wiley and Son 1979; 1(4): 698-711.

[5] Sarin R, Sharma M, Sinharay S, Malhotra RK. Jatroha-Palm biodiesel blends: An optimum mix for Asia. Fuel 2007;86:1365-1371.

[6] E. Natarajan, Stability Studies of Biodiesel, International Journal of Energy Science JES IJES Vol.2 Iss.4 2012 PP.152-155.

[7] Knothe G. Dependence of biodiesel fuel properties on the structure of fatty acid alkyl esters. Fuel Processing Technology 2005;86:1059-1070.

[8] Dunn RO, Knothe G. Oxidative stability of biodiesel in blends with jet fuel by analysis of oil stability index. JAOCS 2003;80:1047-1048.

[9] Dunn RO. Oxidative stability of soybean oil fatty acid methyl esters by oil stability index (OSI). JAOCS 2005;82:381-387.

[10] Polavka J, Paligova J,Cvengros J, Simon P. Oxidation stability of methyl esters studied by differential thermal analysis and Rancimat. JAOCS 2005;82:519-524.

[11 Sarin A., Arora R., N.P. Singh, Sharma M.,. Malhotra R, The influence of metal contaminants on oxidation stability of Jatropha biodiesel, Jounal of Energy, 34(2009),1271-1275.

[12] Mittelbach M, Schober S. The influence of antioxidants on the oxidation stability of biodiesel. JAOCS 2003;80:817-823.

[13] Dunn RO. Effect of antioxidants on oxidative stability of methyl soyate. Fuel Process Technology 2005;86:1071-1085.

[14] Liang YC, May CY, Foon CS, Ngan MA, Hock CC, Basiron Y. The effect of natural and synthetic antioxidants on the oxidative stability of palm diesel. Fuel 2006;85:867-870.

[15] Mittelbach M, Gangl S. Long storage stability of biodiesel made from rapeseed and used frying oil. JAOCS 2001;78:573-577.

[16] Bondioli P, Gasparoli A, Bella LD. Biodiesel stability under commercial storage conditions over one year. EJLST 2003;105:735-741.

[17] Bouaid A, Mercedes M, Aracil J. Long storage stability of biodiesel from vegetable and used frying oils. Fuel 2007;86:2596-2602.

[18] Park JY, Kim DK, Lee JP, Park SC, Kim YJ, Lee JS. Blending effects of biodiesels on oxidation stability and low temperature flow properties. Bioresource Technology 2008;99:1196-1203.

[19] Dunn R, Bagby M. Low-temperature properties of triglyceride-based diesel fuels: transesterified methyl esters and petroleum distillate. JAOCS 1995;72:895-904.

[20] Dunn RO, Shockley MW, Bagby MO. Improving the low-temperature properties of alternative diesel fuels. JAOCS 1996;73:1719-1729.

[21]Coutinho JAP, Mirante F, Ribeiro JC, Sansot JM, Daridon JL. Cloud and pour points in fuel blends. Fuel 2002;81:963-967.

Voltage Stabilization of Wind Energy Conversion System using Chaos Based SVPWM Modulated Power Filter Compensator

Fatehbir Singh
A.P,EEE Deptt.
Gian Jyoti group of institutions
Shambukalan Babur highway
fatehbir9@gmail.com

Sunny Malhotra
AP ,EE Deptt.
ACET,Amritsar,India
sunnymalhotra.13@gmail.com

***Abstract* -The need to exploit ample renewable energy sources such as wind and solar is growing due to world energy shortage, financial and environmental pollution concerns. Wind energy has become one of the important alternatives because of its abundance and the strong thrust for its commercialization. However, the voltage stabilization problem of a wind energy system is dependent on changing wind conditions and varying electric load conditions. In this paper a Chaos based SVPWM MPFC controller is designed .This Chaos based SVPWM MPFC Controller is used to stabilize the varying wind energy output. The proposed controller is tested on system using Matlab Simulink Environment. The Results are compared with conventional PWM based MPFC Controller and it is found that Chaos based SVPWM MPFC controller provides better stabilization of voltage as compared to the SVPWM MPFC controller and PWM based MPFC controller also harmonic contents in load end voltage gets reduced in Chaos based MPFC controller.**

Keywords: - Chaos based SVPWM; MPFC; PWM; Wind energy

I. INTRODUCTION

Use of electricity generation from renewable energy sources increased rapidly in the last decade as industrial sector become more aware about fossil fuel shortages and their environmental impacts. Wind energy is important source of electricity as it directly converts kinetic energy of air mass into electricity [1]. Wind energy Conversion systems are environmental friendly systems and is best suitable option among renewable energy resources, power generated is dependent on the wind speed. The generator is important part of WECS [2]. Induction Generator have been most frequently used in wind energy conversion system. The advantages of using Induction Generator over synchronous generator or doubly fed induction generator are its low unit cost, ruggedness and less maintenance. Due to its constant speed operation and variable wind speed, the power fluctuations are main problem in standalone system or in hybrid system [3].

Voltage stability is a major problem for standalone wind energy conversion scheme employing induction generator, under severe wind variation and dynamic load variation. So a novel stabilization scheme is used to ensure the voltage stability, efficient power utilization and boosts power Quality for a stand-alone wind energy conversion scheme [4]. In order to improve the power quality issue in the distribution systems that are combined with distributed generation (DG), a switched modulated power filter compensator (MPFC) which is driven by a Tri-loop Error Controller is used. MPFC Controller consist of following elements: Tri- loop dynamic error driven controller, three phase diode bridge, switched capacitor, PWM controlled ideal switches ,resistance and inductance[5]. Fig.1. shows equivalent circuit diagram of MPFC Controller.

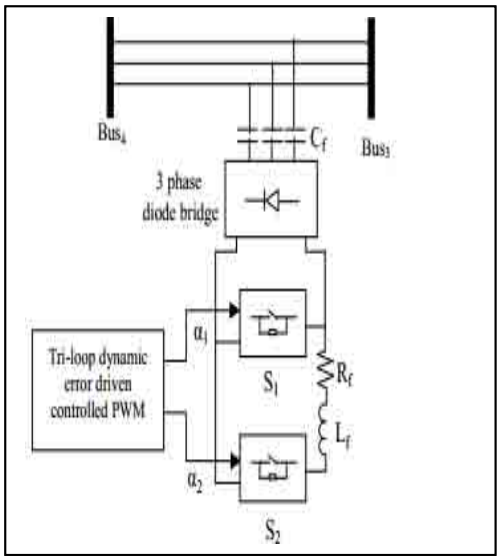


Fig.1.Shows equivalent diagram of MPFC Controller [5]

With switch in open condition and switch closed, the resistor and inductor will form the part of the circuit and the capacitor forms a low-pass filter with the inductor through the diode bridge. If switch S1 is in closed position and switch S2 is opened, the resistor and inductor will not present in the circuit and the capacitor bank will form a capacitive circuit and provide reactive power to the utility grid [6].In order to control these IGBT switches a novel tri-loop driven PID controller is used. The tri-loop error driven controller consists of three basic loops. The main loop is a voltage stabilization loop, second loop consist of current stabilization loop and third loop consist of supplementary power loop to keep a near maximum energy utilization under varying wind and load condition The voltage loop keep the voltage of system at 1p.u and current loop keep the current at 1p.u.[1].

II. WIND INDUCTION GENERATOR TEST SYSTEM

Fig.2. shows sample study system of WECS. Sample study system consists of wind turbine which is mechanically coupled to asynchronous generator which produces electrical energy output, this electrical energy is stepped up using step up transformer and is transmitted via transmission line to distribution end, level of voltage is being stepped down using step down transformer which is then fed to the consumers. Due to the presence of non linear load and varying wind conditions, voltage profile became poor so modulated power filter compensator is used to stabilize the wind energy output.

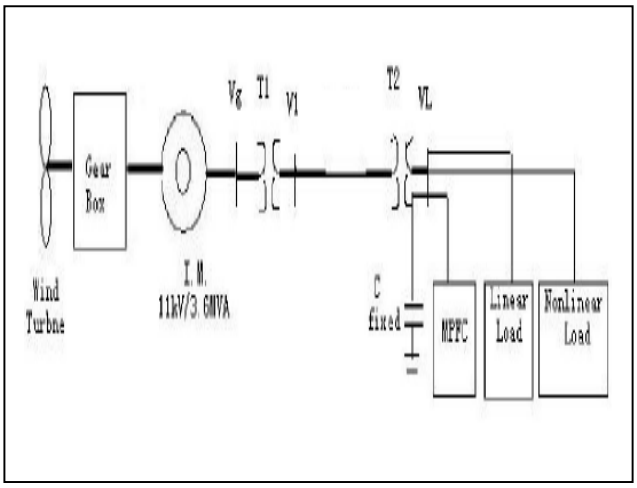


Fig. 2. Sample Wind Induction Generator Test System [1].

The sample study system is tested for serve electric load excursion. From Starting to 0.2 sec both linear and non linear load are present in the system. From 0.2 sec to 0.5 sec, only linear load is present. The performance of system is compared with controller using PWM technique and Chaos based SVPWM technique.

III. CHAOS BASED SVPWM MPFC CONTROLLER

Traditional PWM composes of many harmonic components. The distribution of harmonics is dependent on the carrier. It is also known that due to the cluster harmonics around the multiples of carrier frequency in the output waves of the conventional PWM, it is difficult to control the electromagnetic interference. Therefore combining chaos theory with the PWM, a chaos-based pulse width modulation (CPWM), is employed to distribute the harmonics of the DC-DC converters continuously and evenly over a wide frequency range. As result of which, the electromagnetic interference can be reduced [7]. Chaos-based PWM strategies using a chaotic changing switching frequency are used to widen the harmonics continuously to a large area so that harmonics can be reduced greatly. This is an effective way to decrease the harmonic and reduce ripple current and in induction motor [8].Chaotic sequence can be generated as follows: Consider a simple one dimensional tent map

$$= \qquad (1)$$

Tent map is a simple function capable of producing chaotic motion. It is dependent on initial value .where is a proper fraction. The iteration of the tent map exhibit chaotic behaviour. A periodic orbit of a map has been defined to have period t if the orbit successively cycles through t distinct points. Then, all fractions which have the form 2d/ create a periodic 2× orbit Gc of map, where both c and d are positive integers. Multiplied all numbers in by results in a set of positive integers. Rewriting map as follows:

$$= \qquad (2)$$

Where n = 0, 1,2,--n belongs to[1,0.5(−1)] .Then, when not a multiple of 5, iteration may create a periodic 2× orbit[9]

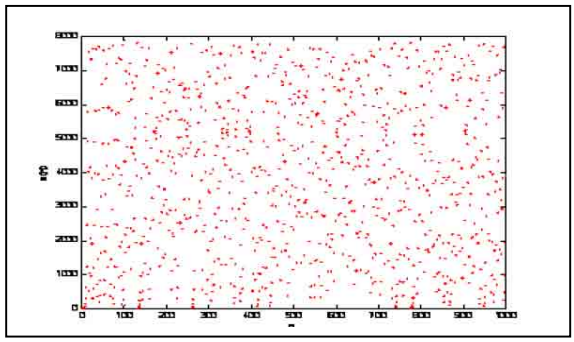


Fig.3. Positive integer sequences of uniform distribution deriving from Eq.(2), c=6[9].

The basic principle of chaos-based PWM is to use a chaotic signal to vary the switching (or carrier) frequency:

(3)

Where is the switching frequency of chaotic PWM, Chaotic sequence can be generated by iterations, thus switching frequency may be varied from to . Chaos-based PWM strategies utilized chaotic changing switching frequency to spread out the harmonics continually to a wide area so that the harmonics can be reduced greatly [7]. Chaos based PWM generator is shown in Fig. 4:

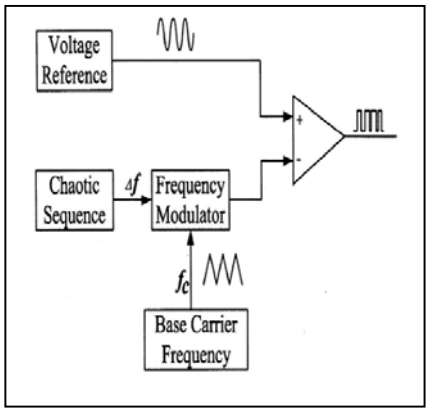


Fig. 4.Chaos based PWM generator

In the chaos based PWM generator the chaotic sequence is applied to frequency modulator whose another input is base carrier frequency and which produces output which is fed as input to the comparter whose another input is reference sine voltage wave which then produces chaos based PWM waves The chaotic signal Fm(t) is then applied to frequency modulator. As be seen from the Fig. 4, the chaotic modulation is a very simple addition to an existing sine-triangle modulator [6].Conventional SVPWM uses fixed switching frequencies, while CSVPWM strategies utilize a chaotic changing switching frequency. Their switching frequencies are varied each cycle [8].

IV. SIMULATION MODEL

Simulink Model of Wind Energy Conversion System is shown in appendix Fig. 13.Here the induction machine equipped with wind turbine act as induction generator. The output of induction generator is fluctuating in nature due to variable wind speed and series of load excursion that are there on the system. Different types of loads that are present on the system are linear load of 100 KVA and non linear load of 100 KVA. Out of 100 KVA non linear load, 50KVA non linear load is present for .02sec and 50 KVA non linear load is present for 0.2sec and 100KVA linear load is present for 0.5sec. A Chaos based SVPWM MPFC controller is used for voltage improvement and the result obtained through simulation is compared with PWM MPFC controller. Given simulation model run under continuous mode.

V. SIMULATION RESULTS

Simulation results are obtained by employing two controllers on the given system as shown in Fig.13. Firstly a Chaos based SVPWM MPFC controller is employed on the system and then afterwards PWM based controller is applied and it s found that results obtained with Chaos based SVPWM controller is better than that of results obtained with PWM based controller

Case a). When Chaos based SVPWM MPFC controller is used: With Matlab/Simulink environment variation of load end voltage v/s time shown in Fig 5, load end current v/s time shown in Fig.6, sending end voltage v/s time shown in Fig.7 and sending end current v/s time shown in Fig.8 are obtained

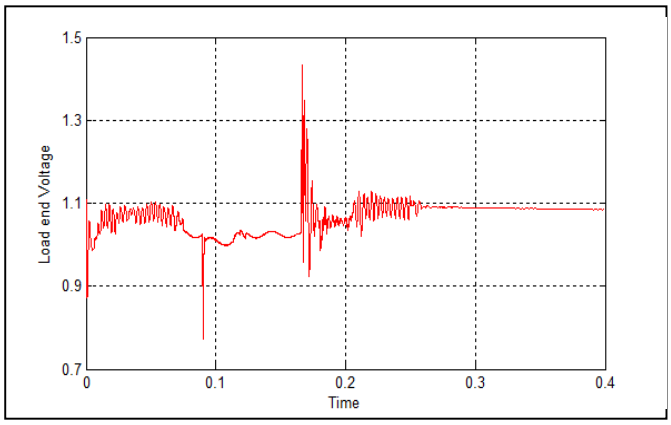


Fig.5. variation of load voltage v/s time of chaos based SVPWM MPFC controller

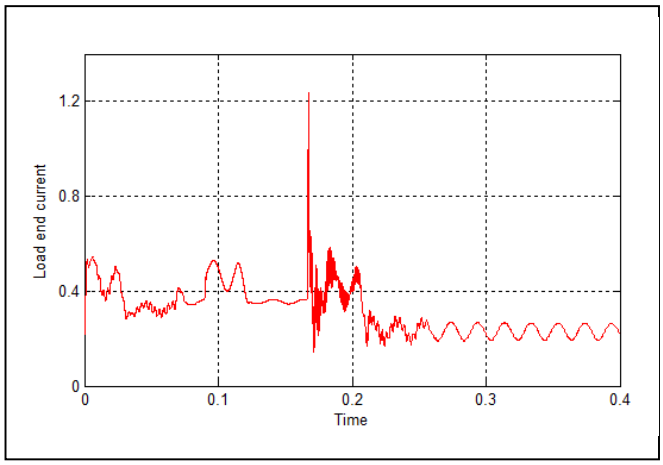


Fig.6. variation of load current v/s time of chaos based SVPWM MPFC controller

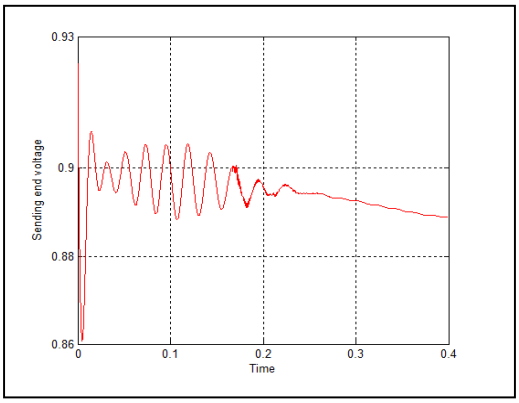


Fig.7. variation of sending end voltage v/s time of chaos based SVPWM MPFC controller

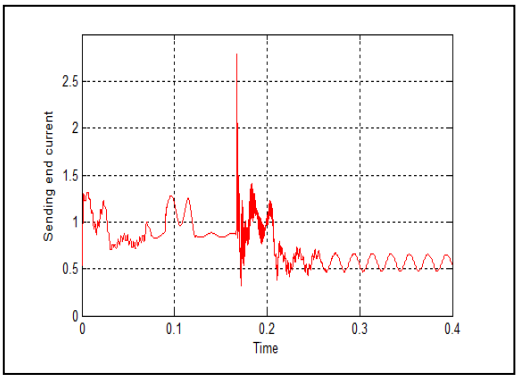


Fig.8. variation of sending end current v/s time of chaos based SVPWM MPFC controller

Case b).When PWM based MPFC controller is used: With Matlab/Simulink environment variation of load end voltage v/s time shown in Fig 10, load end current v/s time shown in Fig.11, sending end voltage v/s time shown in Fig.12 and sending end current v/s time shown in Fig.13 are obtained.

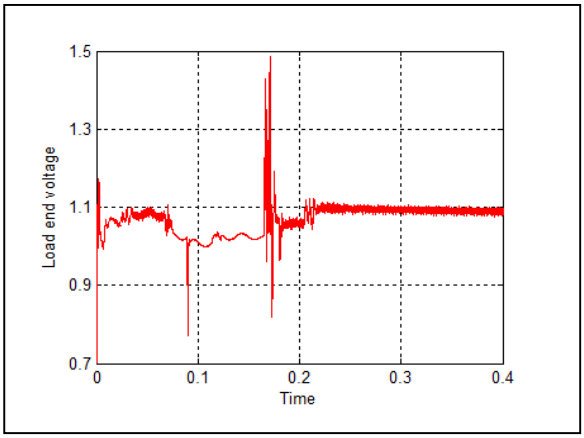


Fig.9. variation of load end current v/s time of PWM based MPFC controller

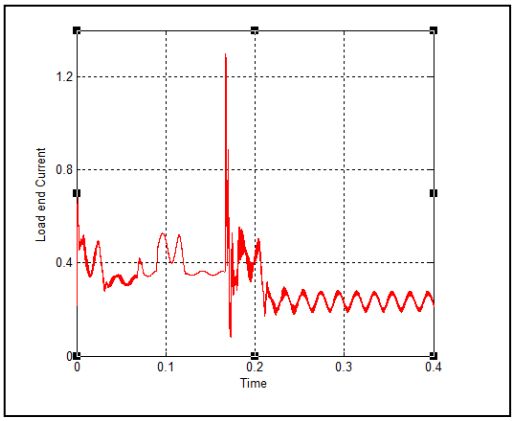


Fig.10. variation of load end current v/s time of PWM based MPFC controller

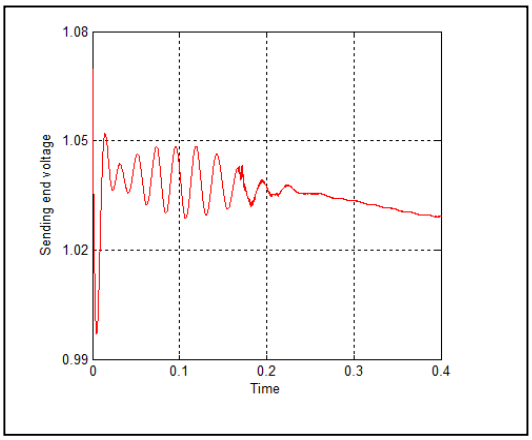


Fig.11. variation of sending end voltage v/s time of PWM based MPFC controller

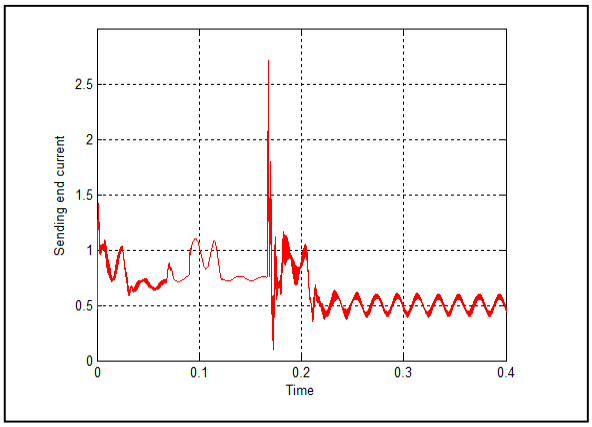


Fig.12. variation of sending end current v/s time of PWM based MPFC controller

Table1. Results with different controller used:

S.No.	Controller With different PWM technique used	Voltage profile on load end side	Harmonics content in output voltage and current
1	PWM based Controller	Distorted	Large
2.	Chaos based SVPWM Controller	Less distorted as compared to PWM based Controller	Small as compared to PWM based Controller

VI. Conclusion

In This Paper, Chaos based SVPWM MPFC controller is successfully designed for providing dynamic voltage stabilization in wind energy conversion system. This control strategy is compared with conventional PWM based MPFC controller for the system as shown in Fig. 13. Simulation results indicate that Chaos based SVPWM MPFC controller provides better voltage stabilization as compared PWM based MPFC controller.

VII. Appendix

A. Data

Data for various components used in matlab simulink model of Fig. 13. are as follows:

1. System per unit base:

   /25KV/600V
   (Generation/Transmission/Load end)
2. Induction Generator Parameters:
   a. Stator:
   b. Rotor:
3. Transformer Parameters:
   11KV/25KV (L-L) Transformer (T1)
   a. Generation side: 11KV/3.6MVA,R=.002 pu L=.08 pu
   b. Load side: 25KV/3.6MVA, R=.002 pu L=.08 pu
   25KV/600V (L-L) Transformer (T2)
   c. Generation side: 25KV/3.6MVA R=.002 pu L=.08 pu
   d. Load side: 600V/3.6MVA R=.002 pu L=.08 pu
4. Transmission Line/Feeder: Length: 10km
   a. Positive Sequence parameters: 0.01273ohms/km
   b. , 12.74e-9 F/km
5. The Chaos based SVPWM switching power filter: Filter capacitor bank:=1.7 mF/phase
   a. Filter inductance:=30mH
   b. Filter resistance:
6. Tri loop error driven PID Controller:,PID Controller Gains :
7. Load sequence excursions:
   a. From 0s to 0.2s: linear load 200KVA (50%)
      Non linear load 200KVA (50%)
   b. From 0.2s to 0.5s: linear load 200 KVA (50%) only

B. Simulation diagram

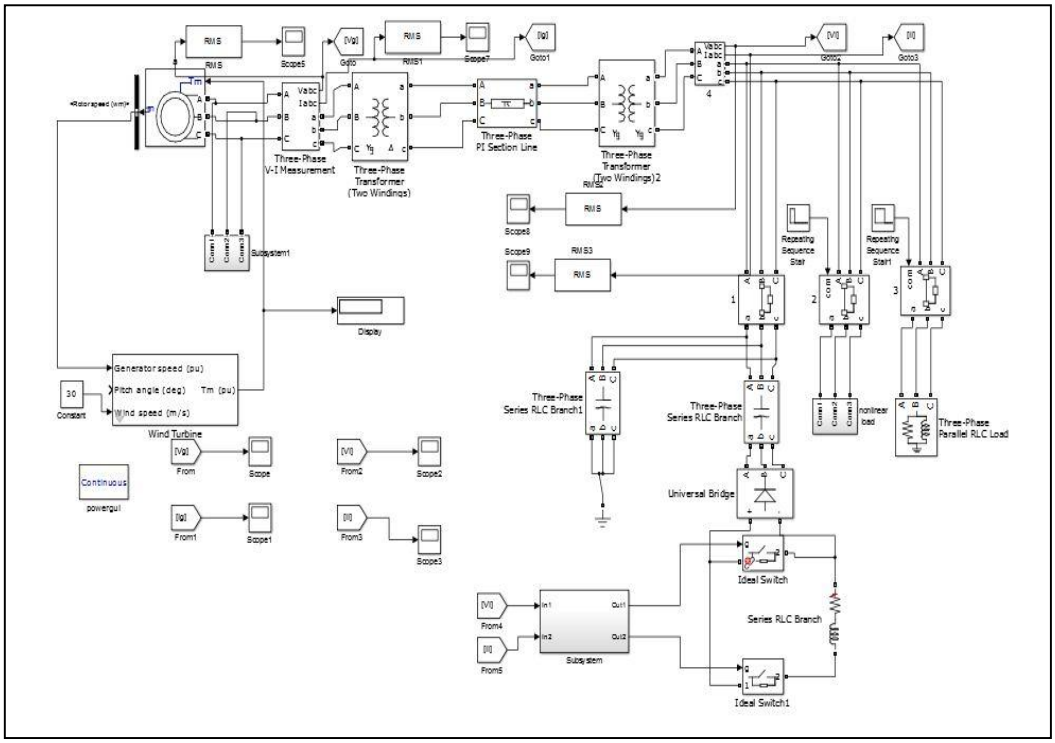


Fig.13. Simulation Diagram for Wind energy conversion system using chaos based SVPWM MPFC controller

C. Subsystem for Chaos based SVPWM MPFC controller

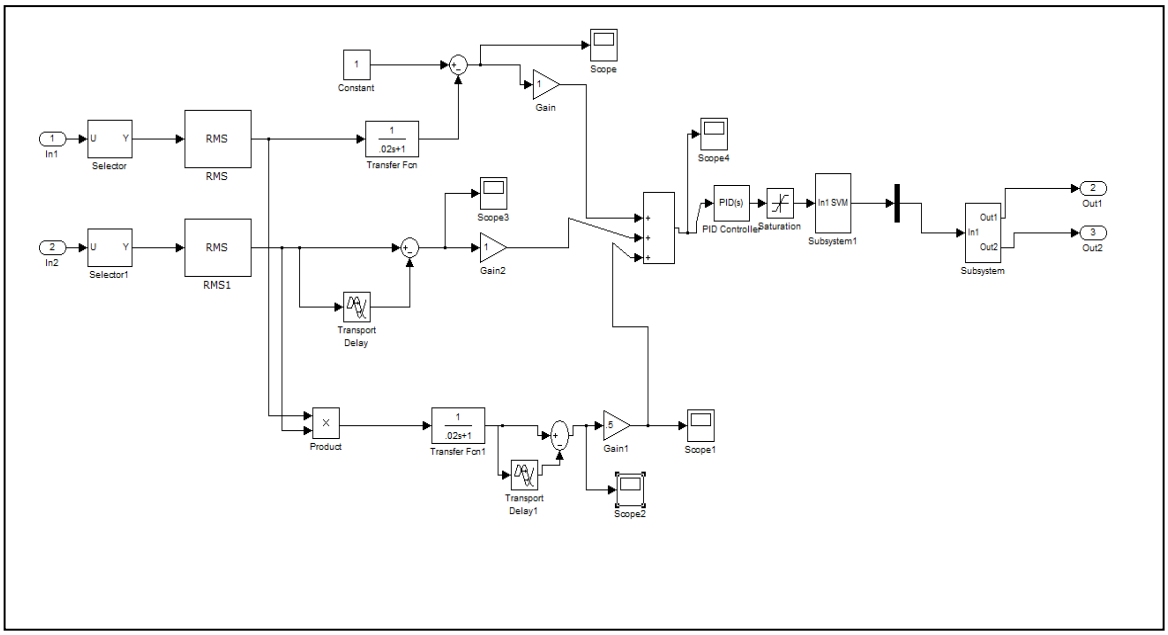


Fig.14. Subsystem for Chaos based SVPWM MPFC controller

VIII. REFERENCES

[1] Abel. M .Sharaf and Weihua Wang "A Low-Cost Voltage Stabilization and Power Quality Enhancement Scheme for a Small Renewable Wind Energy Scheme," IEEE International Symposium on Industrial Electronics, Vol. 3, pp. 1949-1953, 2006.

[2] Neha Adhakari, Bhim Singh and A .L. Vyas "Design of standalone wind energy conversion system using sensorless MPPT approach", IEEE conference on sustainable energy technologies, pp 409, 2012.

[3] W. Huang, "Direct voltage control for standalone wind energy conversion system using induction generator and energy storage", IEEE Electric Power conference, pp 1-8, 2008.

[4] A.M.Sharaf and Guosheng Wang "Wind energy system voltage and energy enhancement using low cost dynamic capacitor compensation scheme", IEEE international conference on Electric, Electronics and Computer engineering, pp 804-807, 2004.

[5] T. Aboul, "A novel modulated power filter compensator scheme for standalone wind energy utilization systems," Canadian conference on Electrical and Computer Engineering, pp 390-393,2009.

[6] A.M. Sharaf, Weihua Wang and Ismail .H. Altas "An novel modulated power filter compensator for distribution network with distributed wind energy" International journal of emerging electric power system, Vol 8, pp 549-555,2007

[7] H. Li, B. Zhang, Z. Liu and G. Chen "Controlling Dc-Dc converter by chaos based pulse width modulator to reduce EMI", Chaos, Solitors and Fractals, Vol 42,pp 1378-1387, 2009.

[8] W.Cui, K. T, Chau ,Z. Wang and J. Z. Jiang "Application of chaotic modulation to ac motor for harmonic suppression", IEEE conference on Industrial Technology, pp 234-237, 2006

[9] Y. Lu, X. Huang ,B. Zhang and Z. Mao "Two chaos based PWM strategies for suppression of harmonics" Proceedings of the 6th World Congress on Intelligent Control and Automation, pp. 953-957, 2006

Books :

[10] John K. Kaldellis "Comprehensive Renewable Energy," Vol. 2, Elsevier Ltd., 2012

[11] Muhammad H. Rashid, "Power Electronics Circuits, Devices and Applications." Pearson Education, Inc., 2004.

.

Effect of etchant concentration on track density registered on LR 115 as SSNTD.

Neerja
PG Department of Physics and Electronics,
DAV College, Amritsar, Punjab, India.
Corresponding author: sameerkkalia@yahoo.co.in

Sameer Kalia
PG Department of Physics and Electronics,
DAV College, Amritsar, Punjab, India

Abstract- α-particle track etch rates in Kodak LR-115 have been recorded by using NaOH solution as an etchant at different normalities (2.5N, 4N and 6N) at (58±2)˚C. Optical microscope was used to measure track density after etching of solid state nuclear track detector. It is observed that track density in the detector exposed to atmospheric air changes with normality.

Keywords- Track etch rate, Kodak LR-115, normality, optical microscope, track density.

I. Introduction

Solid state nuclear track detectors (SSNTD) are used widely in several technical applications for the detection of charged particles from protons to heavy ions, as well as the simple registration of the particle flux density or the fluencies in the environmental dosimetry [1].The passage of heavily ionizing nuclear particle through insulating solids changes the physical, chemical and other properties of the solid along and around the path of the particles and creates narrow paths of intense damage on an atomic scale. The narrow paths created are called latent tracks or etch pits and the insulating damage materials known as solid state nuclear track detectors. They are unaffected by humidity, low temperatures, moderate heating and light. The etched detectors can usually be stored for longer periods of time under various environmental conditions without changing tracks number, or its shape [2]. The technique of enlarging the latent tracks of radiation damaged with suitable chemical agent is called chemical etching. The type of damage produced by irradiation of solid depends not only on the nature of the solid itself. The shape of the etched track in certain materials depends not only on the charge, mass and the velocity of the incoming particle but also on the nature and concentration of the etchant. Many authors had established that the thickness of the removed layer during etching of the solid state nuclear detector is one of the main factors influencing the track characteristics [3-5].Other factors, which determine the track parameters are incident angle and impact angle characteristics, energy and charge of the incident particle. The removed layer of LR-115 is also a decisive factor which influences the detector performance relevant for particle detection of particularly α-particles [6]. The thickness of the removed layer is very important when this detector is used for radon measurements and α- autoradiography. In the present work an attempt has been made to study the effect of varying normality of the etchant on the track density of α-particles observed on LR 115 detector used as SSNTD.

II. Experimental Technique

A. LR 115 Type II SSNTD's (Cellulose nitrate plastic detectors)- The cellulose nitrate plastic detector, commercially known as LR-115 types II manufactured by Kodak-Pathe, France is used for the objective. It is a film made of clear polyester base 100 µm thick on which a red layer of special cellulose nitrate of thickness 11.5 to 12.0 µm is coated. Cellulose nitrate films have been commonly used as solid-state nuclear track detectors (SSNTDs) in which visible tracks can be revealed after ion irradiation and suitable chemical etching. The use of the cellulose nitrate solid-state nuclear track detector which is one of the most commonly used SSNTDs depends critically on the thickness of etched-away cellulose nitrate layer during chemical etching[7-10]. The structural formula for the SSNTD used is as shown in fig.1.

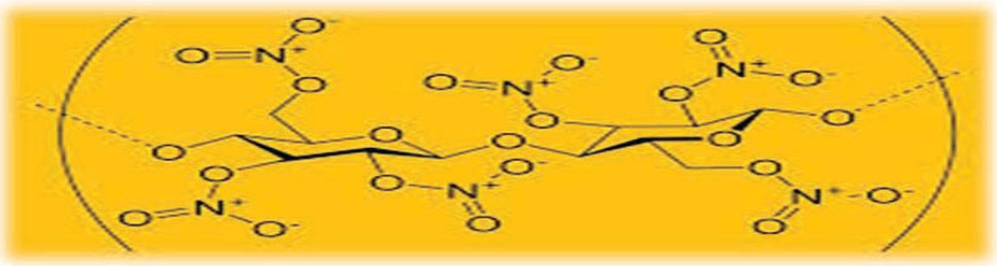


Figure 1: Structural formula of cellulose nitrate

B. Etching Bath- Chemical etching is essential for enlargement of the tracks, so that they become visible under the optical microscope. The etching of samples was carried out in a constant temperature bath manufactured by Narang Scientific Works Pvt. Ltd. New Delhi. It provides an accurate and precise temperature control of the etchant solution with an accuracy of $\pm$1˚C.

C. Optical Microscope- The visible tracks can be counted either by direct observation using an optical microscope or with the help of automated counter [11].Tracks in the samples after etching were scanned by using Binocular microscope with magnification of 400X and has a resolution of 1 μm. It has motion along three mutually perpendicular directions. This microscope can be used in any stage of phase contrast, color contrast and in dark /bright fields. It has also the facility for its operation in the reflection mode.

D. Methodology- The detectors films used in this study were of size 1.5cm x1.5cm ,suspended for a period of 90 days in the different villages of region from Manawala to Jandiala Guru under Amritsar district of Punjab (covering living rooms, dining rooms, bedrooms and bathrooms) at a height 9 feet above the ground level and about 2 feet below the ceiling and away from the walls so that the direct α-particles from the building material of the dwellings do not reach the detectors films. The detectors were removed after three months (from Jan.–March, 2014).Then these samples were etched using **6N,4N and 2.5N NaOH** solution as an etchant at (58 ±2))˚C for 90 minutes in above mentioned etching bath. The track density(number of tracks per unit area) was counted using an optical microscope at 400X magnification.

III. Observations

The values for track density observed at different normalities of etchant solution are summarized in table 1 for samples suspended at various locations of mentioned region as shown below.

Table 1: Values of track density(number of tracks per unit area) observed on SSNTD's at different normalities

Sample no.	Track density at 6N	Track density at 4N	Track density at 2.5N
1.	0.421	0.312	0.232
2.	0.335	0.302	0.121
3.	0.375	0.308	0.214
4.	0.492	0.402	0.35
5.	0.138	0.100	0.087
6.	0.277	0.125	0.075
7.	0.284	0.142	0.120
8.	0.213	0.137	0.125
9.	0.391	0.315	0.153
10.	0.236	0.102	0.086

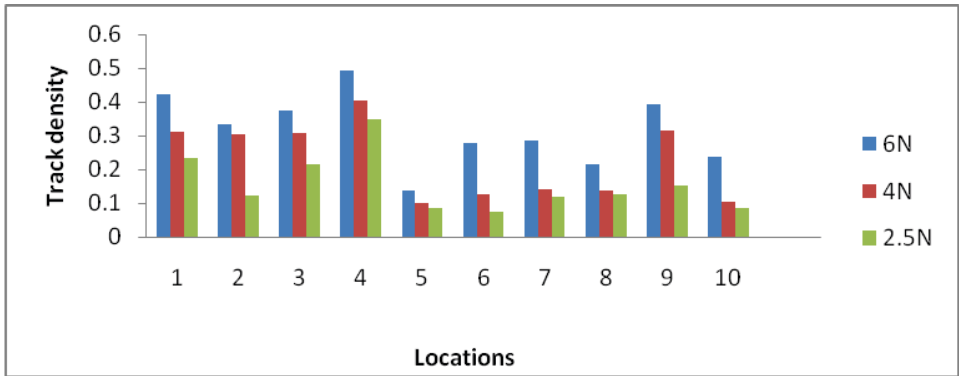


Figure 2 : Graphical presentation of track density vs normality

IV. Results and Discussion

The α-particle track density measured for different locations of district Amritsar, Punjab, are reported in table 1 and it has been found that by changing the normality of etchant solution there is change in track density under same environmental conditions. The changing relation between the etchant concentration and the track density may be related to the attack by hydroxide ion results in the hydrolysis of the carbonate ester bonds and the release of polyallyalcohol from the polymer network [12]. The result obtained is consistent as observed by T.M. Hegazy et al [13].

V. References

[1] D.Hermsdorf, M. Hunger, S. Stark, F. Weickert, Measurement of bulk etch rates for poly-allyl-diglycol carbonate (PADC) and cellulose nitrate in a broad range of concentration and temperature of NaOH etching solution, Radiation Measurements, 42 (2007), pp. 1–7.

[2] G. A. Khougeer, "Measurement of Radon Concentration in Students residential Buildings at King Saud University in Riyadh Using Nuclear Track Technique", Thesis Submitted in Partial Fulfillment in the degree of Master of Science in the Department of physics, at college of science, at KSA, January 1997.

[3] G Somogy, Nucl. Instrum. Methods 173, 21 (1980).

[4] G Somogy, A S Sazaly, Nucl. Instrum. Methods 109, 211 (1973).

[5] G Jonsson, Nucl. Instrum. Methods 10, 407 (1981).

[6]T A Salama, U Seddik, T M Hegazy and A Ahmed Morsy, Parmana Journal of Physics, Vol. 67, No. 3,September 2006, pp. 529-534.

[7] V.A. Nikolaev, R. Ilic, Etched track radiometers in radon measurements:a review, Radiat. Meas. 30 (1999) 1–13.

[8] D. Nikezic, K.N. Yu, Formation and growth of tracks in nuclear track materials, Mater. Sci. Eng. R 46 (2004) 51–123.

[9]R.L. Fleisher, Ion tracks, in: J.H. Westbrook, R.L. Fleischer (Eds.), Intermetallic Compounds Principles and Practice, vol. 3, John Wiley, 2002, p. 263.

[10] F.M.F. Ng, K.N. Yu, Materials Chemistry and Physics ,Vol.100 (2006) ,pp 38–40.

[11] N. Tsoulfanidis," Measurement and detection of radiation" Hemisphere Publishing Corporation, 1983.

[12] J.A. Brydson, Plastics based on styrene, Plastics materials, Butterworth Scientific, London (1975), pp. 386–422.

[13] T.M. Hegazy,M.Y.Shoeib, G.M. HassanBeni-Suef University Journal of Basic and Applied Sciences,Volume 2, Issue 1, March 2013, Pages 36–40.

Plant Leaf Classification using Texture Features

Nancy Jindal
Assistant Professor EEE department
Amritsar College of Engineering and Technology
Amritsar
Er.nancyjindal@gmail.com

Naveen Kr. Singla
M.Tech Student
Thapar University
Patiala

***Abstract*— Plants has very useful in foodstuff and medicine industries and also plays very important role for environment protection. However it is an important task to recognize them. Design a recognition system which can facilitate classifying plants and managing those plants. In this paper, leaf database is taken and then apply some methods to extract features so that this process can be done. GLCM, Gabor Filter, LBP are some of those methods.**

***Keywords*— GLCM, Gabor Filter, LBP and features.**

I. INTRODUCTION

Plant leaf classification is based on leaf identification and is becoming a popular trend.[3] Each leaf carries substantial information that can be used to identify and classify the origin or the type of plant. The recognition and identification of plant helps in exploring genetic relationship of plant and explain the evolution law of plant system. Though the plants can be recognized and identified by their leaf, flower, stem, and fruit and so on to extract discriminating features. These discriminating features can be directly observed and obtained by people when they observing leaf images, people expect to fulfill the recognition and identification of plant automatically or semi-automatically by computers. However, it is a time consuming task. Researchers have tried to recognize a plant using high quality leaf images and complex mathematical formulae for computers to decide the origin and type of plants.[4].

II. OBJECTIVE

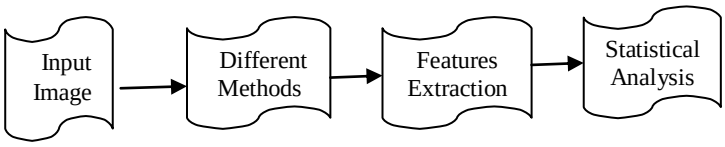
The objective is to classify the plants leaves based on the features that are extracted from different methods. The development tool used will be MATLAB®, and emphasis will be only on the software for performing classification, and not hardware for capturing an image.

- To collect the images from different sources.
- Extract the features from different methods.
- Comparison will be done based on these methods.

III. ALGORITHM

- Read the image from the ImageCLEF database.
- Otsu Thresholding is also done so that local variance should be minimal.
- By this gray level image is converted to BW image.
- Then normalize the image by normalization method.
- Then calculate the GLCM technique and from the matrix features are extracted.
- Similarly, Gabor filter and LBP are calculated and based on that calculate the features.
- Compare the results of the output images based on the methods.

IV. BLOCK DIAGRAM



V. THE DATABASE

The Image CLEF Database is a collection of different species of plants almost noise free.

VI. FEATURE EXTRACTION TECHNIQUES

i INTENSITY BASED FEATURES

Four Intensity based features are extracted namely: mean, intensity, standard deviation, skewness and kurtosis from an histogram is calculated.

ii GRAY LEVEL CO-OCCURRENCE MATRIX

The Gray Level Co-occurrence Matrix (GLCM) is method to extract second order statistical features.GLCM is a matrix consists of no of rows and columns equal to the gray level of image. The special relationship is defined as the pixel of interest and pixel to its immediate right. Each element in the resultant GLCM is simply the sum of the number of times that the pixel with value occurred in specified spatial relationship to a pixel value in the input image. The features are angular second moment, contrast, correlation, variance, inverse difference moment, sum average, sum variance, entropy, sum entropy, difference entropy, difference variance, maximum correlation coefficient, cluser shade and cluster prominence. [1],[2]

iii GABOR FILTER

Gabor Filter is defind as the product of Gaussian kernal and complex sinusoid[5]. A 2D gaussian filter with a spread of σ in both directions is as follows. We use θ=90 as standrad values for plant leaves.

iv LOCAL BINARY PATTERNS

Local Binary Patters (LBP) is an image operator as introduced by Ojala et al[6] which efficiently summarizes the local structure. It compares the pixel with its neighborhood pixel and use to describe local pattern of the image. The original version of the local binary pattern operator works on the 3 x 3 pixel block of image. The pixel in this image is threshold by its central value and then multiplies by the power of 2 according to the position and then summed up to form a decimal number to obtain a label of LBP. There are 8 neighborhood pixel for every step so there are total 2^8=256 different labels of one image. The label depends on the central pixel and their neighborhood pixel[7]. Formally given a pixel at pixels at (x_c,y_c) the resulting LBP is expressed as

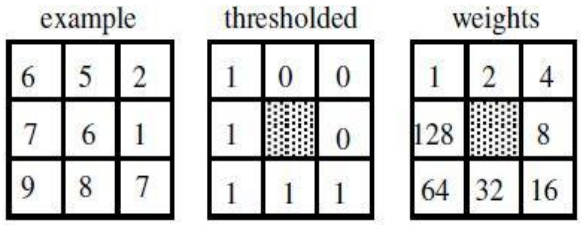
$$LBP(x_c, y_c) = \sum_{P=0}^{P-1} s(g_p - g_c)2^P$$

Where and are the pixel values of gray values of central pixel and P surrounding pixels in the circle

neighborhood with a radius R and function is defined as

$$s(x) = \begin{cases} 1, if\ x \geq 0 \\ 0, if\ x < 0 \end{cases}$$

It is clear from above expression that LBP is invariant to monotonic gray scale transformation which preserves pixel intensity order in local transformation. If image is rotated then the surrounding pixel in each neighborhood is also moved along the perimeter of the image. The contrast is measure by the formula



LBP = 1 + 16 +32 + 64 + 128 = 241
Pattern = 11110001
C = (6+7+8+9+7)/5 - (5+2+1)/3 = 4.7

VII. COMPARISON

Fig: 1. Original Image

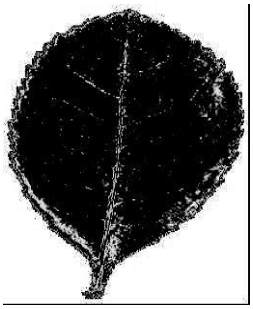


Fig:2. Filtered Image

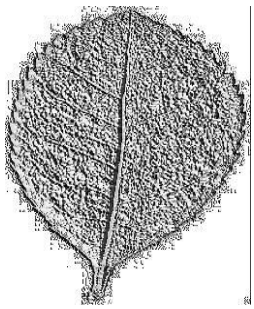


Fig:3. LBP Image

We can see from this figure that Gabor Filter gives edge of image irrespective texture of the leave but LBP gives image based on local texture and local contrast.

VIII. CONCLUSION

As the feature extraction of different images and after the statistical analysis of the features we can classify the different species of plants based on that. Local Binary Patterns described the local structure and based on the pixel value and its neighborhood pixels. The measure of Contrast gives a very important result and gives the local contrast of an image and very well useful for texture of the image

References

[1] R. M. Harlick, K. Shanmugam, I. Dinstein, "Texture Features for Image Classification.", IEEE Transactions on systems, man and cybernatics, Vol. 3(6), pp. 610-621, 1973.

[2] F. Albregsten, "Statistical Texture Measures Computed from Gray Level Coocurrence Matrices.", Image Processing Laboratory, Deptt. Of Informatics, University of Oslo, 2008.

[3] J. Du, X. Wang, G. Zhang, "Leaf shape based plant species recognition.", In proceedings: Applied Mathematics and Computation, pp. 883-893, 2007.

[4] S. Dhaygude, N. Kumbhar, "Agricultural plant Leaf Disease Detection Using Image Processing.", Int. Journal of Adcanced Research in Elect., Electronics and Inst. Engg, Vol. 2(1), 2013.

[5] M. Idrissa, M. Acheroy, "Texture classification using Gabor filters.", Pattern Recognition Letters, pp. 1095-1102, 2002.

[6] T. Ojala, M. Pietikainen, T. Maenpaa, "Multiresolution Gray Scale and Rotation Invariant Texture Classification with Local Binary Patterns", Univ. of Oulu.

[7] D. Huang, Y. Wang, "Local Binary Patterns and Its Application to Facial Image Analysis: A Survey.", IEEE Transactions on systems, man and cybernatics-Part C: Applications and reviews, Vol. 41(6), 2011.

[8] [8] X. Xianchuan, Z. Qi, "Medical Image Retrieval Using Local Binary Patterns with Image Euclidean Distance.", University of China, China.

Empirical study of structural analysis for even-even nuclei in rare earth landscape

Neeru Gupta
D A V College
Amritsar
e-mail: gneeru2007@yahoo.co.in

Sameer Kalia
D A V College
Amritsar
sameerkkalia@yahoo.co.in

***Abstract*- The scheme of nuclear energy levels which results from the collective motion of the nucleons in the core and interplay between the motion of loosely bound surface nucleons depend upon the strength of the coupling between them. The rotation arise from the motion of nuclear core. According to collective model, the low lying rotational levels be characterized by the sequence of states with I= 2^+, 4^+, 6^+ etc. and ratio of excitation successive states carry a constant value. In our work, we have taken experimental excitation energies of all even-even rare earth elements and plotted them against different parameters like mass numbers, isospin etc. and have tried to find if there is any spontaneous breaking of rotational symmetry.**

Key words- collective model, rotational levels, rare earth elememts

I INTRODUCTION

Two major phenomenological approaches that successfully describe nuclear collectivity are interacting boson model (IBM) [1, 2] and the geometric collective model (GCM) [3–5] . While the IBM model is purely algebraic, based on a bosonized form of the many-body problem with even numbers of fermions, the GCM model follows from a geometric description of nuclei using the Bohr-Mottelson (BM) Hamiltonian [6].

Quantum phase transitions are of great interest in many areas of physics, and their manifestations vary significantly in different systems. For nuclear systems, the IBM reveals rich features of their shape phase transitions [7–16]. The purpose of this paper is to discuss the main concepts of the rapid changes in structure of lanthanide and actinide nuclei by using some good indicators like energy ratios and two neutron separation energies.

II ENERGY RATIOS AND NUCLEAR SHAPE TRANSITIONS

As discussed by Khalaf[17], nuclear shape transitions are the proof of the collective motion modes of nuclei. One of the best indications of shape transition is the behavior of the ratio between the energies of the first 4^+ and 2^+ states

$$R(4/2)=E(4^+)/E(2^+) \qquad (1)$$

along the isotopic chain. The members of vibrational nuclei have excitation energies

$$E(I)=C(I)(2) \qquad (2)$$

where C is the vibrational constant. So that the energy ratios are

$$R((I+2)/I_{vib}=I+2/I(3) \qquad (3)$$

The R(4/2) varies from the value which correspond to vibrations around a spherical shape of vibrational nuclide R(4/2)=2 to the characteristic value for excitations of well deformed rotor R(4/2)=3.33. That is, the energy ratio R(4/2) shows sharp change in rapid transitional region. Even-even nuclei can be classified roughly according to ratios R(4/2) as:
1.0 $<R(4/2) <$ 2.0 for magic nuclei,
2.0 $<R(4/2) <$ 2.4 for vibrational nuclei,
2.4 $<R(4/2) <$ 2.7 for -unstable nuclei,
2.7 $<R(4/2) <$ 3.0 for transitional nuclei,
3.00 $<R(4/2) <$ 3.33 for rotational nuclei.
To give the characteristics of the evolution of the collectivity in even-even nuclei, we study the behavior of the energy ratios R(4/2) and R(6/4). For the nuclei included in our study, all chains of lanthanides begins as vibrational with R(4/2) near 1.5 and move towards rotational (R(4/2) – $\rightarrow$3.5) as neutron number increases.

III ELECROMAGNETIC TRANSITION STRENGTHS

When the nucleus is deformed it acquires an electric-multiple moment. Consequently as it oscillates, in $\lambda\mu$ mode, it emits electric $\lambda\mu$ radiation. Now to calculate the radiative transition rates between vibrational states, we need the nuclear electric multiple operator $\widehat{M}$.This is given by

$$\widehat{M} = \int d\tau \rho_c(r)\, \lambda Y_{\lambda\mu}(\theta,\phi) \qquad (4)$$

$\rho_c(r)$is the charge density of the nucleus. The electric multipolemoment is defined by

$$Q_\lambda = \left(\frac{16\pi}{(2\lambda+1)}\right)^{\frac{1}{2}} M(E\lambda,0) \qquad (5)$$

Electric quadruple moment Q_2 of a nucleus is a measure of the deviation of the charge distributionfrom spherical symmetry.

Table I Variation of E2 and E2/E4with N and Z

IV THE TWO NEUTRON SEPARATION ENERGIES

The energy required to remove a neutron from a nucleus with *Z* proton and *N* neutron is called separation energy and isdefined as:

$$Sn(Z,N) = [M(Z,N-1) + Mn - M(Z,N)]C^2 \quad (6)$$

This expression can be rewritten in the form of binding energy as:

$$S_n = B(Z,N) - B(Z,N-1) \quad (7)$$

N	Z	A	N-Z=A-2Z	E2	E4/E2
78	58	136	20	522.2	2.516565
82	58	140	24	1596.237	1.305107
84	58	142	26	641.282	1.901457
82	60	142	22	1575.78	1.333173
84	60	144	24	696.561	1.887371
86	60	146	26	453.77	0.229676
88	60	148	28	301.72	2.49304
90	60	150	30	130.21	2.926811
82	62	144	20	1660.027	1.319792
86	62	148	24	550.225	2.14505
88	62	150	26	333.955	2.315803
90	62	152	28	121.7818	3.009311
92	62	154	30	81.981	3.25462
88	64	152	24	344.279	2.194139
90	64	154	26	123.0709	3.014521
92	64	156	28	88.97	3.239148
94	64	158	30	79.512	3.288268
96	64	160	32	75.26	3.302153
90	66	156	24	137.77	2.933803
92	66	158	26	98.918	3.20608
94	66	160	28	86.7878	3.2703
94	68	162	26	102.04	3.230302
96	68	164	28	91.38	3.276756
98	68	166	30	80.5776	3.288631
100	68	168	32	79.804	3.309218
102	68	170	34	78.599	3.309813
98	70	168	28	87.73	3.266283
100	70	170	30	84.25468	3.292755
102	70	172	32	78.7427	3.305297

104	70	174	34	76.471	3.309974
106	70	176	36	82.135	3.309795

V RESULTS AND DISCUSSIONS

The excitation energies of low lying states as a function of charge number Z ranging from 58 to 72, neutron number N ranging from 75 to 110 and mass region 133 to 180 are presented in figure (1, 2, 3). Only the states of positive parity and spin $I^{\pi} = 2^{+}, 4^{+}$, have been included. The even-even Lanthenides and Actinides have been considered.

The trend of decreasing excitation energies of 2^{+} states with increasing neutron number implies a corresponding fall in deformation as N = 82 shell is approached. In Lanthenide isotopes, we can see that energy values change almost linearly for N≤ 88 and become almost flat for N≥90. This is in agreement with the onset of Z = 64 subshell effect. In Z vs E_2 curve, we find the same effect for Z = 62 after which E_2 is almost straight. Similar fact is observed in A and E_2.

Figure 3 shows that limits are fulfilled in $^{152\text{-}156}$Nd isotopes respectively. There is a smooth transition between them. These nuclei can be considered as transitional nuclei.

Figure 4 is a plot of R(4/2) against N. Thre is a change in curvature, from concave to convex. The behavior is changing from typical shell to near mid shell. Same data for Lanthenide group is plotted between R(4/2) against Z and A and results are consistent.

The nuclei of Lanthenides region would therefore be candidates for a shape transition, vibrator to axially rotator. Nucleus with A = 154 gave evidence for first order phase transition behavior of S_{2n} around N = 90 also indicate that phase shape transitions may occur in this region.

The systematics of the excitation energies of the low-lying states as a function of neutron number changing from 84 to 100 in the even-even lanthanides Nd/Sm/Gd/Dy isotopes in the mass region 144–166 and the actinide Th/U isotopes in the mass region 224–238 are presented in Figures (1,2). Only the yrast state of positive parity and spin *I*_ = 2+; 4+; 6+; 8+ and 10+ has been included. The trend of increasing excitation energy of 2+ state with decreasing neutron number, implying a corresponding fall in deformation as the N = 82 shell closure is approached. The energies of the 4+ and 6+ states also display the same trend. For lanthanides isotopes we can see that the energy values for each spin I states change almost linearly for *N* _ 88 and become quite flat for *N* _ 90. This is consistent with the onset of the Z = 64 sub-shell effect. Furthermore, the linear falling of the energy value for each I state as N goes from 86 to 88 seems to justify the linear variation of the effective proton-boson number in each isotope series.

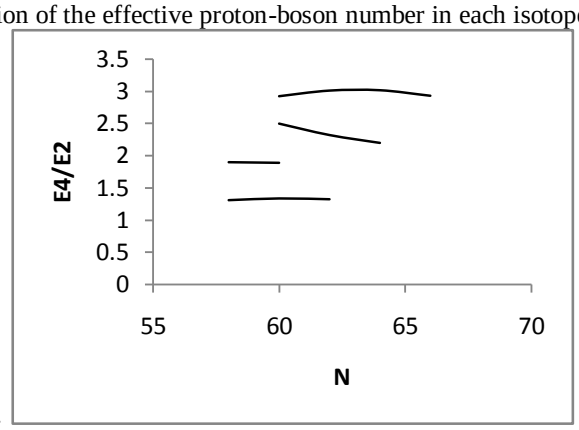


Fig. 1. Variation of E4/E2 vs N

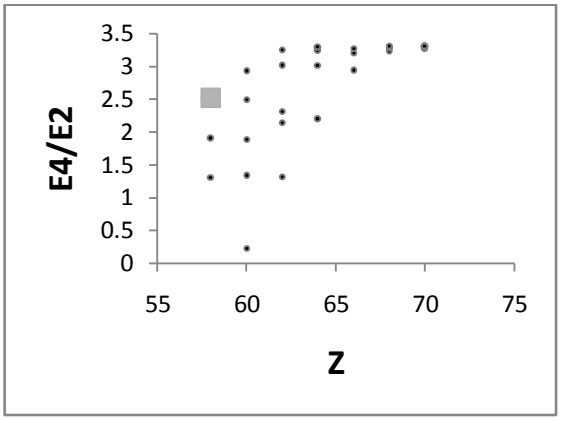


Fig. 2. Variation of E4/E2 vs Z

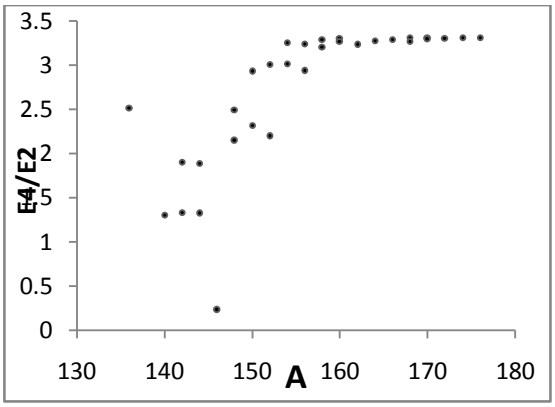


Fig. 3. Variation of E4/E2 vs A

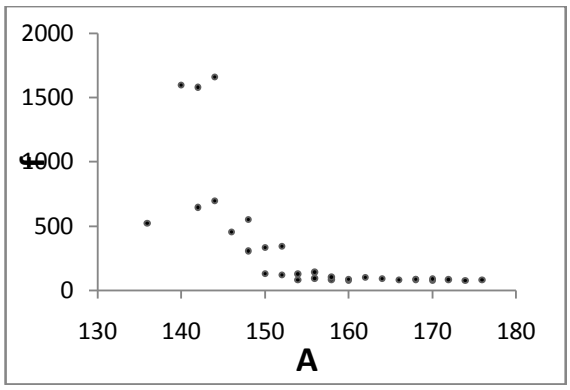


Fig. 4. variation of 'f' vs A

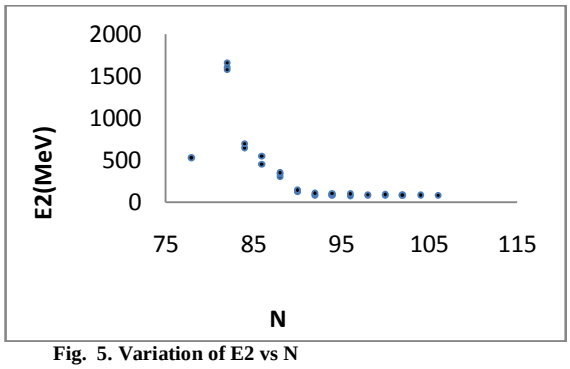


Fig. 5. Variation of E2 vs N

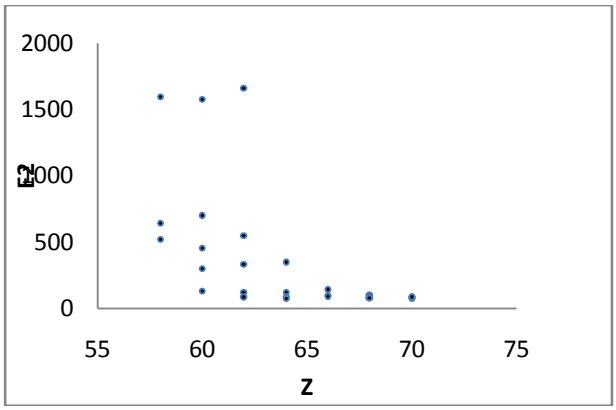


Fig. 6. Variation of E2 vs Z

REFERENCES

[1] Iachello F. and Arima A. The Interacting Boson Model. Cambridge University Press, Cambridge, England, 1987.

[2] Frank A. and VanIsacker P. Algebraic Methods in Molecular and Nuclear Structure Physics. Wiley, New York, 1994.

[3] Eisenberg J. and Greiner W. Nuclear Theory, Vol. I, Nuclear Models: Collective and Single-Particle Phenomena.North-Holland, Amsterdam,1987.

[4] Troltenier D., Hess P.O. and Maruhn J. Computational Nuclear Physics, Vol. I, Nuclear Structure.Springer, Berlin, Heidelberg, New York,1991.

[5] Troltenier D. Das GeneralisierteKollektivmodell. Frankfurt am Main, Germany, Report No. GSI-92-15, 1992.

[6] Bohr A. and Mottelson. Nuclear Structure v. II. Benjamin, New York, 1975.

[7] Jolie J. et al. Two-Level Interacting Boson Models Beyond The Mean Field. *Physical Reveiw*, 2007, v. C75, 014301R–014310R.

[8] Iachello F. and Zamfir N.V. Quantum Phase Transitions in MesoscopicSystems. *Physical Review Letters*, 2004, v. 92(3), 212501–212504.

[9] Cejnar P., Heinze S. and Dobes J. Thermodynamic Analogy for Quantum Phase Transitions at Zero Temperature.*Physical Review*, 2005, v. C71, 011304R–011309R.

[10] Rowe D.J. Quasi Dynamical Symmetry in an Interacting Boson Model Phase Transition. *Physical Review Letters*, 2004, v. 93, 122502-122505.

[11] Liu Y.X., Mu L.Z. andWei H. Approach to The Rotation Driven Vibrational to Axially Rotational Shape Phase Transition Along The YrastLine of a Nucleus. *Physics Letters*, 2006, v. B633, 49–53.

[12] Zhang Y., Hau Z. and Liu Y.X. Distinguishing a First Order From a Second Order Nuclear Shape Phase Transition in The Interacting BosonModel. *Physical Review*, 2007, v. C76, 011305R–011308R.

[13] Arios J.M., Dukelsky J. and Garcia-Ramos J.E. Quantum Phase Transitions in the Interacting Boson Model:Integrability, Level Repulsion and Level Crossing. *Physical Review Letters*, 2003, v. 91, 162502–162504.

[14] Garcia-Ramos J.E. et al. Two-Neutron Separation Energies, Binding Energies and Phase Transitions in The Interacting Boson Model. *NuclearPhysics*, 2001, v. A688, 735–754.

[15] Liu M.L. Nuclear Shape-Phase Diagrams.*Physical Review*, 2007, v. C76, 054304–054307.

[16] Heyde K. et al. Phase Transitions Versus Shape Coexistence. *Physical Review*, 2004, v. C69, 054304–054309.

[17] Khalaf A.M., Ismail A. M.,Structure shape evolution in Lanthanide and Actinide nuclei, Progress in Physics, Vol 2, april 2013

,

A Review - Analysis of Atmospheric Effects on Free Space Optics

Jasmeen Kaur[1]
Student [3rd sem., Batch - (2013-2015)]
Department of Electronics & Communication Engineering
Amritsar College of Engg. & Tech.
Amritsar, India
kangjasmeen@gmail.com

Gaurav Soni[2]
Associate Professor
Department of Electronics & Communication Engineering
Amritsar College of Engg. & Tech.
Amritsar, India
gaurav.ece@acetedu.in

***Abstract*— In these days , Free Space Optics (FSO) communication is a demanding efficient wireless technology which have been accepted due to its low power and mass requirements, high data rates and unlicensed spectrum. Atmospheric disturbances have a significant impact on performance of FSO Link which causes to degrade the laser beam. The attenuation at the output due to these disturbances can be reduced by using a multiple beam concept for a given distance, power and data rate. The performance of FSO Link using BER analyzer is also studied in this review paper.**

***Key words*—Atmospheric turbulences, Attenuation, Bit error rate, Free Space Optics(FSO), Optics Channel, Scintillation.**

I. INTRODUCTION

Free Space Optics (FSO) refers 'Free Space' means air, vaccum or where no wire exist and optics means a communication with a light. So Free Space Optics is like a wireless technology [1] in which information is received at receiver with the help of light, channel used is free space. It is different from fiber optics in which channel used to send information from transmitter to receiver is fiber. Fiber is like a thin transparent flexible tube having a core and cladding interfaces. Many experimental researches today allowing a point to point as well as point to multipoint line-of-sight (LOS) connections in free space optics [1]. FSO is not an new idea it is mainly developed from the fiber –optic cables which are occurred back from 30 years but because of its advantages more on fiber-optic we used it [2]. FSO can carry full-duplex (simultaneous bidirectional) data at gigabit-per-second rates from a several hundred meters to a few kilometers [2]. Applications of FSO are in many fields. Main fields are [2]

1) Metropolitan area networks
2) Internet high-speed connection services
3) Enterprise Connectivity
4) Military applications
5) Service Instantly

When fiber infrastructure is being laid then the services are provided by FSO instantly to optical fiber customers. Generally, FSO works at two wavelengths 850nm or 1550nm. In both wavelengths 1550nm wavelength is more preferred because of the reasons of high power, long distance, eye safety, high data rates and it works at poor propagation conditions(like fog)[2].

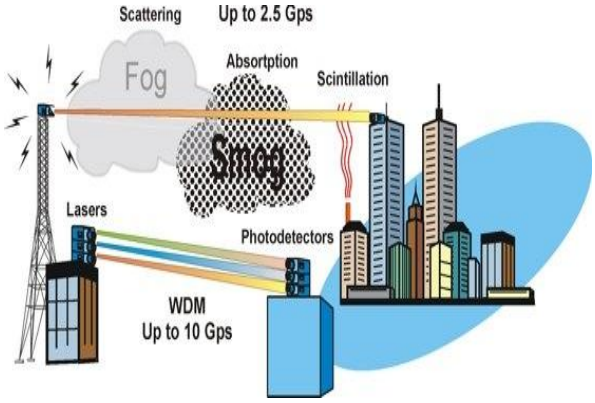


Fig. 1. Free Space Optical System

BLOCK DIAGRAM

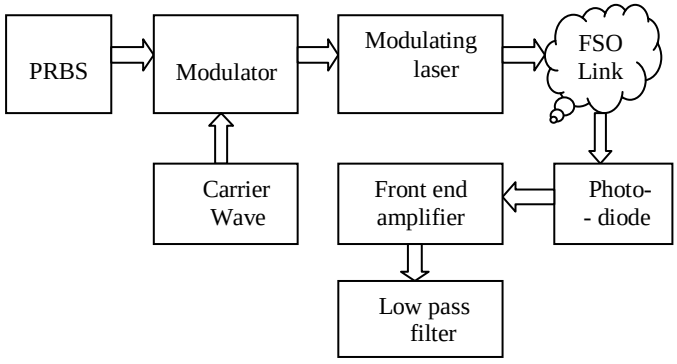


Fig. 2. Block Diagram of Free Space Optics [7]

Figure 2. shows the FSO communication system block diagram. In which transmitter used are LED (Light Emitting

Diodes) or Laser Diodes (LD), receiver used are p-i-n photodiodes or avalanche photodiodes. By using these components data or information is send from transmitter to receiver.

II. Atmospheric Effect

From many years, FSO suffering from a many atmospheric challenges. Main Challenges are absorption, scattering, turbulence, scintillations by which at the receiver, received signal degrade its quality. The purpose of this review paper is to describe these challenges, its BER performance and how to overcome these challenges.

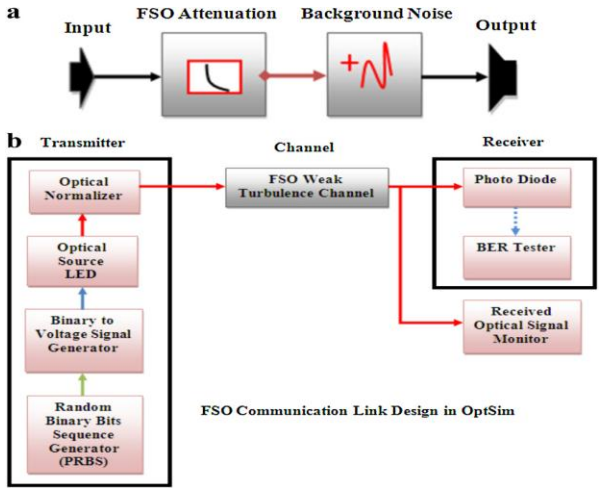


Fig. 3. FSO channel compound component based on weak turbulence approximation. (b) FSO communication link block diagram [3].

Due to a temperature gradient and wind velocities that create air pockets by varying densities produces a turbulences in the atmosphere which changes the indices of optical refraction [3]. Mainly all impact of challenges is done on the information channel by which information is lost there. There are lot of noises like thermal noise, shot noise, dark current noise etc. are produces at the channel due to atmospheric effects. Sun also a one major source which effect the FSO communication system. The impact of sunlight on FSO receiver depends on the angular and spectral sensitivity of the receiver. Also Sunlight impact takes orientation and mount of the installed system or FSO system [1].

Major Challenges are explained below:

ABSORPTION:- Absorption and Scattering mainly constituent of gases and particulates of the atmosphere give rise the attenuation of the beam. Attenuation means loss of energy of signal. In a simple way absorption process is occured due to interaction between light beam and molecules in air that results in attenuation means loss of energy of the beam. The absorption occurs due to molecules of water, carbon dioxide and ozone. Some wavelengths as 850nm, 1310nm and 1550nm are used at which the attenuation produced by absorption can be decreased up to little extent.

SCATTERING:- When the light beam interact with the atmosphere it will get scattered or deflected due to atmospheric particles. There will be no change in the wavelength and energy of the beam even after the interaction with the atmosphere. Scattering phenomenon depends upon size and type of molecules.

Types of Scattering

1. Rayleigh Scattering
2. Mie Scattering
3. Non-Selective Scattering

First two phenomenon are wavelength dependent but the last one is not wavelength dependent.

RAYLEIGH SCATTERING:- When the light wavelength is higher than the particle size then this type of scattering occurs. It means that the atmospheric gases and size of molecules are less than the incident light wavelength. Smoke, small dust and soil particles are also smaller than the wavelengths of light causes to produce this type of scattering.

MIE SCATTERING:- This type of Scattering is opposite to the Rayleigh Scattering in which size of particles is greater than or equal to the wavelength of the light due to which this kind of scattering occurs. Size of particle is greater than one micron or value of X is much greater than unity. In weather conditions like fog this scattering is become dominant.

NON-SELECTIVE SCATTERING:- The scattering particles are large enough that the angular distribution of scattered radiation can be described by geometric optics. Rain drops, snow, hail, cloud droplets, and heavy fogs will geometrically scatter laser bit's signals. The scattering is called non-selective because there is no dependence of the attenuation coefficient on laser wavelength [4].

Attenuation caused by scattering can be estimated by [1]

$$a_{SCAT} \cong \frac{17}{S} \cdot \left(\frac{555}{\lambda}\right)^{0.195 \cdot S} \quad (1)$$

Where a_{SCAT} is the specific attenuation in decibel, per kilometer, S is the visibility for human eyes (sight) in kilometers and λ is the wavelength of transmitted light in nanometers.

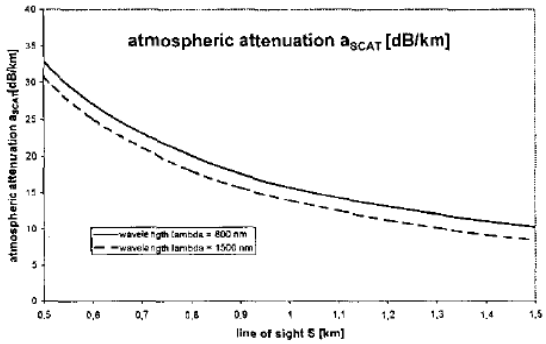


Fig. 4. Atmospheric Attenuation at 800nm and 1500nm[1].

Graph shows the attenuation produced at output by varying wavelengths at 800nm and 1500nm. It shows that by increasing a line of sight (km) the attenuation will decreases.

ATMOSPHERIC TURBULENCES:- Turbulences are occured due to the variations in the properties of atmosphere by which light beams are distort up to great extent. Properties like amplitude, frequency and phase are more affected due to these turbulences. When the temperature and density of the atmosphere are changes variation in the refractive index of the link are observed [3, 4]. Major effects of it can cause attenuation are scintillation, beam wandering and beam spreading. The first and third effects are caused by short-term average beam width and second by long-term beam width [6].

1) SCINTILLATION:- It is the process in which fluctuations in the intensity of the signal occurs at receiver. Its effect is higherat summers and afternoons. The parameter given by scintillation index, σ_1^2 which is also called as normalized variance of intensity used to measure scintillation. It is given as[3]

$$\sigma_1^2 = \frac{< I^2 > - < I >^2}{< I >^2} \tag{2}$$

where I is received signal intensity. For atmospheric weak turbulence, scintillation index is less than unity i.e., $\sigma_1^2 < 1$, otherwise $\sigma_1^2 \geq 1$.

2) BEAM WANDER:- Main reason of beam wander production is larger eddies in atmosphere. Chernov has calculated the wander of a single ray by using a geometrical optics approach. But he did not include the effects of the finite beam diameter in his formulations. Chiba has modified this concept who included the beam size for a collimated or nearly collimated beam. Others as Huygens–Fresnel approach, Andreev and Gelfer also calculated the beam wander for an initial Gaussian beam. This technique was also used for focused beam and which wave-front distortions occured from the above in homogeneities that degrade the link [6].

WEAK TURBULENCE :- For weak turbulence case, the log normal density function provides acceptable measurements and thus, can be used to estimate the link availability and its margins. In FSO, the attenuation in signal is based on the FSO range equation that combines attenuation and geometrical aspects to calculate the received optical power as a function of range and receiver aperture size. The range equation can be given as [3]

$$P_{RX} = \left(\frac{A_{RX}}{\pi \left[\frac{\theta}{2} \times L \right]^2} \right) \times T \times 10^{-\left(\frac{\alpha L}{10}\right)} P_{TX} + P_{BG} \tag{3}$$

Where P_{RX} is the received signal, P_{TX} is the transmitted signal, A_{RX} is the receiver aperture area, θ is the beam divergence angle, T is the combined transmitter receiver optical efficiency, P_{BG} is the optical power of background radiation, L is the link range, and α is the environmental attenuation in dB/km.

The first term in eq. (3) is a geometrical attenuation due to beam spreading. The atmospheric attenuation ˛ is not a linear function of distance. It depends on many factors and changes randomly with time. Combining together geometrical and additional attenuation, we can re-write Eq. (3) in the following form [3]

$$P_{RX} = 10 - \left(\alpha_{geomet} + \alpha_{add} \right) P_{TX} + P_{BG} \tag{4}$$

where α_{add} represents total additional attenuation in dB for given distance and is specified with a mean value and standard deviation. According to log normal model, the logarithm of signal intensity is a Gaussian random variable. Hence, the signal attenuation in dB units , α_{add} is a Gaussian L random variable as well. If values for mean intensity, < I > and scintillation index, σ_1^2 are known from either measurements or theoretical calculations, then we can derive $< \alpha_{add} >$ and σ through the following relationships [3]

$$< \alpha_{add} > = 4.34 \left(\ln < I > - 0.5\sigma_1^2 \right)$$
$$\sigma = 4.34\, \sigma_1 \tag{5}$$

Two optics techniques are used to partially compensate the turbulence . First technique is by tracking and second one is by adaptive optics techniques, and it has a greater impact on higher frequencies within the near infrared sub-band (1550 nm is therefore, less affected)

CASES OF WEATHER CONDITIONS

FOG ATTENUATION:- In actual Fog is composed of very fine spherical water particles of various sizes suspended in the air which results in attenuation of the light beam due to Mie scattering. Fog particles reduce the visibility near the ground and the meteorological definition of fog is when the visibility drops to near 1 km. The areas where frequent heavy fogs, 1550-nm lasers are choosen because of the higher power permitted to transmit at that wavelength. Also Mie scattering is slightly lower at 1550 nm than at 850 nm. Fog gives more problem than rain and snow conditions.

SNOW ATTENUATION:- In which the incident light is absorbed by unregular shapes of particles in the size of about

2 up to 25mm, produces an attenuation which depends on the relation of particle and receiver optics area. This kind of conditions for FSO are worse than Fog.

RAIN ATTENUATION:- In tropical region, FSO Link is influenced by a very limiting factor that is RAIN. Rain attenuation is one of the most important to influence FSO link. In general, weather and installation are the key factors that could possibly reduce visibility and also impair the FSO performance. To predict an Rain Attenuation a mathematical model has been analyzed and correlated with the local rain data. This work is presented by a numerical model based on the Beer's law and Stroke law [4]. The loss or attenuation from atmospheric effects can be calculated using various models available in propagation literatures. The attenuation of the laser power in the atmosphere is described by Beer's law [4] :

$$T(R) = \frac{P(R)}{P(0)} = e^{-\beta R} \quad (6)$$

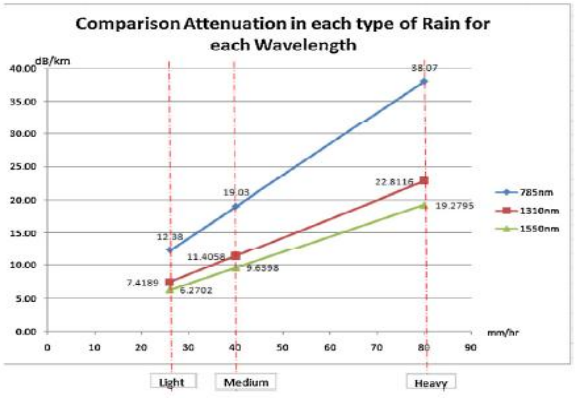


Fig. 5. Comparison attenuation in each type of rain for 785 nm, 1310 nm and 1550 nm wavelength at 1 km[4].

Figure 5. shows that in each type of rainy condition, wavelength 1550nm is the best choice which gives a lowest attenuation in dB/km . Results are recorded as for Light rain, it gives 6.27 dB/km, 9.64 dB/km for medium rain while 19.28 dB/km for heavy rain .

RECEIVED OPTICAL POWER AT RECEIVER DUE TO EACH TYPE OF RAIN CONDITIONS:

Received power(dBm) versus aperture size.

Weather	**Aperture**			
	15 cm	***30cm***	***45cm***	***60cm***
Light rain	-66.96	-54.92	- 47.87	- 42.87
Medium rain	-67.22	-55.18	- 48.14	- 43.14
Heavy rain	-66.31	-54.27	- 47.23	- 42.23

Table 1[4]

Table 1. shows that the aperture sizes are giving an impact on received power at every type of rain conditions. If aperture size will be larger, received power will be better.

III. Multiple Beam Concept

FSO with single beam under heavy rain condition having a attenuation of 19.2 dB/km, which makes whole system vulnerable, so to overcome it use the multiple beam FSO transceiver system. At data rate of 1 Gb/s this multiple beams system(up to four-beams) gives a improved quality of received power along with link distance up to 1141.2 m as compared to one-beam, two-beam, and three-beam, with link distances 833.3 m, 991.0 m, 1075.4 m, respectively[5].

For the single-beam and multi-beam FSO system, the rain attenuation is given by [5]

$$\gamma_{Rain} = K \cdot R^{\alpha} = A_{atmos} \quad (7)$$

Where γ_{Rain} is the rain attenuation, R is the rain intensity in mm/h, K and α are rain coefficients.

So by using a multiple beam concept the FSO link performance can be enhanced.

IV. BER Analysis

Bit error rate (BER) is a very important parameter used in the communication system. This parameter is basically depends on errors resulting from attenuation at receiver due to atmosphere. This paper presents the numerical evaluation of BER. Different turbulent conditions and laser beam characteristics were applied to the calculations. The laser beam size and wavelength have also significant effects in the BER values [6].

A. Atmospheric turbulences

In these conditions, Ferdinandov et al. has proposed a very simple analytical formulations for calculating BER. Basically for evaluating the beam degradation in FSO , short- term exposure (scintillation and beam spreading) as well as long-term exposure (wandering) were considered. In these calculations a 'turbulent parameter' C_n with different values is considered under turbulence conditions. The effects of laser characteristics (beam aperture size and wavelength), and their influences on the BER are also considered. Laser beam propagation in the atmosphere can be described by wave equation solution given by [6]

$$\nabla^2 E + k^2 n^2 (\vec{r}) E = 0 \quad (8)$$

Where E and k represent electric field wave function and wave number, respectively. The parameter n is the refraction index of medium that is generally a random function of time and

space. The mathematical description of random processes and their effects in " refractive index structure parameter" C_n and consequent wave distortion are presented in this paper . It must be noted that the influence of weak refractive index fluctuations ($C_n^2 \approx 10^{-14} m^{-2/3}$), and intermediate refractive index fluctuations ($C_n^2 \approx 10^{-12} m^{-2/3}$) also have been considered in the calculations.

B. Signal-to-noise ratio and the bit error rate parameter

The parameter BER for a signal sending by laser beam at a distance z can be expressed by [6]

$$BER(z) = \frac{1}{\sqrt{\pi}} \int_Q^{\infty} e^{-x^2} \, dx = \frac{1}{2} erfcQ(z) \quad (9)$$

where $Q(z)$ is the signal-to-noise ratio of the system and given by [6]

$$Q(z) = \frac{< i_s(z) >}{2\sqrt{2}\sigma_j(z)} \quad (10)$$

In relation (10) $< i_s(z) >$ is the receiver photodiode current due to laser beam, and $\sigma_j(z)$ is its statistical variance. The parameter $< i_s(z) >$ can be calculated by [6]

$$< i_s(z) > = S_i \phi_s(z) \quad (11)$$

where S_i is the photodetector absolute sensitivity and $\phi_s(z)$ is the optical power received by the detector at the distance z from the laser source.

The statistical variance of $\sigma_j(z)$ in Eq.(10) is expressed by[6]

$$\sigma_j(z) = 2e < i_s(z) > \Delta f \quad (12)$$

Where Δf is the frequency range of the receiver. If the background radiation power is considered, the variance $\sigma_j(z)$ in Eq.(12) must be modified by [6]

$$\sigma_j(z) = \sqrt{(2e < i_s(z) > \Delta f) + \sigma_{jB}^2} \quad (13)$$

In which σ_{jB} is the variance due to background radiation power.

By using these equations bit error rate can be find out. BER reviewed results are shown in figures 6 & 7:

C. The influence of different turbulent conditions in BER

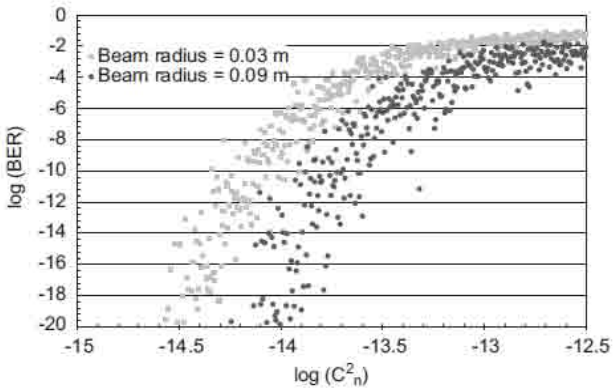


Fig. 6. Typical values of BER versus different turbulent conditions characterised by C_n^2 for two initial laser beam radius 0.03 and 0.09m and laser wavelength λ= 850 nm for a receiver at distance z=1000m[6].

Figure 6. shows the small value of BER at turbulence with weak refractive index fluctuation, and it rises dramatically with theC_n^2. When C_n^2> 5 x 10^{-13} , the BER becomes very large at turbulence.

D. The influence of initial laser beam radius and laser wavelength in BER

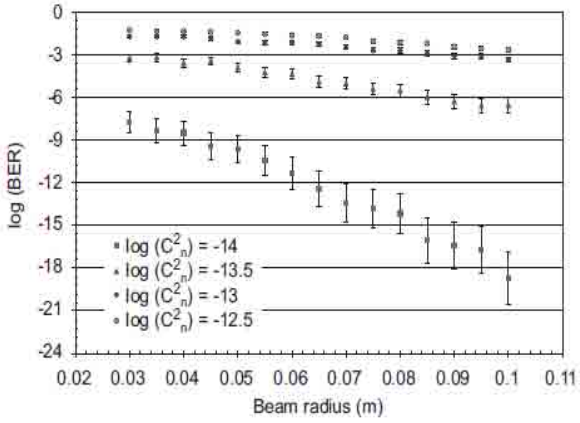


Fig. 7. The parameter log (BER) versus laser beam radius for four different turbulent conditions log C_n^2= -12.5 , -13 , -13.5, and -14 . The laser wavelength is assumed λ = 850 nm and a distance of z= 1000 m[6].

Figure 7. shows that by increasing laser beam radius BER will decreases dramatically. The main reason for it was the different initial beam size does not get increased equally at the receiver position.

E. Effect at received output power with attenuation

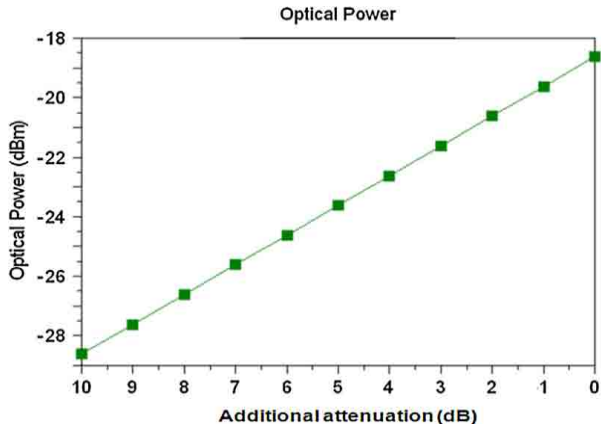


Fig. 8. Attenuation vs. received optical power [3].

From figure 8, it is seen that optical power at receiver is very less i.e. (below −28 dBm) when attenuation has its maximum value. And when attenuation tends to zero, optical received power increased and has maximum value (−19 dBm) . Hence there is a linear relation between the additional attenuation and received optical power.

V. CONCLUSION

In this review paper, the main focus is on the various atmospheric challenges that effects the free space optics system like absorption, scattering and atmospheric turbulences. To overcome these effects multiple beam concept has been used up to four-beams. It is realized that four-beam FSO system can operate successfully for a link distance of 1141.2 m at BER of 10^{-9}, with a received optical power of −34.5 dBm. Performance of these effects on BER analyzer is also reviewed. BER depends on the refractive index structure parameter for different turbulent conditions. With the increase in laser radius for a given distance, BER performance of the system significantly reduces. It is seen that the wavelength at 1550 nm gives the best performance in the atmospheric conditions . Further, the Optical received power depends on the aperture of receiver. This received optical power shows the linear relation with attenuation. As attenuation decreases received power increases.

REFERENCES

[1] M. Gebhart, E. Leitgeb, J. Bregenzer, "Atmospheric effects on optical Wireless Links" 7th International Conference on Telecommunications - ConTEL 2003 ISBN 953-184-052-0. June 11-13, 2003, Zagreb, Croatia, pp. 395-401.

[2] Heinz A.Willebrand & Bakseesh S. Ghuman , "Fiber Optics Without Fiber" Light pointe communications Inc. , IEEE SPECTRUM. AUGUST 2001, pp.40-45.

[3] Anshul Vats, Hemani Kaushal, "Analysis of free space optical link in turbulent atmosphere", International Journal for Light and Electron Optics, Volume 125, Issue 12, June 2014, pp. 2776–2779.

[4] Hilal A. Fadhil, Angela Amphawan, Hasrul A.B. Shamsuddin, Thanaa Hussein Abd, Hamza M.R. Al-Khafaji, S.A. Aljunid, Nasim Ahmed "Optimization of free space optics parameters: An optimum solution for bad weather conditions", International Journal for Light and Electron Optics, Volume 124, Issue 19, October 2013, pp. 3969– 3973.

[5] S.A. Al-Gailani , A.B. Mohammad , R.Q. Shaddad, "Enhancement of free space optical link in heavy rain attenuation using multiple beam concept" International Journal for Light and Electron Optics, Volume 124, Issue 21, November 2013, pp. 4798– 4801.

[6] M.H. Mahdieh , M.Pournoury "Atmospheric turbulence and numerical evaluation of bit error rate (BER) in free-space communication" Journal of Optics & Laser Technology ,Volume 42, Issue 1, Februrary 2010, pp.55–60.

[7] Amninder Kaur, Sukhbir Singh, Rajeev Thakur , " Review Paper: Free Space Optics" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 8, August 2014, ISSN: 2277 128X, pp. 969-976.

Nuclear Fusion: Revival of Sun's Energy on Earth

Suman
Asstt. Prof. (EEE), Panjab University Regional Campus Hoshiarpur (Pb.), India
e-mail:dearsuman@rediffmail.com

***Abstract*: Fusion is the Energy that powers the Sun and other stars. Since 1940's, it has been a goal of Scientist's around the World to harness this process by which the stars "burn" Hydrogen into Helium (i.e. Nuclear Fusion) for Energy production on Earth. In present scenario Eco-friendly and Sustainable energy sources are required to maintain our standard of living. Many researchers are developing a range of Environmentally acceptable, Safe and Sustainable energy technologies. Nuclear fusion technology is one of them. Nuclear reactions so far have not been harnessed to its full potential and in contrast are being implemented using present day technologies under different schemes in different countries .Nuclear Fusion as a matter of fact has great virtues over its fission counterpart. The principal raw material of thermonuclear fusion i.e. deuterium is renewable in nature and it's by product i.e. Helium is non-radioactive in nature. In order to meet the World's energy need for thousands of years, fusion opens numerous ways for research and future innovations in the requisite sector. This paper presents different aspects of Plasma physics, working principle of Tokamak and challenges to present day technologies to make the future brighter using Nuclear fusion.**

Keywords: Confinement, ITER, Lawson Criteria, Plasma, Plasma Amplification Factor, Tokamak

I. INTRODUCTION

Energy consumption of any country is globally accepted indicator of status of Industrialisation, Economic growth, Modernisation and Standard of living of their citizens. Around the World the human beings needs energy in its day to day life in different forms (i.e. electricity, fuels, power).Consequently it is becoming unsustainable to afford energy cost due to unpredictable hike in fossil fuels which have basic energy provider. So in view of the current fossil fuel scenario the focus of energy planners is shifted towards renewable sources & energy conservation. Nuclear fusion is the best substitute for fossil fuel .Nuclear fusion is an important natural process that keeps the Sun and all stars burning. It is the process by which lighter Nuclei fuse together to create a single, heavier nucleus and release energy. Given the correct conditions (such as those found in plasma),nuclei of light elements can smash into each other with enough energy to undergo Fusion .When this occurs, the products of the reaction have a smaller total mass than the total mass of the reactants. This mass difference is converted into energy as determined by Einstein's Famous formula

$E = mc^2$, where

m = mass difference of fusing nuclei (kg)

c = speed of light (m/s)

Even though the mass difference is very small, the speed of the light is extremely large (about 3 $x10^8$ meters per sec), so the amount of energy released is also very large. There are different states of matter where Plasma, represents the 4th state of matter which comes next after the gaseous state as shown in Fig 1.

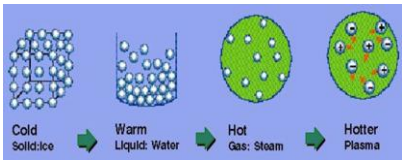


Fig 1:States of Matter[20]

More than 99% of the Universe is made up of plasma[24] .Now what is plasma ?Suppose we have a single atom in gaseous state, and if we add sufficient energy (heat) to it, then negatively charged electrons which are typically bound to the positively charged nucleus of this atom will overcome the pull of the nucleus. The result will be a "soup" of particles consisting of the free electrons (negative charge) and the free nucleus (positive charge).This state is known as plasma. In order to fuse nuclei, only smashing them together is not sufficient. In fact, high temperature and a medium are needed to overcome the electrostatic repulsions among their electrons. Fusion requires temperature about 100 million Kelvin (approximately six times hotter than the sun's core).In plasma, it is common to express its temperature with eV&1eV is approximately 11600^0C[13][25].

There are several fusion reactions possible, selected are depicted below in Fig 2:

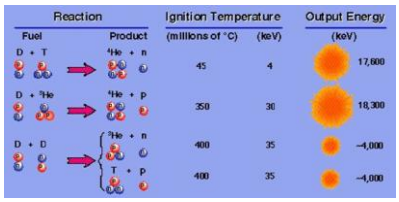


Fig 2: Temperature requirement with Output Energy[20]

The reaction that is best candidate for energy production on earth is between two isotopes of Hydrogen i.e. deuterium (D) and tritium (T) because of large reaction rate. In this process, the helium nucleus is produced (also called α- particle) has an energy of 3.5MeV.It is accompanied by the release of a neutron which receives K.E.(kinetic Energy) of 14.1 MeV and

large amount of liberated energy corresponds to 17.6 MeV as shown in Fig 3.

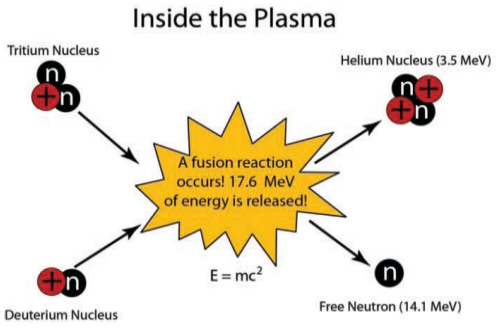


Fig 3:Thermonuclear Fusion Reaction[20]

Deuterium and tritium are the main ingredients in most of the fusion reactions. Deuterium is a stable form of hydrogen that occurs naturally. Moreover it is non-radioactive isotope. Further it can be extracted from water (on average 35g in every cubic meter of water).There is no tritium on earth, but it will be produced from lithium (a light and abundant metal) inside the fusion reactor.

II. PLASMA AMPLIFICATION FACTOR AND PLASMA CONFINEMENT

An important design parameter for a magnetic fusion reactor is its plasma amplification factor Q.A successful fusion power plant requires that the power produced by the fusion reaction exceed the power generated ($P_{Generated}$) to that consumed ($P_{Consumed}$) is called the fusion power amplification factor & it is represented by symbol Q.

$$Q=P_{Generated}/P_{Consumed}$$

- If Q < 1, the power of the fusion reaction is inferior to the power brought by heating.
- If Q=1, the power of fusion reaction is equal to the power brought by heating. This state is known under the name of "break even". In other terms the heating of plasma is assured by its particles α.
- If Q > 1, the power of fusion reaction is superior to the power brought up by heating. In this case we will reach the state of ignition. At this stage, the exterior (input) power is not required and we have infinite factor Q. Plasma is "auto-kept" in other words Fusion reaction will be self sustained, and we will have desired nuclear fusion reactor. In practice, power plant operation would probably correspond to a Q value of 20-40.

III. LAWSON CRITERIA

Once a critical ignition temperature for nuclear fusion has been achieved, it must be maintained at that temperature for a long enough confinement time at a high ion density to obtain a net yield of energy .For this, three parameters are expressed by Lawson Criteria and these are:

First parameter is the temperature; the nuclei of deuterium and tritium do not fuse spontaneously. Because they both have a positive charge and the repelling Coulomb force prevents the fusion .A sufficiently high Kinetic Energy of the nuclei is needed to overcome the Coulomb force .This high kinetic energy is achieved in a gas that has a temperature T of about 100 million degree centigrade. At this temperature gases are purely ionised and we no longer call them a gas, but call them Plasma. Therefore an absolute ignition temperature should be at least 100 X 10^6 K [5] [6][15].

- An absolute ignition plasma temperature

$$T= 100 \text{ X } 10^6 \text{ K[13]}$$

Second parameter is the Plasma Density. Even given a high temperature to overcome the coulomb barrier in nuclear fusion, a critical density of ions must be maintained to make the probability of collision high enough to achieve a net yield of energy from the reaction[23].

- Plasma density of about:

$$n = 10^{20} \text{ particles per } m^3$$

A third important parameter is the Confinement time. Confinement time in nuclear fusion is defined as the time the plasma is maintained at a temperature above the critical ignition temperature [23]. To yield more energy from fusion than has been invested to heat the plasma, the plasma must be held up this temperature for some minimum length of time .If fusion plasma loses its energy faster to the outside World than it can gain energy from fusion reactions and/or from external heating, then the process will die out. The rate at which plasma loses its energy is given by 1/ τ, where τ is called the energy confinement time in seconds.

- An energy confinement time:

$$\tau >/ 1 \text{ seconds}$$

For deuterium & tritium reaction practically it is found to be:

$$n \, T \, \tau > 5x10^{21} \text{ KeV sec/m}^3$$

The triple product nTτ is a figure-of-merit for a fusion reactor: the higher it is, [13] the better will be the reaction. In order to have a reasonable cross-section for the deuterium-tritium reaction a temperature between 1 to 10 KeV is needed. At such high temperature the problem is how to confine the plasma in a vessel! Fig 4 shows the status of unconfined and confined plasma inside the conductor.

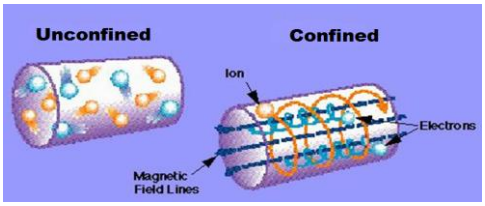


Fig 4: Unconfined and Confined Plasma[19]

There are two approaches for plasma confinement:

1. Inertial confinement[5][6][13] :

   a) $n \approx 10^{30}/m^3$

   b) $\tau \approx 10^{-10}$ s

2. Magnetic confinement[13][19] :

   a) $n \approx 10^{20}/m^3$

   b) $\tau \approx 1$ s

The concept that has given the best results so far in magnetic confinement fusion is the Tokamak. The Tokamak design was introduced by the Russian scientist Basov, Tokamak in Russian stands for: Torodial Magnetic Chamber as shown in Fig 5.

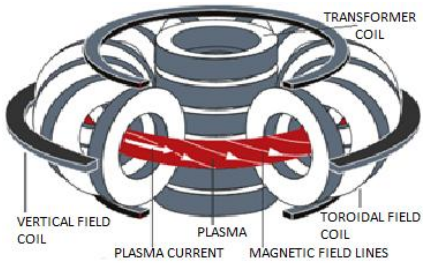


Fig 5 : Tokamak[17]

It is a toroidally shaped device characterised by a hollow vessel or chamber, forming the "doughnut" shape. To construct the magnetic field bottle in a Tokamak requires the generation of three superimposed magnetic fields[5][6][15] namely: 1) Toroidal field 2) Poloidal field 3) Vertical field. In doughnut plasma is confined by a magnetic field and bound to force field lines along a spiralling path .This type of magnetic configuration is obtained by combining an intense toroidal magnetic field, produced by magnetic coils placed around doughnut, with a poloidal magnetic field, obtained by externally inducing current in the plasma. The poloidal current also helps to prevent the plasma particles from migrating towards the vessel walls. The plasma particles spiral around the force field lines. Another set of external magnetic coils is used to provide auxiliary magnetic fields that control the position of the plasma in the doughnut[17]. The Tokamak configuration is particularly stable allows the plasma to be confined for a long time. So the Tokamak has so far been the most successful magnetic confinement scheme.

IV. FUSION POWER PLANT

In nuclear fusion power plant various features such as steam generator, heat exchanger & turbine will be the same as in conventional nuclear or fossil-fuelled power plants as depicted in Fig 6. In fusion power plant, reactor core is arranged in different layers like an onion .The inner region is the plasma, surrounded by the vacuum vessel, outside the vacuum vessel there are the coils for the magnetic field. Since the magnets operate at very low temperatures (superconductors), the whole core is inside a cryostat which provides a super-cool and vacuum environment [4] [6]. The fuel- deuterium and tritium – is injected into the plasma in the form of a frozen pellet, so that it will penetrate deeply into the centre of the core

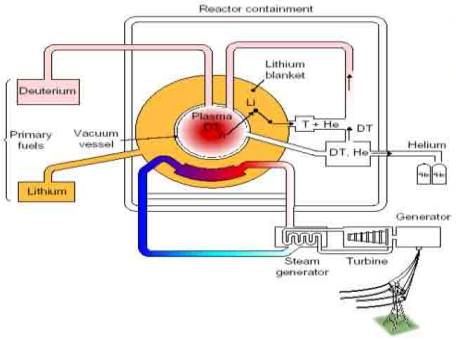


Fig 6:Fusion Power Plant[18]

. The neutrons leave the plasma and are stopped in the so called lithium blanket. The lithium blanket outside the plasma reaction chamber will absorb high-energy neutrons from the fusion reaction to make more tritium fuel .The "ash" of the fusion reaction i.e. helium is removed via the diverter. The outer magnetic field lines of the Tokamak are especially shaped so that they intersect the wall at special planes, namely the divertor planes. Only a small fraction of the fuel is "burnt" so that deuterium and tritium are also found in the "exhaust" and can be recycled. The tritium produced in the blanket is extracted with a flushing gas – most likely helium –and delivered to the fuel cycle. The heat produced in the blanket and divertor is transported via water or helium to the steam generator and used to produce electricity to feed the grid. The power needed to start the fusion reaction will be about 70 MW, but the power yield from the reaction will be 500 MW. The fusion reaction will last from 300 to 500 sec (eventually, there will be a sustained fusion reaction.). A small fraction of power is used to supply electricity to the various components of the plant itself. Like for cryo-system which produces low temperature helium for the super-conducting magnets, the current in the magnets, the current drive and the plasma heating systems.

V. FUEL SELECTION AND AVAILABILITY

Fusion of two small nuclei is energetically advantageous because the joint nucleus has a smaller surface area than the

two original nuclei. When a nucleus is too big, the long distance electrostatic (Coulomb) repulsion between the positive protons sums up and becomes too strong. That is why very large nuclei (transuraniums) are unstable [16] .For nuclei bigger than iron the overall energy loss due to mutual repulsion is more important than the energy gain due to smaller surface. It turns out that the most tightly bound atomic nuclei are around the size of ion(with 26 protons in the nucleus).That is, one can release energy either by splitting very large nuclei(like Uranium with 92 protons) to get smaller products, or fusing very light nuclei(like hydrogen with just one proton)to get bigger products. In both cases the reaction shifts the size of the atoms involved towards iron that is towards lower energies in the "valley" pictured below in Fig 7.

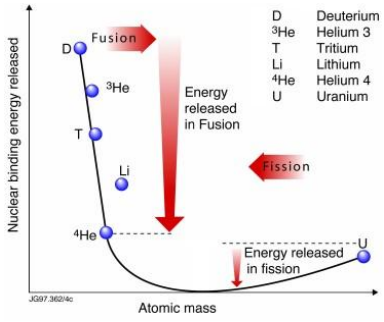


Fig 7: Released Nuclear Binding Energy in Fusion &Fission

Deuterium is a hydrogen isotope. In terrestrial hydrogen sources such as sea water, deuterium makes up one part in 6420 of hydrogen. The oceans have a total mass of $1.4X10^{21}$kg and the deuterium accounts for approximately 0.312% on a mass basis, therefore contain $4.6x10^{16}$kg of deuterium. Moreover there is already a mature technology for extracting the deuterium. What about tritium? As we have mentioned above, tritium, also a hydrogen isotope, will be bred from lithium using flux of fusion neutrons. Lithium is found in nature in form of two stable isotopes i.e. ^{6}Li (7.4%) and ^{7}Li(92.6%) [5].The given nuclear reactions are relevant to produce more tritium.

$$^{6}Li + n \longrightarrow {}^{4}He + {}^{3}T$$

$$^{7}Li + n \longrightarrow {}^{4}He + n - 2.5MeV \text{ [5]}$$

Since the second reaction is endothermic only neutrons with energy higher than the threshold can initiate this process. In most blanket concepts the reaction with ^{6}Li dominates, but in order to reach a breeding ratio exceeding unity the ^{7}Li content might be essential. Lithium can be found in : salt brines(concentrations ranging from 0.15% to 0.2%),minerals like spodumene , petalite, eucrypolite, amblygonite,lepidotite(concentration varies between 0.6 % and 2.1%) and sea water (the concentration in sea water is 0.173 mg/l(Li+)).

While the annual consumption of lithium in a fusion plant is low, the lithium inventories in the blanket are much larger [5].At least a couple of hundred tons of lithium is necessary to build a blanket. It is expected that most of the lithium can be recovered and re-used. The lithium supply is, however, a minor problem in the context of the construction of the whole plant: lithium can be purchased today for around 17 Euro/Kg and the blanket containing 146 ton of lithium needs to be replaced five times in a life of a fusion plant, which would amount to only 12M Euro. Besides the land based resources there is a total amount of $2.24x10^{11}$ton lithium in sea water. The ultimate lithium resources in sea water are thus practically unlimited..

VI. Project Cost

Best confinement of plasma has been achieved so far in Tokamak based design and hence same design is considered here the ITER(International Thermonuclear Energy Reactor). ITER is designed to produce 500MW of fusion power for extended periods of time (several 100s) with time scales of Ten Years of Construction and Twenty Years of Operation.

Total estimated cost of construction phase is Dollar 0.9628185 billion. Annual Operation and maintenance costs of general reactor at 2% of the total capital cost plus an operating and maintenance of $38 million for the lithium –aluminium (Li-Al) process plant, which is assumed to scale with tritium production i.e. to produce 10 kg of tritium /year for a $29 thousand/g [9][14]. The blanket replacement cost, assuming 20% replacement each calendar year. This means a 3.5-year blanket exposure lifetime is assumed [9]. Blanket replacement cost, which should be high because the beryllium would be recycled. The annual electricity cost is the product of energy required and a unit cost of 28 mill/KWh (or power sold at 23 mill/KWh)[9][14].

VII. Advantages

Fusion has potential advantages as a sustainable and environmentally attractive source of energy for electricity generation.

1. The fusion fuel is readily available; Deuterium and Tritium are virtually inexhaustible.

2. Unlike the burning of Coal or other fossil fuels, fusion does not emit harmful toxins into the atmosphere. The combustion of most of the fuels involves some form of the reaction as shown:

$$C + O_2 \longrightarrow CO_2 + \text{heat}$$

The carbon dioxide (CO_2) emitted by this reaction contributes to the global warming so-called "Greenhouse Effect". Fusion however, produces only helium gas that is already present in the atmosphere and will not contribute to greenhouse effect.[22]

3. No runaway reactions or large uncontrolled releases of energy are possible. In the case of a malfunction the plasma strikes the walls of the reactor and cools immediately.

4. A major concern with the use of fission power is the issue of nuclear waste, a dangerous material that can both directly injure people and be manufactured into weapons. Fusion has no such problems; no long lived radioactive materials are produced.

5. Fusion is appropriate for generating base-load electricity and fuel consumption of this power station will be extremely low. A 1GW (electric) fusion plant will need about 100Kg deuterium and 3 tons of natural lithium to operate for a whole year, generating about 7 billion KWh [3]. A coal fired power plant –without carbon sequestration requires about 1.5 million tons of fuel to generate the same amount of energy! In upcoming years as shown in Fig 8, the depletion of fossil fuels will result in the imbalance between the demand and supply of power and alternate source of fusion can bridge this gap

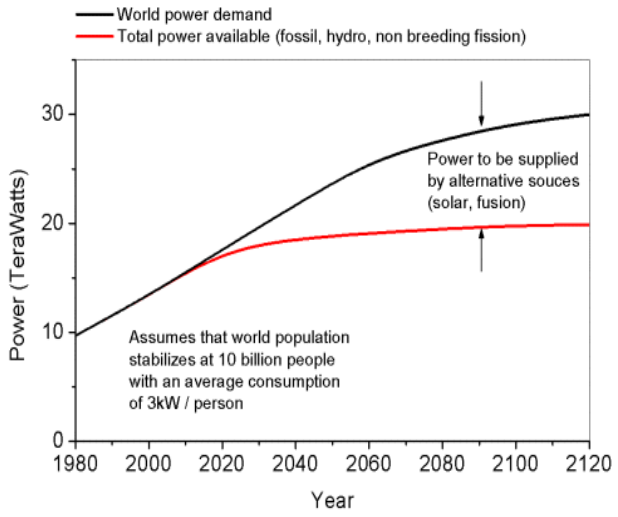


Fig 8: Power Curve[24]

VIII. CONCLUSIONS

As the climate is changing globally and we are out of fossil reserves, it's now time to look at alternative and eco-friendly sources of energy. Nuclear fusion though challenging but contains secrets of future technological innovation, to name one: hydrogen produced can be used to power a hydrogen car etc. This gives us opportunity to switch from conventional sources of energy to Nuclear energy. Nuclear fission has been implemented on large scale by different countries and has been working successfully for many years, but has resulted in radioactivity, waste disposable problems and also the risk of exposure to radiation for the operators of plant is high and replacement of fuel is necessary. While in case of fusion it offers the self-sustaining fuel with minimal health and environmental risks. Members of ITER (International Thermonuclear Energy Reactor) project which aims to make the long-awaited transition from experimental studies of plasma physics to full scale electricity-producing fusion opens a new way of prospective and associated research in the field of fusion. The abundant raw materials if harnessed properly hold the keys for the bright future of World.

REFERENCES

1. photo: Luc viatour/ww.Lucnix.be
2. Google Images
3. Fusion Research: An Energy option for Europe's Future, European Commission.
4. Chapter 14: Nuclear Fusion from ww.ems.psu.edu/~radovic/chapter14.pdf
5. T.Hamacher and A.M Bradshaw,Fusion as a future power source: Recent achievement and prospects,18th World Energy Congress, Max-Plank-Institutfur Plasmaphysik,Garching/Greifswald,Germany.
6. Naima GhoutiaSabri*,Taye Benouaz, Magnetic Confinement of the Plasma Fusion by Tokamak Machine
7. http://science.howstuffworks.com/fusion-reactor4.htm
8. R.Shrinivasan and the India Demo team, Conceptual study of Indian Fusion Power Plant, Institute for Plasma Research,Bhat,Gandhinagar-382 428 , India
9. J.D.Lee, Economic Analysis of a Magnetic Fusion Production Reaction,Vol.06 Journal of Fusion Energy-1987
10. http://library.thinkquest.org/20331/types/fusion/advant.html
11. Maarten De Bock, geboren te Sint-Niklaas,Understanding and controlling plasma rotation in Tokamaks.
12. J.Stockel, Plasma Confinement in Tokamaks,Institute of plasma physics, Academy of Association EURATOM/IPP.CR,Czech Republic.
13. Martin Greenwald, Fusion Plasmas, Encyclopedia of Electrical and Electronic Engineering, John Webster-

editor, Published by John Wiley & Sons, New York(1999)
14. Alexander Bolonkin, New AB-thermonuclear Reactor for Aerospace, Article Thermonuclear corrected 5 18 07, AIAA-2006-7225.
15. T.S. Hahm, Department of Nuclear Engineering, Seoul National University, Seoul 151-744,Republic Of Korea**,** Summary of the magnetic confinement Theory and modeling activity presented at The 24th IAEA Fusion Energy Conference
16. Vincent Massaut,Head Of Fusion Reasearch,SCK-CEN,http://www.bnsorg.eu/index.php?option=com_content&view=article&id=140:vincent-massaut&catid=37:interviews&Itemid=109.
17. http://www.ipp.mpg.de/ippcms/eng/pr/exptypen/tokamak/
18. http://ec.europa.eu/research/energy/message_en.cfm?uripath=research/energy/fu/fu_rt/fu_rt_pp&urifile=article_1236_en.htm
19. J.C Sprott, Plasma Physics and Nuclear Fusion, Department Of Physics, University of Wisconsin-Madison, Physics 208,30 Oct.1998
20. Dirk O. Gericke,Lecture15:Inertial Confinement Fusion, Physics Of Fusion
21. http://library.thinkquest.org/20331/types/fusion/advant.html
22. http://hyperphysics.phy-astr.gsu.edu/hbase/nucene/lawson.html
23. http://www.plasma-universe.com/99.999%25_plasma
24. http://www.plasma.inpe.br/LAP_Portal/LAP_Site/Text/Advantages_of_Fusion.htm
25. http://en.wikipedia.org/wiki/Electronvolt

Role of Distributed Generation in Radial Power System

Er. Ajaypal Singh chhina
Department of Electrical Engineering
Amritsar College of Engineering and Technology
Amritsar, India
ajaypals18@gmail.com

Dr. Yadwinder Singh Brar
Department of Electrical Engineering
Guru Nanak Dev Engineering College
Ludhiana, India
braryadwinder@yahoo.com

Abstract - Due to technology improvement, energy market liberalization and environmental issues it has been witnessed an increasing allocation of distributed generation (DG) in the distribution networks. Every year, Distribution Network Operators (DNOs) receive several requests for installations of new generators in the existing networks. This situation is likely to imply a revolution in the distribution networks. The basic aim behind this is to maintain a sufficient level of system stability and instantaneous operation of power system by including the participation of energy and service. In this paper it has been analyzed how DSM policies can be a valid opportunity to facilitate the development of DG in a given distribution system and which economical benefits the utilities can derive by the complementary employ of both these distributed resources. Simulation studies have been performed on a real distribution networks, showing the effect of DSM action on the growth of DG in the distribution system and on the technical and economic benefits, they permit to realize.

Index Terms— Radial Network, Distributed Generation unit, Maximum cost, Penalty Factor, Energy Saving, Environmental issues.

Introduction

Distributed Generation (DG) - Distributed generation is any electricity generating technology installed by a customer or independent electricity producer that is connected at the distribution system level of the electric grid. This includes all generation installed at sites owned and operated by utility customers, such as photovoltaic systems serving a house or a cogeneration facility serving an office [2]. The definition given does purposely lack information concerning

- Power rating and technology
- Environmental impacts
- Delivery area
- Mode of operation

The main benefit of installing a distributed generation system is the assurance of receiving power from the utility when your system is not running. This is essential for many renewable technologies like solar and wind, which produce intermittent power and for other technologies that may need to be shut down for periodic maintenance.

Demand Side Management (DSM). Demand Side Management (DSM) is another option which is equally important and beneficial as that of distributed generation in improving the energy scenario. It is observed that, by inclusion of new energy sources we are only supplying the increasing demand, while an inherent deficit prevails. Therefore, on the demand side, more efficient ways of utilization of the available energy has to be employed. The purpose of demand side management is energy conservation and the salient features of energy conservation are [3]:

- Setting up of energy conservation standards for any equipment or appliance consuming, generation, transmitting or supplying energy.
- Mandatory energy audit for all designated consumers, as and when required by the designated authority.
- Promotion of mass awareness at both the Central and the State levels for energy conservation, consumer education and guidance.

This paper presents a method to estimate how much a utility can afford to pay for these alternatives when the change in system capacity due to the distributed resource is constant from year to year and when there is no uncertainty.

Literature Review

A number of publications looked at optimizing the placement and sizing of DG based on various criteria.

Ajay P., Vimal R. D., Senthil, Kumar S., Raja J., (2009) authors employ an optimal power flow (OPF) technique to maximize DG capacity with respect to voltage and thermal constraints. Short circuit levels, short circuit ratio, equipment ratings and losses are not considered. The effect of network sterilization is clearly demonstrated by comparison between allocating generation to buses individually rather than as a group.[1].

Chakravorty M. and Das D., (2001) *authors* presented a method for the voltage stability analysis of radial distribution networks. A new voltage stability index is proposed for identifying the node, which is most sensitive to voltage collapse. Composite load modelling is considered for the

purpose of voltage stability analysis. It is also shown that the load flow solution of radial distribution networks is unique.[2]

Clark W. Gellings, (1985) author discussed that Demand side management (DSM) is the planning and implementation of those electric utilities activities designed to influence customers uses of electricity in way that will produce desired changes in the utility's load shape. While the objective of DSM activity is to produce a load-shape change, the art of successful implementation and the ultimate success of program rests with in the balancing of utility and customer needs. This paper describes demand side management for electric utilities and discusses the evolution of this concept for load management, strategic conservation, and marketing.[3]

Eberhart& Kennedy, (2009) authors use a heuristic approach to determine the optimal DG size and site from an investment point of view. Once again short circuit constraints are not considered and the focus of the objective function is on optimal investment rather than maximizing renewable energy. It uses a cost benefit analysis to evaluate various placements of DG.[4]

Hoff. T., (2007) author used genetic algorithm to place generation such that losses, costs and network disruption were minimized and the rating of the generator maximized. The constraints considered were voltage, thermal, short circuit and generator active and reactive power capabilities. Generation is placed in single units at individual buses, while ignoring the interdependence of the buses and the network sterilization that can result from improper DG placement.[5]

Ponnavsikko and Rao, (2006) authors presented a method of optimally choosing fixed and switched shunt capacitors on radial distribution feeders, considering load growth, growth in load factor and increase in cost of energy. Mathematical models were represented predicting cost saving due to energy loss reduction taking the growth factors into account, cost saving due to release in system capacities, capacitor cost and voltage rise during off-peak hours, as a function of capacitive current flows in the feeder sections have been formulated. Cost functions have been defined for optimizing the choice of both fixed and switched capacitors. A direct search technique known as the Method of Local Variations has been employed for solving the resulting discrete variation problem. The problem has also been solved using Dynamic Programming Approach for comparison.[6]

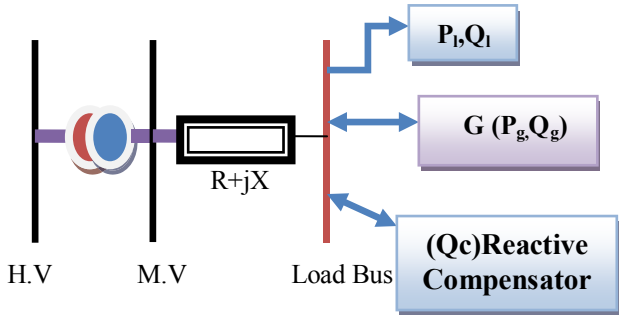
Zeng Y.G, Berizzi G. and Marannino P., (1997) authors developed a simplified approach to estimate maximum loading conditions in the load flow problem. This technique describes a computationally efficient and simple approach to estimate maximum loading conditions in the load flow problem. These operating points were known to result in a number of undesirable phenomena such as the singularity of the Jacobian, solution bifurcations, and voltage collapse. The approach presented here generated precise estimates of the maximum possible amount of load increase that the system can tolerate along a specified path, as well as the corresponding voltage vector. The method described was simple and efficient since it was based primarily on conventional load flow solutions. Tests on several standard power networks confirmed the accuracy and efficiency of the technique.[7]

Problem Formulation

The problems that are formulated in this thesis are related with radial and interconnected power system. Here main problems considered are ---

1) Based on load, Maximum capacity of DG unit during operation in radial connected power system.
2) What is the cost of distributed generation unit during operation with fixed penalty factor?
3) Based on moderate price what is the cost of a DG unit during operation?

In radial connected network the concept of demand side management (DSM) and DG are integrated [3]. But in interconnected network the optimum placement of DG unit is carried out by using Newton Raphson Technique for load flow studies [7]. The maximum power that is generated by distributed generation unit, cost of DG unit is carried out by using appropriate equations and all equations are discussed in the next chapter. The voltage rise caused by DG is a well known effect and can be illustrated using the simple circuit shown in Fig.(a).



Fig(a)

This figure represents the basic features of a distribution system into which a distributed generator, G, is connected at the MVA level. During formulation the major role are played by compensation devices. During light load conditions it takes reactive power from the load bus and when loads at the load centre increases than compensation devices are operated again and dissipates reactive power to the load buses. In this thesis active networks are considered.

Present work done

Radial Connected Network - In radial connected power system the result analysis that is done and discussed later is carried out into three categories, let us study these categories one by one.

4.1.1 Based on load maximum capacity of DG unit during operation---

In this case the operation of distributed generation unit is depending on the quantity of load on the consumer side. If load (P_l,Q_l) connected with the load bus is less corresponding to power available than DG unit is shut down, but if load on consumer side increases beyond the limits of power available in the load bus than DG unit is operated. The maximum power generated by DG unit corresponding to load connected with the load bus is carried out by using this equation [4].

$$P_{gmax} \leq (V_{2max}-V_1)/R \quad 4.1$$

Where

V_{2max}= maximum voltage present at load bus

V_1= voltage at bus 1

R= resistance of tie line between bus 1 and bus 2.

The voltage V_{2max} is further calculated by using this equation [6]:

$$V_2=V_1+R\times(P_g-P_l\pm P_{dsm})\pm X[(\pm Q_g-Q_l\pm Q_c)] \quad 4.2$$

P_{dsm} is the portion of total load that can be moved from peak hours to off peak hours.

4.1.2 Cost of DG unit during operation with fixed penalty factor) ---

In this analysis the cost received by distributed generation unit is taken into account. For this it is necessary to examined the maximum power generated by DG unit and this is depend on the load connected beyond the limit of power available in the load bus. The maximum power generated by DG unit corresponding to negligible load is calculated by using equation (4.1).

Once P_{gmax} is carried out than maximum cost received by DG unit or paid by DG unit is calculated by using following relation [6]:

$$C[P_g]= \lambda[0.01\times(P_{gmax})^2+15\times P_{gmax}] \quad 4.3$$

λ is penalty factor which decides the rate at which power is taken or given by DG unit.

4.1.3 Based on Penalty factor, cost of DG unit during operation---

When DG unit is in operating condition than it either gives power to the load bus or receives power from the load bus. A distributed generation company under such conditions sets his own penalty factor that decides the rate at which power is taken by DG unit or given by DG unit to the load bus. If load on consumer side is less than DG unit absorbed power from the bus. The penalty factor under such conditions is decided by two companies. The deal is basically valid for a period up to which contract is signed. After this period a new contract is signed by company. The penalty factor in new contract may be same or different. This penalty factor decides the rate at which power is taken or given by distributed generation (DG) unit.

The result analysis corresponding to above discussion is calculated by using this equation 4.3.

Result and Discussion

5.1.1 Maximum power generated by DG unit during operation---

In this analysis, it is considered that the demand of consumers is continuously increases. The active and reactive load powers at load centers decide the operation of distributed generation unit. From below written table it is cleared that the concept of DSM involves in the network during peak load conditions. Greater is the load; greater is the capacity of DG unit and vice versa.

Table 5.1.1 - Maximum power generated by DG unit based on load connected

Iteration	P_l(p.u)	Q_l(p.u)	P_{gmax}(p.u)	P_{gmax}(MW)
1	0.80	0.34	-0.20	-20
2	1.00	0.40	-0.16	-16
3	1.40	0.62	8.61	861
4	1.58	0.72	9.40	940
5	1.72	0.80	10.07	1007
6	1.80	0.86	10.43	1043
7	1.94	0.90	11.02	1102
8	2.40	0.98	11.57	1157

Take - Z (p.u) =0.05+j0.15, V_1=2.0 p.u, Base = 100 MVA

From the initial 2 iterations negative sign indicates that the power available at load bus is sufficient to fulfill the requirements of consumers. Under such cases, if DG unit is installed than it draws power from the load bus. The graphical representation of above written results is given below-

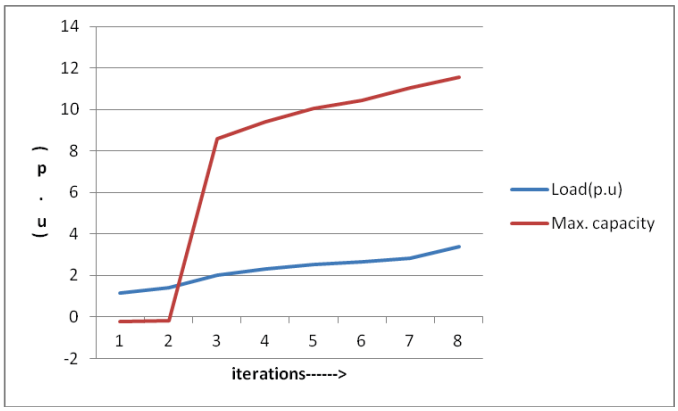


Fig 5.1 - Relation between maximum generation and load connected

5.1.2 Cost of DG unit during operation with fixed penalty factor ---

In this sub part of result analysis, the penalty factor is considered to be same during peak and off peak loads. The penalty factor λ=1.0 and is fixed corresponding to all stages of load.

5.1.2 - Maximum capacity of DG unit based on load connected with fixed penalty factor

Iteration	P_l(p.u)	Q_l(p.u)	P_{gmax}(p.u)	$P_{cost(Rs,/MW)}$
1	0.80	0.34	-0.20	-299
2	1.00	0.40	-0.16	-239
3	1.40	0.62	8.61	13004
4	1.58	0.72	9.40	14188
5	1.72	0.80	10.07	15206
6	1.80	0.86	10.43	15768
7	1.94	0.90	11.02	16651
8	2.40	0.98	11.57	17504

Take - Penalty factor (λ)=1.0 p.u, Z(p.u)=0.05+j0.15, V_1=2.0 p.u, Base = 100 MVA

5.1.3 Based on Penalty factor, cost of DG unit during operation---

In the last sub part of this objective the concept of penalty factor is considered. The penalty factor decides the rate at which DG unit take power from the load bus or gave power to the load bus.

Table 5.1.3 - Based on penalty factor maximum capacity of DG unit during operation

Iteration	P_l (p.u)	Q_l (p.u)	G_{cost} (p.u)	λ	C_{paid} (Rs/MW)
1	0.80	0.34	-2.99	0.8	-239.2
2	1.00	0.40	-2.39	0.8	-191.2
3	1.40	0.62	130.04	1.10	14304.4
4	1.58	0.72	141.88	1.10	15606.8
5	1.72	0.80	152.06	1.10	16726.6
6	1.80	0.86	157.68	1.10	17344.8
7	1.94	0.90	166.51	1.10	18316.1
8	2.40	0.98	175.04	1.50	26256

The graphical representation of above written results is shown below. It shows that the relation between maximum power of distributed generation unit during operation corresponding to different stages of load. From below plotting graph the relationship between cost and load in MW with penalty factor λ=0.8, 1.10, 1.5 is analyzed.

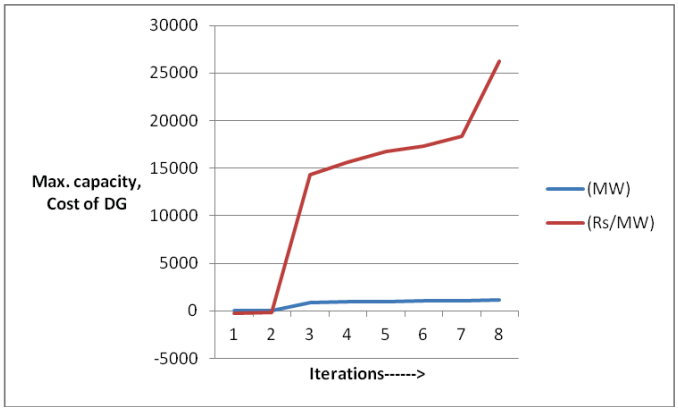


Fig 5.2 - Graph between cost of DG unit and load connected with moderate price

Conclusion and Future Scope

6.1 Conclusion

In this paper the relationship between loads connected with maximum output of distributed generation unit (P_{gmax}), the cost of DG unit (P_{cost}) with fixed rate, the cost of DG unit with variable price is done by taking radial connected power system. It is to be observed that with the increase in load the cost of DG unit and the maximum generation of DG unit increases and vice versa. The cost further depends upon the price set by two companies at different instants of load. The deal sign by two companies play a great role when DG unit is in operating condition. The basic aim behind this is energy conservation. The tariff given by customers during peak and off peak loads is depending on the penalty factor. This concept is further integrated with DSM.

6.2 Future Scope

This technique can be applied on radial and interconnected power system. Defined value of penalty factor (λ) is same for both networks. Large capacity of distributed generation (DG) unit install at the load centre may increase the cost of operation. This is because demand of customers increases day by day. This technique can be applied on radial and interconnected power system. Defined value of penalty factor (λ) is same for both networks. Large capacity of distributed generation (DG) unit install at the load centre

may increase the cost of operation. This is because demand of customers increases day by day. Further work is recommended programming technique like matlab may be applied to analysis of maximum capacity of distributed generated unit in radial as well as other type of power system.

References

[1] Ajay P., Vimal R. D., Senthil, Kumar S., Raja J., 2009, "Optimization of Distributed Generation Capacity for Line Loss Reduction and Voltage Profile Improvement using PSO, Vol.10, No. 2, 41-48.

[2] Chakravorty M. and Das D., 2001, "Voltage Stability Analysis of Radial Distribution Networks", International Journal of Electrical Power and Energy Systems, Vol.23, No. 2, 129-135.

[3] Clark W. Gellings, 1985, The concept of demand side management for electric utilities. IEEE Vol.73, No. 10, page no. 1468-1470.

[4] Eberhart& Kennedy, 2009," Optimization of Distributed Generation Capacity for Line Loss Reduction and Voltage Profile Improvement using PSO", Vol.10, No. 2, 41-48.

[5] Hoff. T, 2007, "Optimization of Distributed Generation Capacity for Line Loss Reduction and Voltage Profile Improvement", Vol.20, No. 2, 40-47.

[6] Ponnavsikko and Rao, 2006,"Optimal Choice of Fixed and Switched Shunt Capacitors on Radial Distributors by the Method of Local Variations", IEEE Transactions on Power Systems, Vol.PAS-102, No.6, pp.1607-1615.

[7] Zeng Y.G, Berizzi G. and Marannino P., 1997, "Voltage stability analysis considering dynamic load model", International Conference on Advances in Power System Control, Operation and Management, Proceedings of APSCOM,Vol.1,396-40.

Measurement of Radon level in dwellings of regions belonging to Amritsar district of Punjab, India.

Sameer Kalia[a]
[a]PG Department of Physics and Electronics, DAV College, Amritsar, Punjab, India
Corresponding author : neerjakalia@yahoo.co.in

Neerja[b], Meetu Singh[c]
[b]PG Department of Physics and Electronics, DAV College, Amritsar, Punjab, India
[c]Department of Applied Sciences, Punjab Technical University, Jalandhar, Punjab, India.

***Abstract*-- Radon gas is a significant health threat linked to thousand of preventable deaths each year. In the present research, radon concentration was measured in the dwellings of the different villages, which are open to public, belonging to Amritsar district of Punjab. The measurements were done by using LR-115 SSNTD (solid-state nuclear track detector). The concentration of radon was found to vary from 12.24–85.35 Bqm^{-3} with an average value of 51.58 Bqm^{-3} which is less than the lower limit of the action level (200-300 Bqm^{-3}) recommended by International Commission on Radiological Protection but are on the higher side than the world average of 40 Bqm^{-3}.**

***Keywords*-- Radon Concentration, LR 115, SSNTD, Lower limit.**

I. INTRODUCTION

Radioactivity present in human environment is the major source of radiation dose being received by population. The exposure of population to natural sources of radiation has become an important issue in terms of radiological protection. Radon is a chemically inert, naturally occurring, cancer causing radioactive gas. Radon gas has no smell, color, or taste and is produced from the natural radioactive decay of uranium which is found in rocks and soil. Despite being the member of noble gases, it spontaneously decays into daughter elements. Radon-222 (radon gas), radon-220 (thoron) and radon-219 (actinon) are considered as the most common isotopes of radon **[1]**. Among the different isotopes of radon, Rn-222 is most stable with the half life of 3.82 days and decays into many short lived daughter progenies. For humans, the greatest importance among radon isotopes is attributed to 222Rn because it is the longest lived of the three naturally produced isotopes **[2]**. Radon gas escapes easily from rocks and soils into the air and tends to concentrate in enclosed spaces, such as underground mines, houses, and other buildings. Soil gas infiltration is recognized as the most important source of residential radon [3]. The radiation dose from inhaled decay products of radon (222Rn) is the dominant component of radiation exposure to the general population and causes an increased risk of lung cancer [4]. Radon was classified as a human carcinogen by International Agency for Research on Cancer [5]. In general, residential radon is regulated by a reference level of radon concentration between 200 and 300 Bqm^{-3} based on International Commission on Radiological Protection recommendations [6]. Radon has no commercial uses other than as a radiation standard for calibrating radon monitoring equipment in support of environmental surveys of homes and other buildings. According to the U.S. Environmental Protection Agency (EPA), radon is a carcinogen and the second leading cause of lung cancer in the U.S **[7]**. Many extensive studies have been performed on radioactivity worldwide in recent years **[8-10]**. Radon in soils and rocks mixes with air and rises to the surface where it quickly dilutes in the atmosphere. Indoor radon levels depend on the concentration of radon in the ground, details of construction of the house, and the way the house is heated and ventilated. It is important to note that the reduced ventilation rate helps enhance the concentration of radon and its progenies in the air [**11]**. In the present study, radon level was measured in dwellings of regions belonging to Amritsar district.

II. GEOGRAPHY OF THE STUDY AREA

The study was conducted for the villages fall under the Amritsar district of Punjab. Amritsar city situated in northern Punjab state of northwestern India. It is located at 31.63°N 74.87°E [12]. The villages from where the most of samples were collected lie in the location from 31.84°N to 74.76°E in Punjab near to the border with Pakistan (as shown in Figure 1).

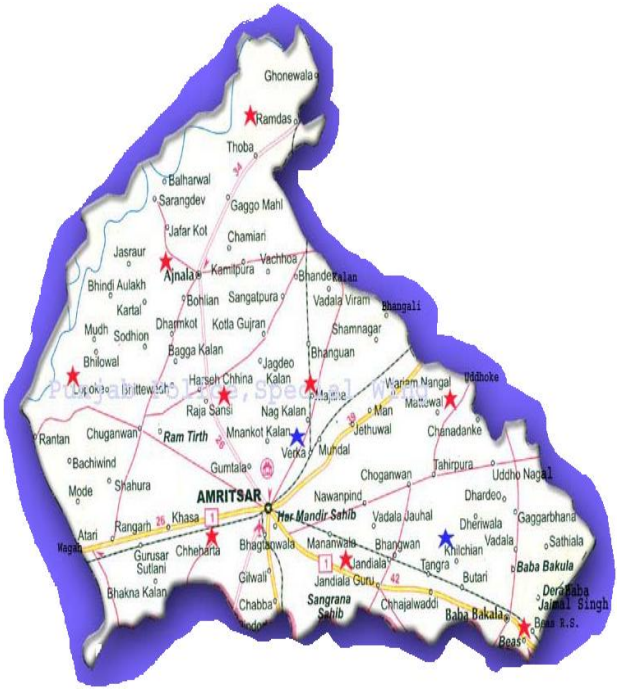


Figure 1: MAP OF THE STUDY AREA

III. MEASUREMENT TECHNIQUE

Here in the present work, LR-115 type II plastic track detector films in the bare mode technique were used to measure the concentration of radon in the indoor environment. The track etch technique is recognized as the most reliable for the integrated and long term measurement of indoor radon [13]. The detectors of size 1.5 cm X 1.5 cm were suspended in the rooms of the dwellings at a height >2 m above the ground level (so that the detectors were not disturbed by the movement of the residents) and about 1 m below the ceiling of the room so that direct alpha particles from the building material of the ceiling did not reach the detectors. After exposure of 90 days the detectors were removed and etched using 2.5 N NaOH solutions at (60$\pm$1) ºC for 90 min in a constant temperature bath. Chemical etching is essential for enlargement of the tracks, so that they become visible under the optical microscope. The etching of samples was carried out in a constant temperature bath manufactured by Narang Scientific Works Pvt. Ltd. New Delhi as shown in fig.2. It provides an accurate and precise temperature control of the etchant solution with an accuracy of $\pm$1˚C. After thorough washing, the detectors were scanned for track density measurements using an optical microscope at a magnification of 400X. The track density so obtained was converted into the units of Bqm^{-3} of the radon concentration using the calibration factor of 0.020 - 0.002 tracks cm^{-2} d^{-1} (Bq m^{-3}) determined experimentally by Eappenet.al [14], which satisfies the conditions prevailing in the Indian dwellings. In the bare mode technique there can be some contribution from thoron (220Rn) also. However, the report by UNSCEAR (2000) reveals that the contribution from 220Rn and its progeny in dwellings is in general about 10% of that of 222Rn and its progeny. So this component can be neglected from the point of view of inhalation dose [15].

Figure 2: ETCHING BATH

IV. OBSERVATIONS

The values for radon concentration observed for 20 samples suspended at 10 different locations of study area are summarized in table 1 as shown below.

Table 1: RADON CONCENTRATION IN DIFFERENT DWELLINGS.

Sample no.	Sample Location	Number of samples	Ventilation Conditions	Mean of Average Radon Concentration (in Bqm^{-3})
1.	Bal	2	Well ventilated	18.9
2.	Gurala	2	Partially ventilated	42.83
3.	Granthgarh	2	Poorly ventilated	79.05
4.	Terre	2	Well ventilated	12.24
5.	Gujjarpura	2	Partially ventilated	36.12
6.	Fathewal	2	Partially ventilated	41.87
7.	Sarawan	2	Poorly ventilated	67. 26
8.	Shekhpatti	2	Poorly ventilated	85.35
9.	Gujjapir	2	Partially ventilated	53.64
10.	Lakhuwal	2	Poorly ventilated	78.61

V. RESULTS AND DISCUSSION

As mentioned above, indoor radon levels have been measured in 20 samples from 10 dwellings of Amritsar district of Punjab, India. The results obtained are summarized in Table 1. The radon concentration values varied from 12.24–85.35 Bqm^{-3}. The value of radon concentration in the air samples from the study area lies well within the safe limit level (200-300 Bq m^{-3}) recommended by International Commission on Radiological Protection.

REFERENCES

[1] Mudd, G. (2008). Radon sources and impacts: a review of mining and non-mining issues. Reviews in Environmental Science and Biotechnology, 7 (4): 325-353.

[2] Durrani, S. A. and Iliç, R. Radon measurements by etched track detectors: Applications in radiation protection, earth sciences and the environment (Singapore: World Scientific Publishing Co. Pte Ltd) ISBN 9810226667 (1997).

[3] WHO handbook on indoor radon. (2009a). A public health perspective who.int/publications/2009/ 9789241547673_eng.pdf.

[4] United Nation Scientific Committee on the Effects of Atomic Radiation Report. (2000). Sources and effects of ionizing radiation.

In Annex B:Exposure due to Natural Radiation Sources (Vol. 1) New York: United Nation.

[5] International Agency for Research on Cancer, World Health Organization. (1988). Man-made mineral fibres and radon. In IARC Monographs on the Evaluation of Carcinogenic Risks to Humans (Vol. 43). Lyon, France: IARC. IARC.

[6] International Commission on Radiological Protection. (2010). Lung Cancer risk from radon and progeny and statement on radon. ICRP Publication 115 Annals of the ICRP, 40(1).

[7] [EPA] U.S. Environmental Protection Agency 1999. National primary drinking water Regulations;radon-222;proposed rule: Federal Registry,64(211). U.S. EPA.

[8] V. M. Choubey and R. C. Ramola, J. Environmental Geology 1997, 32(4), 258.

[9] L. Salonen and P. Huikuri, High Levels of Natural Radiation and Radon Areas: Radiation Dose and Health Effects. General Exposure Assessment, 2000, 24, 87.

[10] Ganesh Prasad, Yogesh Prasad, G. S. Gusain and R. C. Ramola, Radiation Measurements, 2008, 43(1), 375.

[11] Mehra R., Bala P., Advances in Applied Science Research, 2013, 4(1): 212-215.
[12] "Falling Rain Genomics, Inc - Amritsar". Fallingrain.com. Retrieved 2012-07-17.
[13] Jarad FA, Fremlin JH, Radiation protection Dosimetry, 1981,1, 221-226.
[14] Eappen, K. P., Ramachandran, T. V., Shaikh, A. N., & Mayya, Y. S. (2001). Calibration factor for SSNTD-based radon/thoron dosimeters.Radiation Protectionand Environment, 24(1&2), 410e414.
[15] United Nation Scientific Committee on the Effects of Atomic Radiation Report. (2000). Sources and effects of ionizing radiation. In Annex B: Exposure due to Natural Radiation Sources (Vol. 1). New York: United Nation.

Wireless Power Transfer: A Future Need

Jaspreet Singh
Research Scholar, Electronics & Communication Engineering.
Amritsar College of Engineering &Technology, Amritsar. (INDIA)
Jaspreet140@gmail.com

***Abstract*—In this paper, I present the concept of electric power transmission without using wires. Some technologies for the transmission of the electricity through wireless medium and its need is being discussed here in order to reduce the transmission and distribution losses. We also discussed its advantages, disadvantage and its economical consideration. The paper summarizes the possible ways to get useful and practical results out of all research carried out so far elsewhere.**

***Keywords*—Wireless Power Transmission, Solar Power Satellite, Microwave Electric Power, Wireless Transmission Technologies.**

I. INTRODUCTION

As the demand of the electrical power increases day by day, the power generation and losses also increases. The major issue in power system is the losses occur during distribution and transmission of electrical power. Most of the power is wasted due to the resistance of wire during transmission from main generation plant to consumer. The loss of the power is approximated as 26-30% of the power generated. However by certain levels the efficiency of power transmission can be improved by using high strength composite over head conductors and underground cables that use high temperature super conductor. But, still the transmission is insufficient. This implies that our present electrical system is 70-74% efficient. India's electricity grid has the highest transmission and distribution losses in the world – a whopping 27%. Numbers published by various Indian government agencies put that number at 30%, 40% and greater than 40%. This is attributed to technical losses (grid's inefficiencies) and theft [1].

We have to think for an alternate technology for efficient power transfer. Microwave Power Transmission may be one good alternative for electricity transmission. Wireless Power Transmission can give us a way of efficient power transmission from one point to another without using wires or any physical medium.

II. WIRELESS POWER TRANSMISSION

Nikola Tesla, Best known for his contributions to the design of the modern alternating current electricity supply system. He is indeed the "Father of Wireless". He is the one who first imagine the Wireless Power Transmission and demonstrated "Wireless Transmission of Electricity" that depends upon electrical conductivity as early as 18901 [2]. In 1893, Nikola Tesla demonstrated the illumination of vacuum bulbs without using wires for power transmission at the World Columbia Exposition in Chicago. The Wardenclyffe tower shown in Figure 1 was designed and constructed by Tesla mainly for wireless transmission of electrical power rather than telegraphy [3].

Tesla wanted to transmit electricity from this Tower to the whole globe without wires using the Ionosphere Layer. This was to be the first broadcasting system in the world.

Fig.1. 187-foot Wardenclyffe Tower (Tesla Tower) [16]

Niagara Fall's power plant was to be the source of the transmitted electricity [4]. In 1904, an airship ship motor of 0.1 horsepower is driven by transmitting power through space from a distance of least 100 feet [5]. First paper proposing microwave energy for power transmission published by Brown in 1961, and in 1964 the demonstration of helicopter with microwave-powered was done with microwave beam at 2.45 GHz [6] from the range of 2.4GHz – 2.5 GHz frequency band which is reserved for Industrial, Scientific, and Medical (ISM) applications.

In 1965 Experiments at Goldstone in California in power transmission without wires in the range of tens of kilowatts have been performed [7] and at Grand Bassin on Reunion

Island in 1997 [8]. Microwave Ionosphere Non-linear Interaction Experiment was the world's first MPT experiment in the ionosphere and rocket experiment is demonstrated in 1983 at Japan [9]. Similarly, the world's first fuel free airplane powered by microwave energy from ground was reported in 1987 at Canada. This system is called SHARP (Stationary High – Altitude Relay Platform) [10].

In 2003, NASA demonstrated a laser powered model airplane indoors at Dryden Flight Research Centre. In 2004 Japan proposed wireless charging of electric motor vehicles by Microwave Power Transmission. Powercast introduced wireless power transfer technology at the 2007 Consumer Electronics Show using RF energy [11].

A. Conponents of Wireless Power Transmission

Most important components of Wireless Power Transmission are Microwave Generator, Transmitting antenna and Receiving antenna.

1) Microwave Generator

The microwave transmitting devices are classified as Microwave Vacuum Tubes (magnetron, klystron, Travelling Wave Tube (TWT), and Microwave Power Module (MPM)) and Semiconductor Microwave transmitters (GaAs MESFET, SiC MESFET, GaN pHEMT, AlGaN/GaN HFET, and InGaAS). Magnetron is widely used for experimentation of WPT. The microwave transmission often uses 2.45GHz or 5.8GHz of ISM band. The other choices of frequencies are 8.5 GHz [12], 10 GHz [13] and 35 GHz [14]. The highest efficiency over 90% is achieved at 2.45 GHz among all the frequencies [14].

2) Transmitting Antenna

The slotted wave guide antenna, parabolic dish antenna and microstrip patch antenna are the most popular type of transmitting antenna. The slotted waveguide antennas suppose to be ideal for power transmission because of its high aperture efficiency (> 95%) and high power handling capability.

3) Receiving Antenna

The Receiving antenna is a passive element consists of antenna, rectifying circuit with a low pass filter between the antennas and rectifying diode. The antenna used in rectenna may be dipole, Yagi – Uda, microstrip or parabolic dish antenna. The patch dipole antenna achieved the highest efficiency among the all. The performance of various printed rectenna is shown in Table I. Schottky barrier diodes (GaAs-W, Si, and GaAs) are usually used in the rectifying circuit due to the faster reverse recovery time and much lower forward voltage drop and good RF characteristics.

III. APPLICATIONS

Wireless power transmission would have many interesting applications. Some of the applications involve vehicles from a remote power source or simply powering devices. Some applications are as follows-

- Satellites with solar array can be placed at Geosynchronous Earth Orbit, So that it can transmit the power as microwaves to the earth station known as Solar Power Satellites (SPS).
- It can power various devices for their operation as well as charging purposes
- Wireless Power Transmission can be used in very effective manner for many industrial applications. Uses of direct microwave power across rotating and moving joints eliminate costly and failure-prone wiring [15].
- Direct microwave power for wireless actuators and sensors, eliminating the need for expensive power wiring or battery replacement.

IV. MERITS AND DEMERITS OF WIRELESS POWER TRANSMISSION

Wireless power transmission is consider as one of the most emerging and effective power transmission technique and has following merits and demerits of using it.

- Low Transmission Loss and High Efficiency: - Due to no physical medium the efficiency of the wireless power transmission can be as high as 96 or 97 per cent, and there are practically no losses.
- Wireless Power transmission eliminates the insufficient cost of towers and cables.
- Some places where the need of electricity exists but the installation of the cables is not possible. This System could be a good idea.
- Some Biological elects may take place with this system.

V. CONCLUSION

The Wireless Transmission of Electricity is not only theory, it is now a reality. Many observations, experiments and measurements have done. Dr. Nikola Tesla is the father of the Wireless Transmission. Wireless Electricity Transmission have the advantages of high efficiency and can be transmitted over large distance and also eliminate the need of costly, inefficient cables, substations and towers. Dr. Neville of NASA states "You don't need cable to receive power. We can send it to consumer like a cell phone call – when you want it, where you want it, in real time". It has a amazing economic impact to human society.

References

[1] http://cleantechindia.wordpress.com/2008/07/16/indiaselectricity-transmission-and-distribution-losses/

[2] Nikola Tesla, My Inventions, Ben Johnston, Ed., Austin, Hart Brothers, p. 91, 1982.

[3] Nikola Tesla, "The Transmission of Electrical Energy Without Wires as a Means for Furthering Peace," Electrical World and Engineer. Jan. 7, p. 21, 1905.

[4] Nikola Tesla, ―The Transmission of Electrical Energy without Wires as a Means for Furthering Peace, Electrical World and Engineer. Jan. 7, p. 21, 1905
[5] The Electrician (London), 1904.
[6] W.C. Brown, J.R. Mims and N.I. Heenan, "An Experimental Microwave-Powered Helicopter", 965 IEEE International Convention Record, Vol. 13, Part 5, pp.225-235.
[7] Brown., W. C. (September 1984). "The History of Power Transmission by Radio Waves". Microwave Theory and Techniques, IEEE Transactions on (Volume: 32, Issue: 9 On page(s): 1230- 1242 + ISSN: 0018-9480). http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1132833.
[8] POINT-TO-POINT WIRELESS POWER TRANSPORTATION IN REUNION ISLAND 48th International Astronautical Congress, Turin, Italy, 6-10 October 1997 - IAF-97-R.4.08 J. D. Lan Sun Luk, A. Celeste, P. Romanacce, L. Chane Kuang Sang, J. C. Gatina - University of La Reunion - Faculty of Science and Technology.
[9] Matsumoto, H.N. Kaya, I. Kimura, S. Miyatake, M. Nagatomo, and T. Obayashi, MINIX Project toward the Solar Power Satellites --- Rocket experiment of microwave energy transmission and associated plasma physics in the ionosphere, ISAS space energy symposium, pp 69-76, 1986.
[10] J.J. Schelesak, A. Alden and T. Ohno, A microwave powered high altitude platform, IEEE MTT-S Int. Symp. Digest, pp - 283-286, 1988.
[11] "CES Best of 2007"
[12] www.tgdaily.com
[13] L.W. Epp, A.R. Khan, H.K. Smith, and R.P. Smith, "A compact dual-polarized 8.51-GHz rectenna for high-voltage (50 V) actuator applications," IEEE Trans. Microwave Theory Tech., vol. 48, pp. 111-120, 2000.
[14] T-WYoo and K. Chang, "Theoretical and experimental development of 10 and 35 GHz rectenna," IEEE Trans. Microwave Theory Tech., vol. 40, pp. 1259-1266, 1992.
[15] WiTricity Corp. ― Applications of WiTricity Technology‖, www.witricity.com/pages/application.htm

Energy and Intensity distribution of Two-Photon Compton Scattered Radiation

M. B. Saddi*, B. S. Sandhu and B. Singh
Physics Department, Punjabi University, Patiala-147002, India
E-mail: saddimanju@rediffmail.com, Tel: +91 0 9872235057

Abstract:

The collision integral cross-sections of two-photon Compton process are measured experimentally for 662 keV incident gamma photons. The energy spectra of one of the two final photons, originating in this process, in direction of the gamma ray detector are observed as a long tail to the single-photon Compton line on lower side of the full energy peak in the recorded spectra. An inverse response matrix converts the observed pulse-height distribution of a NaI(Tl) scintillation detector to a true photon spectrum. This also results in extraction of events originating from two-photon Compton interactions. The present measured values of collision integral cross-section, although of same magnitude, deviate from the corresponding values obtained from the theory. In view of the magnitude of deviations, in addition to small value of probability of occurrence of this process, the agreement of measured values with theory is reasonably acceptable.

1. Introduction

The Two-photon Compton scattering is a quantum electrodynamics (QED) process in which the interaction of a gamma photon with an electron results in a final state consisting of two simultaneous degraded photons at the same time as the recoil electron. This phenomenon needs to be investigated in detail because it is a major background process to the study of another QED process namely photon splitting in the fields of heavy atoms, a test of QED implicitly, a mechanism of photon multiplication along with bremsstrahlung in astrophysics and there is appreciable contribution to attenuation coefficients at higher incident photon energies where this process is more likely to occur.

Mandl and Skyrme [1] using S-matrix formalism of quantum electrodynamics have provided an exact theory of this process. The triply differential collision cross-section of this process, involves two solid angles and one independent final photon energy. Thus all the experimental observations on this process performed so far are based on coincidence measurements. In the experiments reported on this process, the directions of both final photons are kept fixed and their coincidences are counted. The greatest difficulty in such experiments lies in the low value of intensity to be measured as the cross-section for this process is already low in itself.

The singly differential collision integral cross-sections of this process, obtained by integrating over direction of one of the two final photons and energy carried by that photon, is given by

$$\left(\frac{\partial\sigma_D}{\partial\Omega_1}\right) = \int_{E_{lower}}^{E_{upper}} \int_0^{2\pi} \int_0^{\pi} \left(\frac{\partial^3\sigma_D}{\partial\Omega_1\,\partial\Omega_2\partial E_1}\right) \sin\theta_2\, d\theta_2\, d\phi_2 dE \quad (1)$$

The characteristic features of this higher order process with regard to these cross-sections are still to be investigated. In the present measurements, the singly differential collision integral cross-sections have been measured experimentally for 662 keV incident gamma photons. The energy spectra of one of the two emitted photons, originating in this process, in the direction of the gamma detector are observed as a long tail to the single-photon Compton line on the lower side of the full energy peak in the recorded scattered energy spectra.

2. Experimental set-up

In the present measurements an intense collimated beam of gamma rays from a 6 Ci (1 Ci = 37 GBq) ^{137}Cs radioactive source is made to impinge on a thin aluminium target. The details of the experimental set-up and procedure of present measurements are given in our previous measurements [2]. The gamma ray detector, 51mm diameter x 51mm thick NaI(Tl) scintillation crystal, detects the photons originating from interaction of incident gamma radiation with the target electrons at angular positions of 110°.

The target-in scattered spectra are recorded for a period of 10 ks by placing each of the four different aluminium targets (having thicknesses 40.0, 60.8, 159.6 and 236.4 mg-cm^{-2}) in the primary gamma ray beam. The events registered in the recorded energy spectra originate from single and two-photon Compton

scattering in which one of the two final photons is emitted in the direction of gamma detector. In addition to these, there are many other systematic effects contributing to the registered events.

The formula, derivation reported in measurements [6], used to evaluate the doubly differential collision integral cross-section is

$$\left(\frac{d^2\sigma_D}{d\Omega_1 dE_1}\right)_{\Delta E_1} = \frac{N_d}{N_S}\left(\frac{d\sigma_{KN}}{d\Omega_1}\right)\frac{\beta_{\gamma s}}{\beta_{\gamma d}}\frac{\varepsilon'(E')}{\varepsilon_1(\Delta E_1)} \quad (2)$$

Where N_d and N_s are count rates resulting from double and single-photon Compton events respectively. $\left(\frac{d\sigma_{KN}}{d\Omega_1}\right)$ is the Klein-Nishina cross-section for single-photon Compton scattering in direction of the gamma detector. $\varepsilon'(E')$ is photo-peak efficiency of the gamma ray detector corresponding to the energy E' due to single-photon Compton scattering in the direction of the gamma ray detector and $\varepsilon_1(\Delta E_1)$ is average photo-peak efficiency of the gamma detector corresponding to photon energy (in the interval E_1 and $E_1 + \Delta E_1$) of one of the two final photons resulting from double photon Compton scattering and detected by the gamma ray detector. The quantities $\beta_{\gamma s}$ and $\beta_{\gamma d}$ are the self-absorption correction factors [7] for the incident and scattered radiations in single-photon and two-photon Compton scattering processes respectively. The quantities such as N_d and N_S are measured experimentally.

3. Results and discussions

In the present experiment, the scattered energy spectra are recorded for a period of 230 ks for each thickness of the aluminium target and the observed spectra at scattering angle of 110° are shown in Fig. 1.

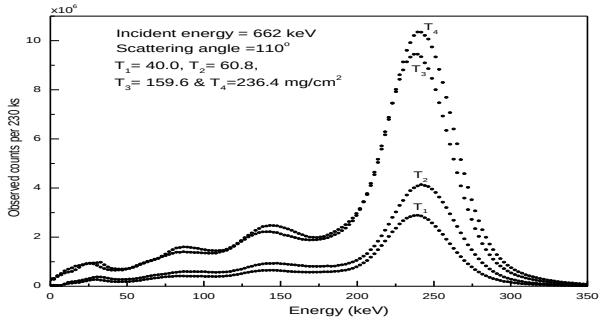


Fig. 1: Observed scattered spectra for 662 keV incident photons at scattering angle of 110° for different target thicknesses.

The main contribution to energy spread is caused by intrinsic energy resolution of the gamma detector. The energy spread due to detector aperture is small in comparison to intrinsic energy resolution of the gamma detector. No doubt the contribution to energy spread (FWHM) due to finite target thickness shows a slight increase with target thickness but is also negligible in comparison to resolution of the gamma detector. This increase in energy spread as the target thickness increases is mainly caused by multiple interactions of the incident gamma photons in the target with the final photon escaping in the direction of gamma detector. Each of the resulting spectra is corrected for backscattered events and X-rays originating from lead shielding. One such typical spectrum (curve-a) for target thickness of 60.8 mg-cm^{-2} is shown in Fig. 2.

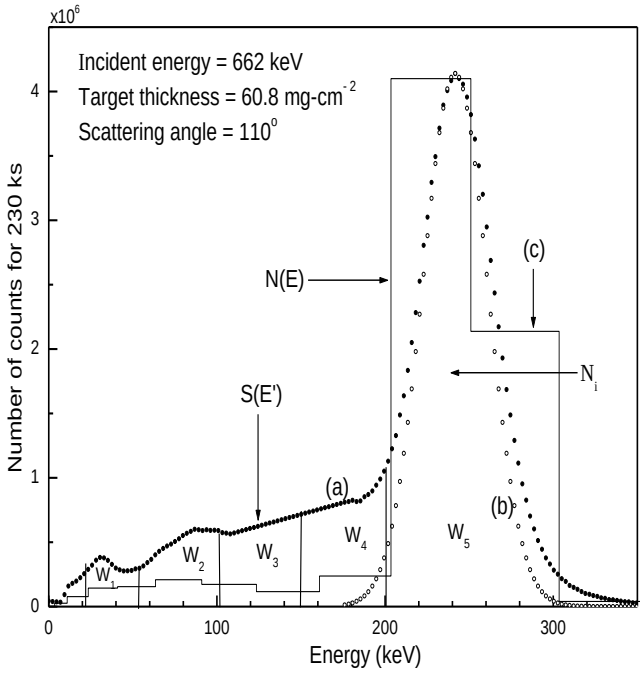


Fig. 2: Experimentally observed pulse-height distributions, S(E'), (curve-a) corrected for backscattered events for 60.8 mg/cm^2 target thickness. Normalized analytically reconstructed singly scattered full energy peak (curve-b) and resulting calculated histogram (curve-c) of N(E) converting observed pulse-height distribution to a true photon spectrum.

The events registered in the spectrum account for the followings:

(i) One of the two final photons originating from two-photon Compton scattering process in direction of the gamma ray

detector.

(ii) The photon originating from single-photon Compton scattering (SPCS) process in the direction of gamma detector.

(iii) The bremsstrahlung, originating from slowing down of photo-electrons and recoil-Compton electrons in the target, in direction of the gamma detector, and

(iv) Multiple interactions taking place in the target in which the final photon escapes in direction of the gamma detector.

These spectra are divided into five different energy windows, W_1 to W_5, each having nearly 50 keV span except for the first and last energy windows which have spans nearly 30 and 41 keV respectively. The energy selection criterion is from channel number point of view and is then converted into energy value. The two-photon Compton collision integral cross-section is evaluated first at the scattered peak window and then in the Compton continuum part. To obtain counts purely due to two-photon Compton scattering, in which one of the two final photons is emitted in direction of the gamma detector, the counts due to other processes are eliminated or minimized. The major contribution among the registered events is from single-photon Compton scattering (SPCS). The spectrum of SPCS is reconstructed analytically on the basis of Gaussian nature of the scattered gamma ray peak using the following equation

$$y(E) = y(E_o)\exp\left\{-\frac{\left(\frac{E-E_o}{\sigma}\right)^2}{4\ln(2)}\right\} \qquad (3)$$

Where $y(E_o)$ is the number of counts at the peak energy E_o. The quantity σ is FWHM of the NaI(Tl) detector at energy E_o. The reconstructed spectrum is then normalized at the peak of the experimentally observed spectrum and thus results in events purely due to the single-photon Compton scattering at the Compton scattered energy window. A typical analytically reconstructed spectrum (curve-b), taking into account the angular spreads due to source collimator opening and detector aperture [2]. The subtraction of this normalized singly scattered spectrum from the observed experimental spectrum results in elimination of events under the full energy peak originating from single-photon Compton scattering (SPCS) process in the direction of gamma detector. However to take into account the contribution due to low pulse-height counts resulting from the partial absorption of higher energy photons, we make use of an inverse matrix approach which shifts these low pulse-height counts into their photo-peak energy region by unscrambling the pulse-height distributions recorded by NaI(Tl) gamma ray detector. The curve-c of Fig. 2 is the resulting calculated histogram of N(E) converting pulse-height distribution S(E') to a photon spectrum. Low pulse-height counts resulting from partial absorption of higher energy photons are shifted to the photo-peak energy region. The events under the histogram (curve-c) in Compton continuum accounts for photons of reduced energy (less than that of inelastic Compton scattered peak) originating from two photon Compton scattering (having continuous energy spectra and in which one of the two final photons is emitted in direction of the gamma detector), bremsstrahlung and multiple interactions in the target in which final photon escapes in the direction of gamma detector.

The two-photon Compton collision cross-section is evaluated first at the scattered peak window and then in the Compton continuum part. The area under the analytically reconstructed full energy peak provides single-photon Compton scattering (SPCS) count rate, N_s. The events under the calculated histogram corresponding to energy range of inelastic scattered peak account for single and two-photon Compton scattering, in addition to bremsstrahlung and multiply scattered events having energy equal to that of singly scattered ones. The events under analytically reconstructed singly scattered Compton profile are divided by peak-to-total ratio, $\varepsilon_p(E)$, of the gamma detector and then their subtraction from events under the calculated histogram in the specified energy range results in elimination of events originating from single-photon Compton scattering. These residual events are divided by intrinsic (crystal) efficiency [7], and when corrected for iodine escape peak [8], and absorptions in aluminium window [9] of scintillation detector and in the air column [10] present between target and detector, provides emergent flux from the target at 110° originating from double-photon Compton scattering, bremsstrahlung and multiple interactions in the target. This process is repeated for observed pulse-height distributions recorded for all the four different aluminium targets (having thicknesses 40.0, 60.8, 159.6 and 236.4 mg-cm^{-2}) used in the present measurements. An experimental approach suggested in our previous measurements [5], is used to eliminate the bremsstrahlung and multiple-scattering events. The two-photon Compton count rate varies linearly and the bremsstrahlung count rate quadratically with target thickness. The dependence of count rate of multiple-Compton scattering will be higher power in target thickness. The targets used in the present experiment are of small thickness, so the probability for multiple interactions taking place in the target, in which the final photon escapes in the direction of the gamma detector, is negligible. A plot of residual counts per unit thickness versus thickness is shown in Fig. 3.

The extrapolation of this linear curve to unit thickness provides the counts purely due to the two-photon Compton scattering in which one of the two final photons is emitted in direction of the detector. The bremsstrahlung amounts on the average to about 9.4% of the double-photon Compton scattering

count rate at scattering angle of 110° for 236.4 mg-cm^{-2} target thickness.

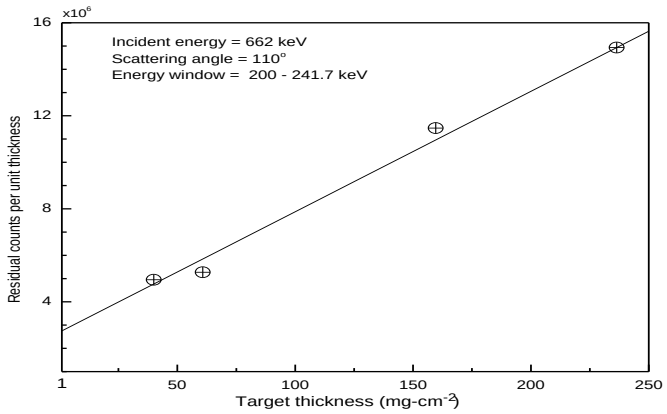


Fig. 3: The count rate per unit thickness (double + bremsstrahlung + multiple scattering) - vs – target thickness for energy window = 200 – 241.7 keV.

In Fig. 2, the energy window (W_4 with energy span from 150.8-200.0 keV) to the left of the observed inelastic peak accounts for events originating from two-photon Compton scattering, multiple scatterings and bremsstrahlung produced by recoiling electrons in the thick target. These events do not result from single-photon Compton scattering of 662 keV incident photons. Some of the photons of this energy region get registered in the lower bin meshes owing to partial absorption of energy in the gamma detector. The use of above stated procedure employing inverse response matrix, and elimination of bremsstrahlung and multiply scattered events provides numbers of events purely due to two-photon Compton scattering in which one of the two final photons having energy in the range from 150.8–200.0 keV is emitted in direction of the detector. The procedure is then repeated for other selected windows W_3, W_2 and W_1 having energy spans of 101 - 150.8, 51 - 101 and 21.3 - 51.0 respectively. The normal Compton scattering count rate at this angular position being 1225824.5 $\pm$ 73.0 per ks. The statistical uncertainty corresponding to this high counting rate is thus negligible. On the other hand statistical uncertainty in two-photon Compton scattering is quite significant (3-12.3%).

The experimental measured values of count rates originating purely from two-photon Compton scattering, in which one of the two final photons is emitted in direction of gamma detector, for different selected energy windows are given in column 3 of Table 1.

Table 1: Experimental measured values of doubly differential collision integral cross-sections of two photon-Compton scattering at scattering angle of 110° for 662 keV incident gamma photons.

Energy window	ΔE_1 (in keV)	N_d (per ks)	Experimental $\left(\frac{d^2\sigma_D}{d\Omega_1 dE_1}\right)_{\Delta E_1}$
W1	21.3 – 51.0	1191.8 ± 10.9	1.02 ± 0.04
W2	51.0 – 101.0	636.8 ± 74.4	0.53 ± 0.06
W3	101.0 – 150.8	831.2 ± 74.8	0.67 ± 0.06
W4	150.8 – 200.0	2902.4 ± 16.3	2.46 ± 0.04
W5	200.0 – 241.7	12083.5±105.4	11.09 ± 0.09

The errors quoted in count rates and experimentally measured values of collision integral cross-section represent statistical uncertainties only.

The experimental value of singly differential collision cross section, for 0.662 MeV incident photon, comes out to be (1.58$\pm$0.02) x 10^{-28} cm^2/sr. This is in agreement with the deduced value of 1.66 x 10^{-28} cm^2/sr [1]. Thus the present measurements support the theory of Mandl and Skyrme. The measured value is to be compared with the Klein-Nishina cross section having value 1.18 x 10^{-26} cm^2/sr, hence the probability for occurrence of two photon Compton scattering is fine structure constant (α) 1/137 times that of single Photon Compton scattering, a prediction of the theory of two photon Compton scattering.

An overall error of 8-15% is estimated in the present measurements and is due to statistical uncertainties in the count rates due to two (3-12.3%) and single-photon (<0.5%) Compton scatterings, detector efficiency (≅5%), target thickness (<1.1%) and self-absorption (<1%) of incident and scattered radiation in the target. The major contribution to the error is caused by statistical uncertainties in the count rate due to two-photon Compton scattering. This uncertainty is small when one of the two final photons is soft. The maximum uncertainty in the measurement of energy is estimated to be less than 1%. The probability of photons being split by the nuclear electrostatic field [11] followed by one of the photons travelling in direction of the gamma detector is negligible.

The measured values of collision cross-section are although of the same magnitude but deviate from the corresponding values calculated from the theory, especially for W_2 and W_4 windows. The major contribution to observed counts for each energy window results from single-photon Compton scattering. The spectra for these events are reconstructed analytically on the basis of Gaussian nature of scattered gamma ray peak. It is impossible to state with certainty what fraction of the detector volume contributes to full or partial absorption of the

photon energy incident on it, and may be the possible reason for these deviations. On the other hand, keeping in mind that the probability for occurrence of this process is quite small and order of deviations, the agreement of the measured values with theory is acceptable.

There are no other experimental data, except at scattering angles of 90° [6] and 30° [12], available for comparison with the present results of two-photon Compton collision cross-section at scattering angle of 110°. The present measurements, employing response matrix technique for spectrum unfolding, fulfil the objective of observing double-photon Compton scattering without the use of coincidence measurements. Like earlier investigations [**3-6**, 12], the present measurements also confirm that the probability of occurrence of this process is being quite small, energy spectra of the two final photons being continuous and the occurrence of this process is more pronounced when one of the two final photons is soft. Moreover, the present measurements are a test of QED in an implicit way and support the collision differential cross-section formula provided by Mandl and Skyrme [1]. Here it is also important to note that the detector response unfolding converting the observed pulse-height distributions to a photon energy spectrum is quite satisfactory. Our present findings will serve very good reference for future investigations on this process. The phenomenon further requires more experimental data at higher incident photon energies to support the currently acceptable theory of this process.

References

1. F. Mandl and T.H.R. Skyrme, Proc Roy Soc (London) **A 215** (1952) 497.
2. M.B. Saddi, B.S. Sandhu, and B. Singh, Nucl. Instr. & Meth. **B 266** (2008) 3309.
3. M.R. McGie, F.P. Brady, and W.J. Knox, Phys. Rev. **152** (1966) 1190.
4. B.S. Sandhu, R. Dewan, B. Singh, and B.S. Ghumman, Phys. Rev. **A 60** (1999) 4600.
5. B.S. Sandhu, R. Dewan, M.B. Saddi, B. Singh, and B.S. Ghumman, Nucl. Instr. & Meth. **B 168** (2000) 329.
6. M. B. Saddi, B.S. Sandhu, and B. Singh, Ann. Nucl. Energy **33** (2006) 271.
7. C.E. Crouthamel, Applied Gamma-ray Spectrometry, (Pergamon Press, London, 1960) pp202-216, 673.
8. P. Axel, Rev. Sci. Instrum. **25** (1954) 39.
9. W. J. Veigele, At. Data **5(1)** (1973) 51.
10. J.H. Hubbell, Radiation Research **70** (1977) 58.
11. R.N. Lee, A.I. Milstein, and V.M. Strakhovenko, Phys. Rev. **A 58** (1998) 1757.
12. Gulshan Datta, M. B. Saddi, Bhajan Singh, and B.S. Sandhu, Radiation Measurements **42**, (2007) 256.

Study of production methods of biodiesel and performance characteristics of CI engine fuelled with various biodiesel blends

Arshdeep Singh Gill[1], Nehal Bansal[1],
[1](Department of Mechanical Engineering
A.C.E.T., Punjab Technical University
Amritsar. INDIA

Amit Sarin[2]
[2](Department of Applied Sciences
A.C.E.T., Punjab Technical University
Amritsar INDIA

***ABSTRACT*—The massive generation of waste and their significant environmental consequences has risen in the past two decades. This is due to the rapid industrialization and its associated impact upon the world economy. As the fossil fuels are depleting day by day and there are lots of technological advances which are highly dependent on the fossil fuels, there is an utmost need to look after some alternative renewable source. This arouses the interest in new sustainable energy source and led to the highly extensive research towards Biodiesel and its production. This paper will delve into the production and performance characteristics of biodiesel along with its blends and the problems associated with it. Biodiesel is one of the best available sources to fulfill the energy demand of the world. The production of biodiesel from vegetable oil comprises of several methods which include transesterification, thermal cracking, micro emulsion, etc. Among these methods; transesterification is an attractive and widely accepted technique. This present paper shows that brake specific fuel consumption increases with the increase in concentration of biodiesel, whereas brake thermal efficiency decreases. Fuel with lower biodiesel content can be used in engine without any modification. The variation of these above parameters is not fixed, but mainly depends on fuel to fuel.**

I. INTRODUCTION

The various factors responsible for the search for alternative sources of energy include global warming, increase in energy demand and availability of latest technologies. With the commercialization of bioenergy, there is an effective way to fight against the problem of petroleum scarce and their influences on the environment by finding an alternative fuel [1]. The countries that are already using alternative fuel for the transportation sector are Brazil, the United States, Germany, Australia, Italy and Austria [2]. Biodiesel fuels are attracting attention worldwide as blending components or direct replacements for diesel fuel in vehicle engines. Biodiesel is mainly a long chain of lower alkyl fatty acid (chain length C14–C22) and chain of methanol or ethanol. The various properties of Biodiesel which make it superior over petro diesel are, biodiesel is renewable, non-toxic and free of sulfur and aromatics [3].Biodiesel will be a realistic fuel for coming future and it will be highly attractive because of its environmental benefits. Though biodiesel costs 1.5-3 times more than fossil diesel, but through large scale production cost can be minimized. Biodiesel will be a reasonably available fuel in the near future depending upon the governmental policies. The major advantage of using biodiesel is that it is a derivative of natural products. As demand rises, the production of the required agricultural products can be increased to compensate [4]. This present paper generally comprises of two parts. The first half includes the various methods used for the production of biodiesel and the second half emphasis on the performance of different types of biodiesel and their blends.

Table 1

Abbreviations	
CI	Compressed Ignition
FAME	fatty-acid methyl esters
FAEE	fatty-acid ethyl esters
SANS	small-angle neutron scattering
FFEM	freeze-fracture electron microscopy
SFC	Specific fuel consumption
WCO	Waste Cooking Oil
DI	Direct Injection
BTE	Brake Thermal Efficiency
B20	20 vol.% Biodiesel in blend with diesel
UCOME	Used Cooking Oil Methyl Ester
BSFC	Brake Specific Fuel Consumption
WFOME	Waste Fried Oil Methyl Ester

II. BIODIESEL

Biodiesel is a renewable alternate fuel for diesel engines. It is produced chemically by reacting a vegetable oil or animal fat with alcohol. The most common acyl acceptors used are alcohols, particularly methanol and ethanol. Methanol is more reactive and cheaper than ethanol. The fatty-acid methyl esters (FAME) produced from methanol is more volatile than fatty-acid ethyl esters (FAEE). Ethanol can be easily produced from renewable sources through the process of fermentation whereas methanol is currently mainly produced from non-renewable fossil sources, such as natural gas. FAME and FAEE show slight differences in their characteristics. FAME has slightly low viscosity and high cloud and pour points than the corresponding FAEE. Thus biodiesel is defined as monoalkyl ester derivatives of long chain fatty acids [5, 6]. Biodiesel is a clear amber-yellow liquid with a similar viscosity to that of

petroleum diesel. Biodiesel is a non-flammable fuel, with a flash point of 423 K as compared to 337 K for petroleum diesel. The concentration of biodiesel in the blends can be identified by a single nomenclature, known as the BXX nomenclature, where XX represents the percentage in volume of the biodiesel in the diesel/biodiesel blend. For example, B2, B5, B20 and B100 are fuels with a biodiesel concentration of 2%, 5%, 20% and 100% respectively. The B5 blend can be used as such in diesel engine without any modification [7].

III. PRODUCTION

Huge efforts have been made to develop various derivatives of vegetable-oil having similar properties and performance to that of hydrocarbon-based diesel fuels. The various troubles introduced by replacing diesel fuels by tri-glycerides are mostly associated with their (i) high viscosity; (ii) low stability against oxidation; and (iii) low volatility, which influences the formation of a relatively high amount of ash due to incomplete combustion [8]. These can be altered by four methods, as follows:

A. Direct use and blending

The blends of vegetable oil and diesel are used as a fuel in diesel engines. The direct use of vegetable oil in diesel engine has generally been considered to be unsatisfactory and impractical. The various problems include high viscosity, free fatty-acid content, acid composition, polymerization during storage and combustion, and carbon deposits. The major drawback of using pure vegetable oil as fuels in compression–ignition engine is increase in its viscosity. Micro-emulsification, pyrolysis and transesterification have been used as a remedy to solve the problems encountered due to high fuel viscosity [9].

B. Micro emulsion

Micro emulsions are clear or translucent, dispersions of oil, water or a surfactant. The diameter of droplet of micro emulsion range from 100 to 1000 Å. Vegetable oil along with an ester and dispersant (co-solvent) can be converted into a micro emulsion. The second alternative to produce micro emulsion is from alcohol, surfactant and vegetable oil. The reason for lower volumetric heating values of micro emulsion as compared to conventional diesel is the presence of alcohol content. The present alcohol content is used as cooling agent in combustion chamber which reduces nozzle choking. The performance of micro emulsion of methanol with vegetable oil is preferably same to diesel fuels. The phase behavior of a micro emulsion was studied by wellert et al. [10] using small-angle neutron scattering (SANS) and freeze-fracture electron microscopy (FFEM) in which bi-continuous phase was identified. Micro emulsion method can be used in the determination of sodium and potassium present in biodiesel introduced by Jesus et al. [11] using a water-in-oil emulsion process. This process can be used for various types of biodiesel produced from different sources such as soybeans, castor, sunflower oil, animal fat and other vegetable oil.

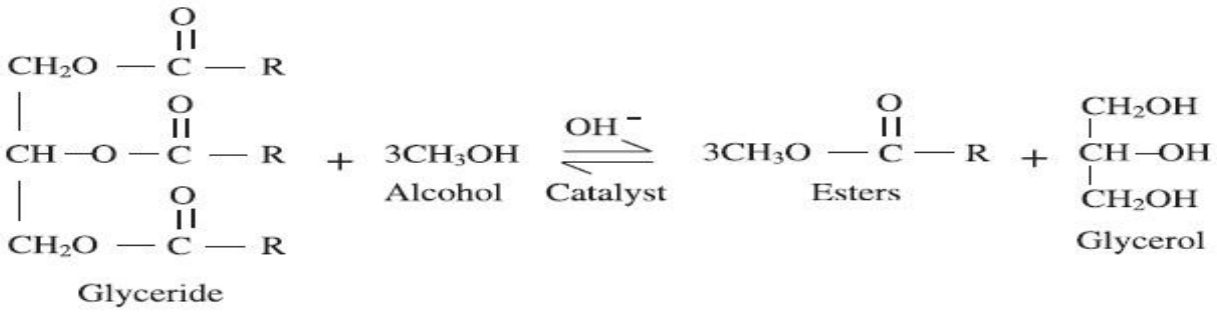
C. Thermal cracking (pyrolysis)

Pyrolysis is the process of converting one organic substance into another by using heat in the presence of a catalyst. The various pyrolyzed material include animal fat, vegetable oil, methyl esters of fatty acids. Many investigators have studied the pyrolysis of triglycerides to obtain products suitable for diesel engines. Thermal decomposition of triglycerides produces alkanes, alkenes, alkadienes, aromatics and carboxylic acids [12, 13].

D. Transesterification

Transesterification is a process of producing fatty-acid esters and glycerol in the presence of an alkaline catalyst by reacting triglyceride such as vegetable oil with alcohol. Methanol and ethanol are highly used in transesterification process because of their low cost and various physical and chemical advantages too. They are highly soluble and react vigorously with tri-glycerides and NaOH. Biodiesel production is carried out through an alkaline catalyzed transesterification process. Sodium and potassium meth oxide are widely used catalysts for the base-catalyzed transesterification of triglycerides [14, 15].

Equation 1



The kinetics of palm-oil transesterification in a batch reactor is studied by Darnoko and Cheryan [16]. The study showed that the rate of the transesterification process increases with the increase in temperature. The kinetics reaction depends on the individual rate constants for the conversion of glycerides to di-glycerides, mono-glycerides and alcohol esters. The rate of transesterification process increases with the increase in temperature leading to higher rate of mass transfer in a short time.

IV. PERFORMANCE REVIEW

Literature survey reveals that biodiesel perform satisfactorily during diesel engine operation. Biodiesel as an eco-friendly and

renewable fuel is getting the attention of researchers/scientists of all over the world. Pryor et al. [17] performed short-term and long-term test using soybean oil as a fuel. They reported that the in short-term test the engine performance was similar but due to power loss and carbon build-up on the injectors the study on performance could not be carried out in long-term test. Strayer et al. [18] reported that the Specific Fuel Consumption (SFC) was higher with degummed canola oil and rapeseed oil and the performance of engine was better with degummed canola oil as compared to crude canola oil. Hamaski et al. [19] studied the performance of a single-cylinder engine fuelled with the various blends of Waste Cooking Oil (WCO) with diesel fuel having different acid values at different loads and constant engine speed. Mc Donnel et al. [20] investigated the performance of diesel engine blended with semi-refined rapeseed oil. They concluded that the engine performance was better for 25/75 rapeseed oil/diesel blend. They observed carbon deposits on injectors, even though there was no wear on engine components or lubricating oil contamination. Monyem and Gerpen [21] studied the impact of oxidized biodiesel on engine performance. The engine performance of the pure biodiesels and their blends were similar to that of diesel fuel with the same thermal efficiency, but higher fuel consumption. The performance of turbo-charged four-cylinder Direct Injection (DI) diesel engine with mustard oil/diesel blend was studied by Niemi et al. [22]. They concluded that the engine develops power equal to that of diesel. The performance of direct injection diesel engine blended with ethyl ester of waste vegetable oil blends in proportions of 75/25, 50/50, 25/75 was studied at different speed by Al-Widyan [23]. A higher fuel economy was recorded. They concluded that 75/25 WCO blend gives the best performance. They observed that the Brake Thermal Efficiency (BTE) was similar in all cases. The performance and durability test of a diesel engine fuelled with crude palm oil was studied by Bari et al. [24]. They observed heavy carbon deposits in the combustion chamber, wear of piston rings and uneven spray by injection pump. Kalligeros [25] investigated the performance of stationery diesel engine by using two different compositions of biodiesel below 50% concentration. Engine performance was same for two different biodiesels. Canakci and Van Gerpen [26] studied the performance of 57 kW engine using waste oil and soybean oil as two different biodiesel fuels. They reported 2.5% and 20% increase in BSFC of waste and soybean oil and 14% from those with pure biodiesel. They observed no variations in BTE when using different types of biodiesel blends. Pramanik [27] investigated the performance of engine blended with jatropha oil and diesel fuel. Acceptable thermal efficiencies were obtained for blends containing up to 50% of jatropha oil. However, SFC was reduced due to decrease in the viscosity of the vegetable oil. O¨zkan et al. [28] observed 25% power loss when WCO biodiesel is tested in a single-cylinder DI diesel engine. The maximum torque was 21.0 Nm for diesel at 1500 rpm, and a maximum torque of 18.4 Nm was recorded for WCO biodiesel at 2250 rpm. Also, a significant change of 11.5% SFC recorded for diesel than that of biodiesel. Ramadhas et al. [29] studied the performance of 5.5 kW single cylinder direct injection diesel engine using blends of rubber seed oil and diesel fuel in proportion of 20/80, 40/60, 60/40 and 80/20. They concluded that the blend up to 80/20 gives acceptable SFC and thermal efficiency. Murillo et al. investigated the performance of a three-cylinder naturally aspirated engine using WCO blends [30]. They reported 7.14% power loss at full load. Also rated power was reduced by 1.50% using B20 blend and 8% reductions while using B100 blend. Performance of microwave-enhanced WCO biodiesel in four-cylinder, four-stroke diesel engine is studied by Reefat [31]. Their results shows a slight increase in BSFC of biodiesel blends compared to conventional diesel. Rao et al. also reported the performance analysis of Used Cooking Oil Methyl Ester (UCOME) and its blends in a DI Compressed Ignition Engine [32].The results showed that there is slight increase in BSFC for UCOME and its blends, but BTE for UCOME blends was lower as compared to conventional diesel fuel by 2.5%. A higher Brake Thermal Specific Fuel Consumption (BSFC) was observed by Lapuerta et al. [33] when testing of commercial DI diesel engine was done using blends of WCO biodiesel and diesel fuel. With the increase in biodiesel concentration in blend, the BSFC increase but on the other hand the efficiency of the engine remains unchanged. Canakci et al. [34] with their test on diesel engine fuelled with waste frying palm oil biodiesel shows the significant increase in BSFC as there is increase in biodiesel percentage in blend whereas brake torques and BTE decreases slightly with the increase in amount of biodiesel in the fuel blend. Valente et al. [35] investigated the impact of fuel consumption on diesel power generator operating with biodiesel. The results showed increase in fuel consumption with higher biodiesel concentration in the fuel. Dwivedi G. et al. [1] studied the BSFC for Jatropha oil methyl ester (JOME). The results were found to be 14.8% higher than diesel. Also a higher BTE was recorded up to B30 in comparison to diesel while BTE of B100 (24%) was almost equals to diesel (24.5%).Engine performance with biodiesel and its blends with diesel fuel depend largely on the factors such as combustion, air turbulence, air–fuel ratio, injector pressure, actual start of combustion which can vary depending upon the quality and origin of biodiesel and engine operating parameters such as speed, load, operating temperature, etc. [36]. Hirkude J.B. and Padalkar Atul S. [37] through their tests showed that the BTE decreases slightly with the increase of Waste Fried Oil Methyl Ester (WFOME) in the blend. A BTE for B100 and B50 was 25.97% and 28.02%. The SFC increases with increase in concentration of WFOME in the blend. B50 gave BSFC of 0.31 kg/kW h while that of conventional diesel was 0.29 kg/kWh. Verma P. and Singh V. M. [38] investigated the performance of diesel engine fuelled with cotton seed biodiesel in which a higher BTE was recorded when the blend was preheated with B20, B40 and B60 and was 3.74%, 10.46%, and 3.27% more than that for diesel at full load.

V. CONCLUSION

This Paper is a complete review of the various methods of production and emphasis on the production parameters. In long run this paper will help the authors and researchers to get a

complete review of number of authors with their comparative study. Hereby from our deep and thorough study, we conclude that transesterification is the most eco-friendly and reasonable method for the production of biodiesel. Biodiesel properties unquestionably increase the efficiency of the diesel engine. Engine fuelled with biodiesel shows slight increase in BSFC with the increase in concentration whereas BTE decreases to some limit when operated at low rpm and low pressure conditions. Our study is confined to the performance parameters of CI engine which includes BSFC and BTE. In last few years there is a double-digit annual growth rate production capacity of biodiesel. In coming years it will be a challenge for researchers to use 100% biodiesel in CI engines for complete replacement of diesel fuel by biodiesel.

REFERENCES

[1] Dwivedi G., Jain S., Sharma M.P. Impact of Biodiesel and its Blends with Diesel and Methanol on Engine Performance. *International Journal of Energy Science;* Vol.1 No.2 2011 PP.105-109

[2] Dorado MP, Cruz F, Palomar JM, Lopez FJ.An approach to the economics of two vegetable oil-based bio-fuels in Spain. *Renew Energy* 2006; 31:1231–7.

[3] Demirbas A. Progress and recent trends in biodiesel fuels. Energy Conversion and Management 50 (2009); 14–34

[4] Demirbas A. New liquid biofuels from vegetable oils via catalytic pyrolysis. *Energy Educ Sci Technol* 2008; 21:1–59.

[5] Bozbas K.Biodiesel as an alternative motor fuel: production and policies in the EuropeanUnion.*RenewSustain Energy Rev 2008; 12:542 – 52.*

[6] Sarin A, Arora R, Singh N.P, Sarin R, Malhotra N.P, andSarin S. Blends of Biodiesels Synthesized from Non-edible and Edible Oils: Effects on the Cold Filter Plugging Point. *Energy Fuels* 2010, 24, 1996–2001*:* DOI: 10.1021/ef901131m

[7] Al-Zuhair S. Production of biodiesel: possibilities and challenges. *Biofuels Bioprod Bio* refin 2007; 1:57-66.

[8] Robles-Medina A, González-Moreno PA, Esteban-Cerdán L, Molina-Grima E. Biocatalysis: towards ever greener biodiesel production. *Biotechnol Adv*2005; 119:291–9.

[9] Ramadhas AS, Jayaraj S, Muraleedharan C. Use of vegetable oil as I.C. engine fuels-a review. *Renew Energy* 2004; 29:727–42.

[10] Wellert S, Karg M, Imhof H, SteppinA, Altmann HJ, Dolle M, et al. Structure of biodiesel based bi continuous micro emulsions for environmentally compatible decontamination: A small angle neutron scattering and freeze fracture electron microscopy study. *J Colloid Interface Sci* 2008; 352:250–8.

[11] Jesus AD, Silva MM, Vale MGR. The use of micro emulsion for determination of sodium and potassium in biodiesel by flame atomic absorption spectrometry. *Talanta* 2008; 74:1378–84.

[12] Pramanik K. Properties and use of Jatrophacurcas oil and diesel fuel blends in compression ignition engine. *Renew Energy* 2003; 28:239–48.

[13] Canakci M, Ozsezen AN, Arcaklioglu E, Erdil A. Prediction of performance and exhaust emissions of a diesel engine fueled with biodiesel produced from waste frying palm oil. *Expert SystAppl* 2009; 36:9268–80.

[14] Ma F, Hanna MA. Biodiesel production: a review. *Bio resour Technol* 1999; 70:1–15.

[15] Ramadhas AS, Jayaraj S, Rao KLN. Experimental investigation on non-edible vegetable oil operation in diesel engine for improved performance. *In:National conference on advances in mechanical engineering, J.N.T.U., Anantapur,* India; 2002.

[16] Darnoko D, Cheryan M. Kinetics of palm oil transesterification in a batch reactor. *J Am Oil ChemSoc* 2000; 77:1263–7.

[17] Pryor RW, Hanna MA, Schinstock, Bashford LL. Soybean oil fuel in a small diesel engine. *Transactions of the ASAE* 1983; 26:333–7.

[18] Strayer RC, Blake JA, Craig WK. Canola and high erucic rape seed oil as substitutes for diesel fuel: preliminary tests. *JAOCS* 1983; 60:1587–96.

[19] Hamasaki K, Kinoshita E, Tajima S, Takasaki K, Morita D. Combustion characteristics of diesel engines with waste vegetable oil methyl ester. *In: The 5th International Symposium on Diagnostics and Modelling of Combustion in Internal Combustion Engines;* 2001

[20] Mc Donnel KP, Ward SM, Mc Nully PB, Howard Hildige R. Results of engine and vehicle testing of semi refined rapeseed oil. *Transactions of the ASAE* 2000; 43:1309–16.

[21] Monyem A, Van Gerpen JH. The effect of biodiesel oxidation on engine performance and emissions. *Biomass and Bioenergy* 2001; 20:317–25.

[22] Makinen Mika LK, Niemi Seppo A. Performance and exhaust emissions of a tractor engine using mustard seed oil as fuel. *SAE Paper 970219*.

[23] Al-Widyan, MohammadI, TashtoushG,Abu-quadaisM. Utilization of ethyl ester of waste vegetable oil as fuel in diesel engines. *Fuel Processing Technology* 2002; 76:91–103.

[24] Bari S, Yu CW, Lim TH. Performance, deterioration and durability issues while running a diesel engine with crude palm oil. *Journal of Automobile Engineering*2002; 216:785–92.

[25] Kalligeros S, Zannikos F, Stournas S, Lois E, Anastopoulos G, Teas Ch, et al. An investigation of using biodiesel/marine diesel blends on the performance of a stationary diesel engine. *Biomass and Bioenergy* 2003; 24:141–9.

[26] Canakci M, Gerpen JH V. Comparison of engine performance and emissions for petroleum diesel fuel, yellow-grease biodiesel and soybean-oil biodiesel. *Trans ASAE* 2003; 46(4):937–44.

[27] Pramanik K. Properties and use of jatropha curcas oil and diesel fuel blends in compression ignition engine. *Renewable Energy* 2003; 28:239–48.

[28] O¨ zkan M, Ergenc¸ AT, Denı´z O. Experimental performance analysis of biodiesel, traditional diesel and biodiesel with glycerin. *Turk J Eng Environ Sci* 2005; 29:89–94.

[29] Ramadhas AS, Jayaraj S, Muraleedharan C. Characterization and effect of using rubber seed oil a fuel in the compression ignition engines. *Renewable Energy* 2005; 30:795–803.

[30] Murillo S, Mı´guez JL, Porteiro J, Granada E, Mora´n JC. Performance and exhaust emissions in the use of biodiesel in outboard diesel engines. *Fuel* 2007; 86:1765–71.

[31] Reefat AA, El Sheltawy ST, Sadek KU. Optimum reaction time, performance and exhaust emission of biodiesel produced by microwave irradiation. *Int J Environ SciTechnol* 2008; 5(3):315–22.

[32] Rao GLN, Sampath S, Rajagopal K. Experimental studies on the combustion and emission characteristics of a diesel engine fuelled with used cooking oil methyl ester and its diesel blends. *Int J Appl Sci Eng Technol* 2008; 64–70.

[33] Lapuerta M, Herreros JM, Lyons LL, Garcı´a-Contreras R, Bricen˘o Y. Effect of the alcohol type used in the production of waste cooking oil biodiesel on diesel performance and emissions. *Fuel* 2008; 87:3161–9.

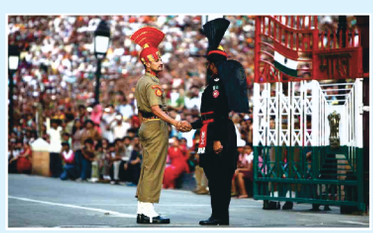
[34] Canakci M, Ozsezen AN, Arcaklioglu E, Erdil A. Prediction of performance and exhaust emissions of a diesel engine fuelled with biodiesel produced from waste frying palm oil. *Expert Sys Appl* 2009; 36:9268–80.

[35] Valente OS, da Silva MJ, Pasa VMD, Rodrigues C, Belchior P, Sodre JR. Fuel consumption and emissions from a diesel power generator fuelled with castor oil and soybean biodiesel. *Fuel* 2010; 89:3637–42.

[36] Fazal MA, Haseeb.ASMA, MasjukiHH, Biodiesel feasibility study: an evaluation of material compatibility; performance; emission and engine durability. *Renewable and Sustainable Energy Reviews* 2011; 15(2):1314–24.

[37] Hirkude J. B., Padalkar A. S., Performance and emission analysis of a compression ignition Engine operated on waste fried oil methyl esters. *Applied Energy* 90 (2012) 68–72.

[38] Verma P., Singh V. M., Assessment of Diesel Engine performance using Cotton Seed Biodiesel. *Integr. Res. Adv.* 2014, 1(1), 1-4



ORACLE | WORKFORCE DEVELOPMENT PROGRAM

SEDULITY™ Solutions & Technologies®

D-LINK INSTITUTE

VMM Education

ISBN 978-81-924867-3-4