A Performance Comparison of Routing Protocols(DSR and TORA) for Security Issue In MANET(Mobile Ad Hoc Networks)

Rakesh Kumar Jha
Department of Electronics and Communication Engineering,
SVNIT Surat, INDIA

Suresh V. Limkar
Department of Computer Engineering,
(Faculty at G.H.Raisoni College of Engg & Mgt Pune)
SVNIT Surat, INDIA

Dr. Upena D. Dalal
Department of Electronics and Communication Engineering,
SVNIT Surat, INDIA

ABSTRACT

Mobile Ad-hoc Networks (MANETs) allow wireless nodes to form a network without requiring a fixed Infrastructure.Dynamic Source Routing (DSR) for mobile Ad Hoc network. It is a reactive source routing protocol for mobile IP network. Temporally-Ordered Routing Algorithm (TORA) routing protocol is for mobile ad hoc networks. It can be made to operate in both reactive and proactive modes. It uses IMEP for link status and neighbor Connectivity sensing. Internet MANET Encapsulation Protocol (IMEP) is used for link status and neighbor connectivity sensing. It is used by the TORA routing protocol. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We present and examine analytical simulation results for the routing protocols DSR and TORA network performance, using the well known network simulator OPNET 10. 0

Keywords- Mobile Ad Hoc Networks, Security, DSR, TORA, SIP-Proxy

I. INTRODUCTION

Security has become a primary concern in order to provide protected communication in Wireless as well as wired environment. In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment.

Although security has long been an active research topic in wire line networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. Table 1 describes the security issues in each layer. In this article we consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. In other words, we seek to protect the network connectivity between mobile nodes over potentially multihop wireless channels, which is the basis to support any network security services. Multihop connectivity is provided in MANETs through two steps: (1) ensuring one-hop connectivity through link-layer protocols (e.g., wireless medium access control, MAC); and (2) extending connectivity to multiple hops through network layer routing and data forwarding protocols (e.g., ad hoc routing). Accordingly, we focus on the link- and network-layer security issues, challenges, and solutions in MANETs in this article. One distinguishing characteristic of MANETs from the security design perspective is the lack of a clear line of defense.

Table.1: The security solutions for MANETs should provide complete protection spanning the entire protocol stack.

Layer	Security issue
Application Layer	Detecting And Preventing Viruses, Worms, Malicious Codes, And Application Abuses.
Transport Layer	Authentication And Securing End-To-End Communications Through Data Encryption.
Network layer	Protecting The Ad Hoc Routing And Forwarding Protocols.
Link Layer	Protecting The Wireless Mac Protocol And Providing Link- Layer Security Support
Physical Layer	Preventing Signal Jamming Denial-Of-Service Attacks.

Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. There are basically two approaches to protecting

MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques in contrast, the reactive approach seeks to detect security threats a posteriori and react accordingly. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both approaches and encompass all three components: prevention, detection, and reaction.

Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. There are basically two approaches to protecting MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques in contrast, the reactive approach seeks to detect security threats a posteriori and react accordingly. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both approaches and encompass all three components: prevention, detection, and reaction. For example, the proactive approach can be used to ensure the correctness of routing states, while the reactive approach can be used to protect packet forwarding operations. As argued in, security is a chain, and it is only as secure as the weakest link. Missing a single component may significantly degrade the strength of the overall security solution.

Different routing protocols are suitable for different network characteristics. DSR routing protocol, for example, performs well when the proxy disabled on the Node As the Proxy enabled on the node it performance degrades. However, TORA routing protocol is well suited for proxy enabled Node too. An analytical performance comparison of some of the most important algorithms is presented, like Dynamic Source Routing (DSR) [1], [2] and Temporary Ordered Routing Algorithm (TORA) [3], [4]. DSR is the main and most known protocol of the reactive family of protocols while TORA uses a unique approach in hop-by-hop routing, guiding every packet to its destination.

We compare the security issue in TORA and DSR by using SIP Proxy Enabled at client. [OPNET] allows comparing both at a same time by using different scenarios. All protocols are provided with identical traffic load and mobility patterns and considered TCP as transport protocol and FTP as traffic generator. He performance metrics evaluated include bandwidth efficiency for control and data, as well as end-to-end message packet delay and throughput.

We test the performance of both DSR and TORA concurrently in the same network. The objective is Create the four Scenarios two for DSR and two for TORA like DSR without Proxy DSR with Proxy.

The paper is divided as follows: section 2 Basic information on the routing protocols chosen for the experiment. Section 3 and 4 present the design, implementation and testing results. Section 5 concludes this Paper.

II. BASIC INFORMATION

In general, routing protocols are classified into two main categories: Table-driven routing protocols and source initiated on-demand driven routing protocols. The table driven routing protocols maintain consistent and up-to-date routing information from each node to the rest of the nodes in the network in one or more routing tables regardless of the need of such routes.

The source initiated on-demand routing protocols are developed and employed in mobile ad-hoc networks and initiates routing activities only when needed. DSR [Johnson, Maltz and Broch, 2001; Johnson, Maltz and Hu, 2004; Johnson and Maltz, 1996; Broch, Johnson and Maltz, 1998] and TORA [Park and Corson, 1997; Park and Corson, 2000] routing protocols are two examples of such routing protocols.

They maintain at least one route to destination in their routing tables but initiate the first search for such route only when the source wants to send data packets to the destination node. "Listen before talk". For low collision probability it uses binary exponential back off mechanism.

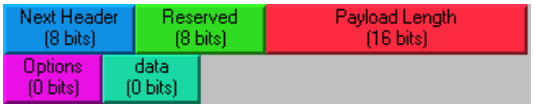
A. Dianamic source routing(DSR)

The Dynamic Source Routing protocol is composed of two main mechanisms to allow the discovery and maintenance of source routes in the ad hoc networks.

Route Discovery: is the mechanism by which a Source node wishing to send a packet to a destination node, obtains a source route to the destination. Route Discovery is used only when the source node attempts to send a packet to a destination and does not already know a route to that destination.

Route Maintenance: is the mechanism by which a node wishing to send a packet to a destination is able to detect, while using a source route to the destination, if the network topology has changed. If this is the case then it must no longer use this route to the destination because a link along the route broken. Route Maintenance for this route is used only when the source node is actually sending packets to the destination.

To limit the need for route discovery, DSR allows nodes to operate their network interfaces in promiscuous mode and snoop all (including data) packets sent by their neighbors. Since complete paths are indicated in data packets, snooping can be very helpful in keeping the paths in the route cache updated. To further reduce the cost of route discovery, the RREQs are initially broadcasted to neighbors only (zero-ring search), and then to the entire network if no reply is received. Another optimization feasible with DSR is the gratuitous route replies; when a node overhears a packet containing its address in the unused portion of the path in the packet header; it sends the shorter path information to the source of the packet (Automatic Route Shortening).



Packet format: DSR

Another important optimization includes the technique to prevent "Route replies Storms": because many route replies may be initiated simultaneously a delay time proportional to the hop's-distance can be used in order to give higher priority to near nodes. In addition a method called "Packet Salvaging" is often used in DSR.

When an intermediate node forwarding a packet detects through Route Maintenance that the next hop along the route for that packet is

broken, if the node has another route to the packets' destination it uses it to send the packet rather than discard it.

We provide the basic characteristics of the Dynamic Source Routing (DSR):

- Uses source routing
- Provides loop-free routes
- Supports unidirectional links and asymmetric routes
- With the optimizations available it is a good choice for an ad hoc network

B. Temporally-Ordered Routing Algorithm (TORA)

The Temporally-Ordered Routing Algorithm (TORA) is a distributed routing protocol for multihop networks with a unique approach for routing the packets to their destination.

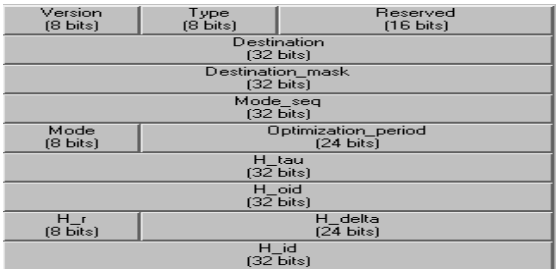


Figure 1. Packet format: TORA

TORA is fully distributed, in that routers need only maintain information about adjacent routers (i.e.one hop knowledge) and there is no centralized control. This is essential for all Ad Hoc routing protocols. Like a distance-vector routing approach, TORA maintains state on a per-destination basis. However, it does not continuously execute shortest-path computation and thus the metric used to establish the routing structure does not represent a distance. The destination-oriented nature of the routing structure in TORA supports a mix of reactive and proactive routing on a per-destination basis. During reactive operation, sources initiate the establishment of routes to a given destination on demand. This mode of operation may be advantageous in dynamic networks with relatively sparse traffic patterns since it may not be necessary or desirable to maintain routes between every source/destination pair at all times.

At the same time, selected destinations can initiate proactive operation, resembling traditional table-driven routing approaches. This allows routes to be proactively maintained to destinations for which routing is consistently or frequently required (e.g., servers or gateways to hardwired infrastructure).

TORA is designed to minimize the communication overhead associated with adapting to network topological changes. The scope of TORA's control messaging is typically localized to a very small set of nodes near a topological change. A secondary mechanism, which is independent of network topology dynamics, is used as a means of route optimization and soft-state route verification. The design and flexibility of TORA allow its operation to be biased towards high reactivity (i.e., low time complexity) and bandwidth conservation (i.e., low communication complexity) rather than routing optimality--making it potentially well-suited for use in dynamic wireless networks.

So TORA is offering following characteristics

- Distributed execution
- Loop-free routing
- Multi-path routing
- Reactive or proactive route establishment and maintenance
- Minimization of communication overhead via localization of algorithmic reaction to topological changes

III. SIMULATION MODEL DESIGN AND IMPLEMENTATION

A design goal was to analyze the performance and security compression of DSR and TORA routing protocols. The performance was based on the measurement of the following parameters: Throughput (bits per second), media access delay (sec), Traffic sent (Bytes/sec). The performance analyses between DSR and TORA routing protocols was accomplished using the Optimized Network Engineering Tool simulation environment [OPNET]. The size of data packet for FTP was calculated using a Constant (1024) function the buffer size of the LAN parameter 256000 (Bits). Nodes communicate over wireless links with a transmission range of 1500 meters with a transmission power of 0.001W. The MANET traffic generator starting time was Constant 0(sec) and the duration period Constant 10(sec). Also the data rate was 1 Mbps. Strict match criteria used in channel. Number of Repetition calculated Constant 3 Each simulation was 3600 seconds in length. DSR Route expiry was 300 seconds. DSR Request table size of route discovery was 64 nodes. DSR Maximum request retransmission of route discovery was 16 retransmissions. DSR Broadcast jitter of route discovery was calculated using a uniform [0, 0.01] seconds function. Finally, TORA IP packet discard timeout was 10 seconds.

Table 2: Simulation Parameters

Parameter	**Value**
Size of data packet for FTP	1024
Buffer size of LAN	256000 (Bits).
Transmission range	1500(Metter).
Transmission power	0.001(Watt)
Data rate	1(Mbps)
Simulation time	3600(Second)

The network has 50 fixed wireless workstations placed as shown in figure 2. In this research, work four different scenarios were considered.

1. All the stations in this scenario generating Ad-Hoc Routing Parameter on the base of DSR Protocol.

2. All the stations in this scenario generating Ad-Hoc Routing Parameter on the base of TORA Protocol.
3. All the stations in this scenario generating Ad-Hoc Routing Parameter on the base of TORA Protocol. And station node 5,7,12,17,23,38 with SIP proxy enabled.
4. All the stations in this scenario generating Ad-Hoc Routing Parameter on the base of DSR Protocol. And station node 5,7,12,17,23,38 with SIP proxy enabled.

A. Model description

Figure 3: Simulation Network Model consists with 50 fixed wireless work stations. Node 24 is source node Node 18 is destination node. Node No.5, 7, 12,17,23,38 set with SIP proxy enabled (Circle_wkst).In our research MANET Used the Rx Group Config node is added to speed up the simulation. Rx Group Config also helped regarding to avoid the effect of simulation more than specified result i.e they simulate here only up to 1500 meters. Since OPNET MODELER have a very good features for we can simulate more than one scenario at a same time. I am giving some concept regarding the scenario.

Step 1: Since here we are comparing different scenario so create one full scenario.

Step 2: Apply above mentioned parameter to the entire scenario is same.

Step 3: Create different Scenario with duplicate scenario and changes in according to applying concept.

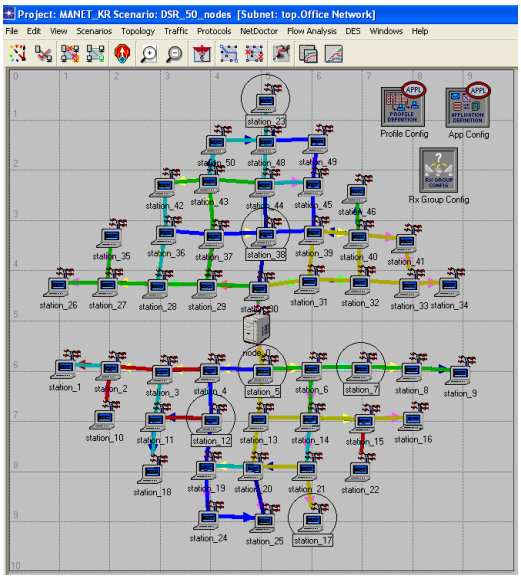


Figure 2. Simulation Network Model .50 fixed wireless work station. Node 24 is source node Node 18 is destination node. Node No.5, 7, 12,17,23,38 set with SIP proxy enabled (Circle_wkst)

It is configured to eliminate all receivers that are over 1500 meters away. This network shows a 50 node DSR and TORA network. All nodes in the network are configured to run DSR and TORA multiple FTP sessions.

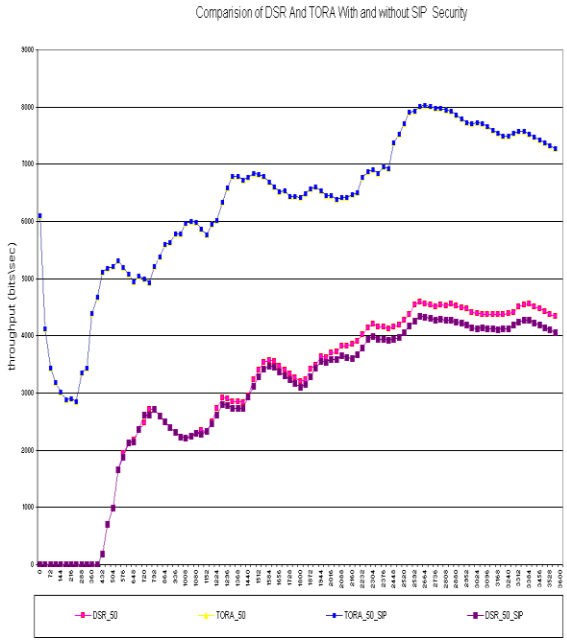


Figure 3. Comparision of average throughput of different scenario in DSR and TORA with and without proxy.

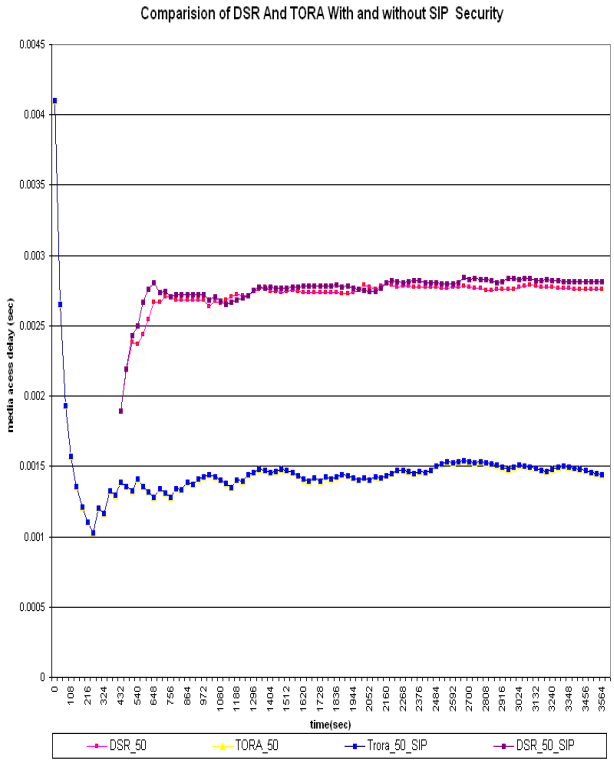


Figure 4. Comparision of average Media access delay of different scenario in DSR and TORA with and without proxy.

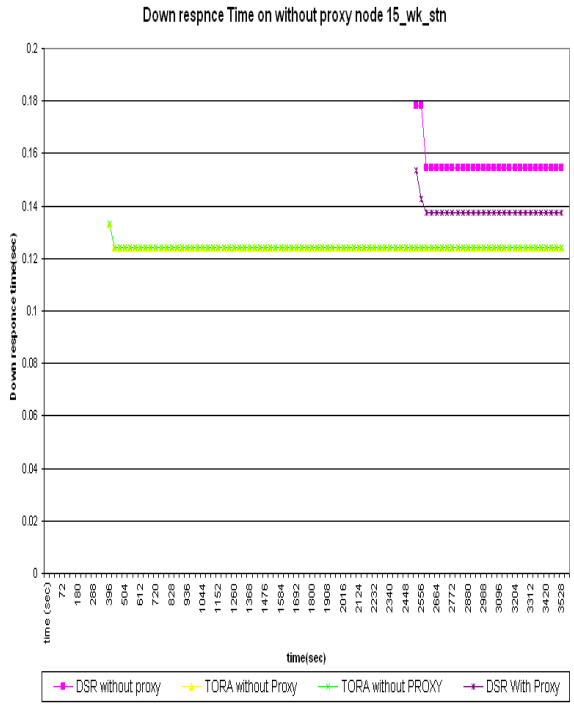


Figure 5. Comparasion of average Down Load Response at node 15(without proxy enabled) for both case DSR and TORA.

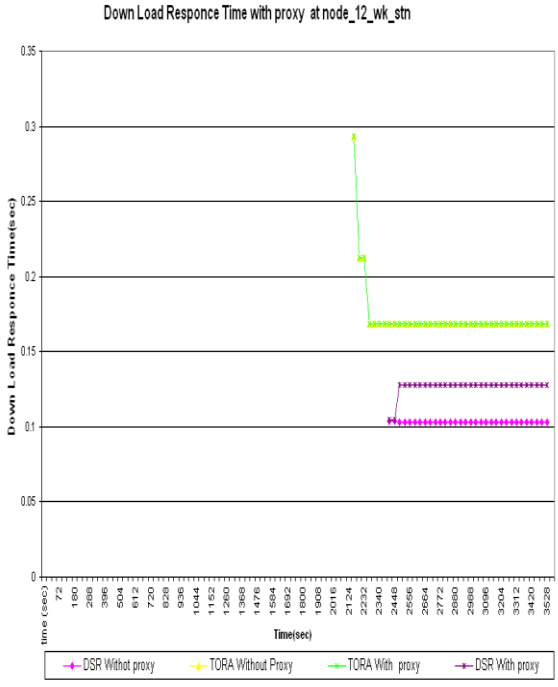


Figure 6. Comparision of average Down Load Response at node 12(With Proxy Enabled) for both case DSR and TORA.

IV. RESULT ANALYSIS

A. Throughput (bits/sec)

Figure 4: Compression of average throughput of different scenario in DSR and TORA with and without proxy. The throughput of TORA is Greater than DSR in both case Normal case and Proxy Enable case. This figure shows that DSR is less secure than TORA routing because in case of DSR proxy enabled condition the throughput is higher than normal or secure (Without proxy enabled).In case of TORA the throughput is constant in both case (with and without proxy) so we judge that from result TORA is more secure than DSR.

B. Media access delay (sec)

Figure 5: Compression of average Media access delay of different scenario in DSR and TORA with and without proxy. The Graph shows that Total time (in seconds) that the packet is in the higher layer queue, from arrival to the point when it is removed from the queue for transmission in case of DSR with Proxy Enabled is higher in all case with DSR without proxy enabled and both condition of TORA (With and Without proxy).Since in case of TORA Media access delay is lowest because it not effected by proxy as well as normal condition.

C. Down Load response time (sec)

Figure 6: Compression of average Down Load Response at node 15(without proxy enabled) for both case DSR and TORA.This result shows that when we consider those Node whose SIP proxy disabled EX. Node 15.Then down load response time in TORA is lower than DSR.In case of DSR Down load response with proxy is lower than without proxy because we seen the result for without proxy node Work station. We also observe that here down load response time decreases from high to low value in both case DSR and TORA.

D. Down Load response time (sec)

Figure 7: Compression of average Down Load Response at node 12(With Proxy Enabled) for both case DSR and TORA. This result shows that when we consider that Node whose SIP proxy enabled EX. Node 12. Then down load response time is in TORA is higher than DSR. In case of DSR Down load response with proxy is higher than without proxy because we seen the result for with proxy node Work station. We also observe that here down load response time decreases from high to low value in both case but in case of DSR with proxy it increases from lower value to higher value but when proxy disabled it remains constant.

V. CONCLUSION

Concurrent routing of both DSR and TORA routing protocols in the same network have been evaluated for security issue. Nodes are divided into two ways without proxy enabled and proxy disabled Node work station. TORA is better suited for both cases in without and with security purpose for 50 fixed node work station environment. We conclude that proxy environment is suitable for TORA Routing because the network will maintain the same behavior after proxy enabled too but DSR routing is highly affected by proxy. Finally, future work in this area will examine the effect of algorithm use for DSR Routing so that it can also use in case of Proxy.

REFERENCES

[1] D. Johnson, D. Maltz and Yih-Chun Hu. "The Dynamic Source Routing Protocol for Mobile Ad HocNetworks,"http://www.ietf.org/internet-drafts/draftietfmanet-DSR-09.txt,IETF Internet draft, Apr. 2003.

[2] David B. Johnson and David A. Maltz. "Dynamic source routing for ad hoc wireless networks". In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153-181. Kluwer Academic Publishers, 1996.

[3] Vincent D. Park and M. Scott Corson. "Temporally-Ordered Routing Algorithm (TORA) version 4: Functional specification". Internet-Draft, draft-ietfmanet-TORA-spec-04.txt, July 2001.

[4] Vincent D. Park and M. Scott Corson. "A performance Comparison of TORA and Ideal Link State routing." In Proceedings of IEEE Symposium on Computers and Communication '98, June 1998.

[5] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," in The Sixth Annual ACM/IEEE Conference on Mobile Computing and Networking, Boston, MA, USA, Aug. 2000.

[6] Rakesh Kumar Jha and Dr Upena Dalal "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)" International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE Xplore,kerela,March 2010.

[7] Yi Wang et.al, "Cluster based Location - Aware routing Protocol for Large Scale Heterogeneous MANET", in Proceeding of the Second International Multi symposium on Computer and Computational Sciences, IEEE Computer Society, 2007, pp.366-373.

[8] S. Ahmed and M. S. Alam, "Performance Evaluation of Important Ad-hoc Nnetwork Protocols",Proceedings of EURASIP Journal on Wireless Communications and Networking Volume 2006, Issue 2 (April 2006), pp- 42 – 42

[9] Mohammed Bouhorma, H. Bentaouit and A.BoudhirA "Performance Comparasion of ad-hoc routing protocols AODV and DSR" , Multimedia Computing and Systems, 2009. ICMCS '09. International Conference on,pages 511-514,April 2009

Mr. Jha Rakesh presently is full time Research Scholar at S. V. National Institute of Technology, Surat, INDIA. He has completed his B.Tech. (Hons in Electronics) from Bhopal and obtained M.Tech. (Wireless Communications) from NIT, Jalandhar, India.He have done live project in development and support both in Industries also.

He has published many conferences and journal papers at national and international level including Scientific Research Journal. His one concept related to Router of Wireless Communication is accepted by ITU (International Telecommunication Union).He is now pursuing PhD in S. V. National Institute of Technology, Surat, INDIA. Surat. His research interest's area is Wireless and Optical Communication. Currently he is doing his research work in WiMAX and its Security issues. He is working on OPNET simulation and NS2 tools for Wireless Communication. Free to contact: jharakesh.45@gmail.com, https://sites.google.com/site/jharakeshnetworkcom/

Dr. (Mrs.) U. D. Dalal presently working as Associate Professor in Electronics Engineering Department of S. V. National Institute of Technology, Surat, INDIA. She has 18 years of academic experience. She completed her B.E. (Electronics) from SVRCET, Surat in 1991 and obtained M.E. (Electronics & Communications) from DDIT, Gujarat with Gold Medal. She is also awarded with 5th N.V. Gadadhar memorial Award by IETE. She has published many conference and journal papers at national and international level. She has guided many UG and PG projects, dissertations and seminars in the area of advance communication systems. She has completed Ph.D. in 2009 and guides 5 research scholars presently. Her book on "Wireless Communication" is published by Oxford University Press in July 2009. One more book edited by her and Dr Y P Kosta titled "WiMAX New Developments" is published by Inteh, Vienna, Austria. She is honored by "Rashtriya Gaurav Award" by India International Friendship Society. Recently she is received Best Technical Woman award by Divyabhaskar.