ISSN:0975-9646

Dual Digest Symmetric Key Security Scheme for AODV in MANET

Gandhi Krunal A.
[1] *Information Technology, Parul Institute of Technology,*
Vadodara, Gujarat, India

Patel Tejal K.
[2] *Assistant Professor, Information Technology, Parul Institute of Technology,*
Vadodara, Gujarat, India

***Abstract*—Mobile Ad hoc Network's because of maliciousness that intentionally disrupts the network by using variety of attacks and due to routing protocols (e.g. AODV), which were already developed without considering security features to prevent the various kinds of attacks. And also there is infrastructure less environment, and having open peer-to-peer architecture, shared wireless medium and dynamic topology, MANETs are frequently established in insecure environments like disaster sites and military applications. The AODV routing protocol was initially developed without considering security in mind. So it is not able to defend against any kind of security attack. But there are many security schemes available that make AODV secure. However, by doing more research in this area, one major flaw in any of the existing secure routing protocols was discovered. That is security schemes that are available consume more processing power and required complex key-management system. In this work I am going to present a novel security scheme which integrates dual digest mechanism with symmetric key distribution security scheme to protect the AODV routing protocol that is capable of defending itself against both malicious and unauthenticated nodes. The proposed security scheme will also be simulated in the Network Simulator 2.**

***Keywords:* MANET, AODV, Symmetric Key Distributor, Dual Digest.**

I. INTRODUCTION

Wireless networking is a rising technology that allows users to access information and services, without considering their geographic position. The usage of wireless communication between mobile users becomes very popular due to recent advancements in computer and wireless technologies. It provides the service at really low cost and high data rates, which are the two main reasons why mobile computing is making impact on the current environment.

There are two interesting approaches for establishing wireless communications between mobile hosts. According to first approach, use a fixed network infrastructure that has wireless access points. In this kind of network, a mobile host communicates with the network through an access point within its coverage radius. When it comes out of range of one access point, it connects with a new access point within its range and starts communication through it. The second approach is to build a wireless ad hoc network among users demanding to communicate with each other with no reestablished infrastructure, which is the focus of this thesis research. [6]A Mobile Ad Hoc Network (MANET) is a set of mobile nodes that perform basic networking functions like packet forwarding, routing, and service discovery without the need of an established infrastructure. All the nodes in the ad hoc network depend on each another for forwarding a packet which is send by the source node to the destination node, due to the limited transmission range of each mobile node's wireless transmission. There is no centralized administration in ad hoc network.It guarantees that the network will not stop functioning just because one of the mobile nodes moves out of the range of the others. Every node should be able to enter and leave the network.

II. RELATED WORK

[1] There are many attacks in the AODV protocol which caused the damaged to the AODV. The researchers also provide the secure version of the AODV protocol which is SAODV (Secure AODV) which will ensure the integrity and authenticity of the data. Therefore, sender node generate a routing message signs it with its private key, and the destination node that receive this message verify the signature using the sender's public key. Still SAODV has some issues, which is solved by the A-SAODV protocol (Adaptive SAODV) protocol. [2] AODV and SAODV protocols are used to illustrate the scope of security vulnerabilities in MANET protocols. AODV uses unauthenticated routing control message and has no mechanism for dealing with malicious manipulation of these messages. We then use the vulnerability profile of SAODV to examine proposed extensions that seek to combat these vulnerabilities. Possible attacks by both insider nodes and un-authenticated nodes are identified. The researchers have proposed two methods to monitor the nodes which drop the routing packets. [3] The double digital signature encryption mechanism that improve the security and performance in AODV. This mechanism calculates signature using appropriate encryption algorithm for all the fields of an AODV message. It also calculates signature with secret key and then both signatures will be transmitted along with the AODV messages. But the overhead is too high because of the digital signature is used. [4] There are various attacks of the MANET and different mechanism that have been used to prevent the attacks. There are different mechanisms using various cryptographic techniques to provide security against the routing attacks against MANET. But there are some issues are still there, which can be harmful to the MANET.

So, my proposed mechanism used double digest which will provide the security against the attacks of the AODV and SAODV, it will provide better performance from these protocols.

III. PROPOSED WORK

The Proposed mechanism will improve the security against the attacks of AODV. This mechanism uses the symmetric key distribution, which broadcast the key over the network. All the nodes in the network will receive the key. After that the following steps tell us that the how different node will work with this mechanism.

A. Sender Node Algorithm

After receiving the symmetric key from the distributor the sender will append the RREQ packet with the SHA (Secure Hash Algorithm) which will produce the digest 1. After generation of digest 1, the key will append with it and again passes through the SHA. Now this time it will generate digest 2. Then this digest 2 will append with the RREQ packet and flood in the network, and wait for the RREP.

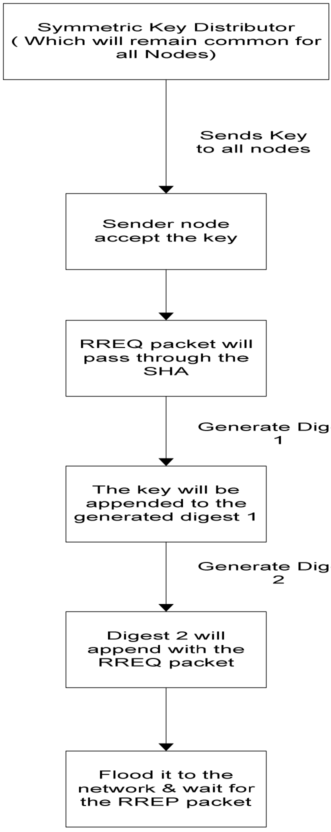

Symmetric Key Distributor (Which will remain common for all Nodes)
Sends Key to all nodes
Sender node accept the key
RREQ packet will pass through the SHA
Generate Digest 1
The key will be appended to the generated digest 1
Generate Digest 2
Digest 2 will append with the RREQ packet
Flood it to the network & wait for the RREP packet

Fig.1 Sender node algorithm.

B. Intermediate Node Algorithm

After receiving the RREQ packet with the digest 2 from the sender node, the intermediate node will follow the same procedure, until the generation of digest 1.And at the end of the generation of digest 1; it will compare it with the received one and the digest 1 of the generated one. If it matches then, it will forward the packet to the next node, else discard the packet. While forwarding, it will check that the next node is the destination node then it will forward it or the whole procedure will be continued until the destination node is found.

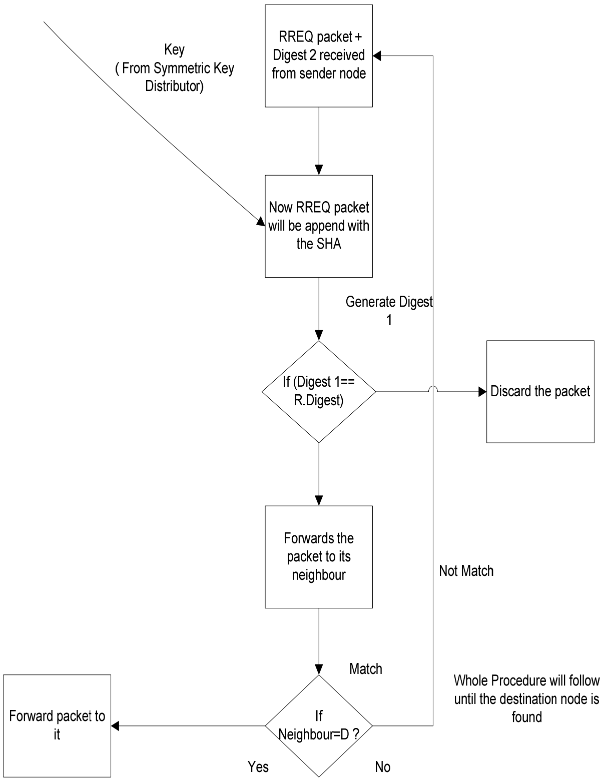

Key (From Symmetric Key Distributor)
RREQ packet + Digest 2 received from sender node
Now RREQ packet will be append with the SHA
Generate Digest 1
If (Digest 1== R.Digest)
Discard the packet
Forwards the packet to its neighbour
Not Match
Match
Whole Procedure will follow until the destination node is found
Forward packet to it
If Neighbour=D ?
Yes
No

Fig.2 Intermediate node algorithm.

C. Destination Node Algorithm

After receiving the RREQ packet with the digest 2 from the intermediate node, the destination node will follow the same procedure of the generation of digest as intermediate node. And at the end of the generation of digest 2, it will compare it with the digest 2 of the received one and the digest 2 of the generated one. If it matches then, it will send the RREP packet towards the sender node, else it will discard the packet.

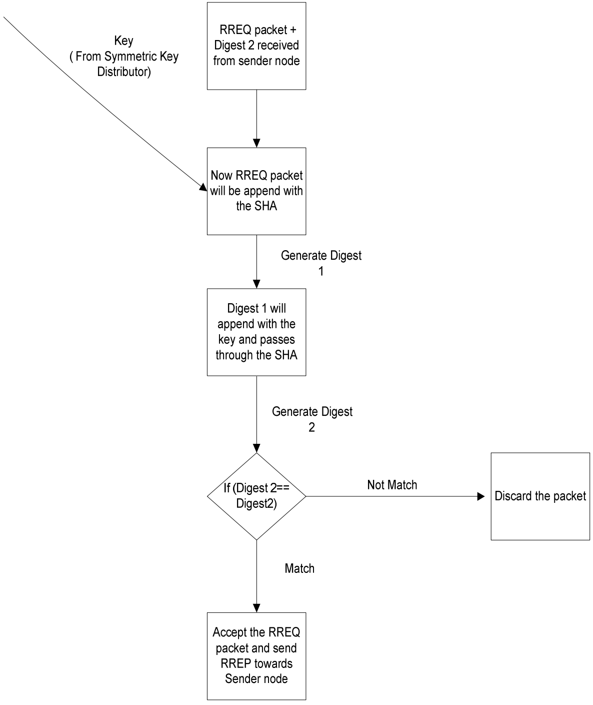

Key (From Symmetric Key Distributor)
RREQ packet + Digest 2 received from sender node
Now RREQ packet will be append with the SHA
Generate Digest 1
Digest 1 will append with the key and passes through the SHA
Generate Digest 2
If (Digest 2== Digest2)
Not Match
Discard the packet
Match
Accept the RREQ packet and send RREP towards Sender node

Fig.3 Destination node algorithm.

Table 1 General Simulation Parameters

Parameter	Value
MANET Area	1500*300 sq.m.
Total number of nodes	10,30,60
Node speed	0 up to 20 m/s
Application	Constant bit rate
Number of generated packets	10000 packets per CBR
Size of packets	512 bytes
Simulation Time	300 Sec

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83 GHz machine using Ubuntu 12.0.4 with 2 GB RAM and the network simulator NS2 version NS- 2.34. The choice of this simulation package in specific is due to the various reasons. The whole network consist of 50 mobile nodes with the space of 1500*300 square meters. Propagation style is Two Ray Ground, 32 Antenna type is Omni Antenna. As for the MAC layer communication, the IEEE 802.11 is used. Total simulation time is 300 seconds. The above table shows the values that were used in performed simulations.

IV. RESULT AND ANALYSIS

After implementation of successful proposed secure AODV, There were two different situations to be highly regarded. First is without attack situation and second is with attack situation. Total three times the simulation was ran and three different trace files were generated. With the use of AWK scripts the three different trace files were analyzed.

A .Data Traffic Comparison

In order to measure packet delivery fraction, it is necessary to count the total number of sent, received and routed packets. Following graph shows the total number of sent, received and routed packets for simulation environment.

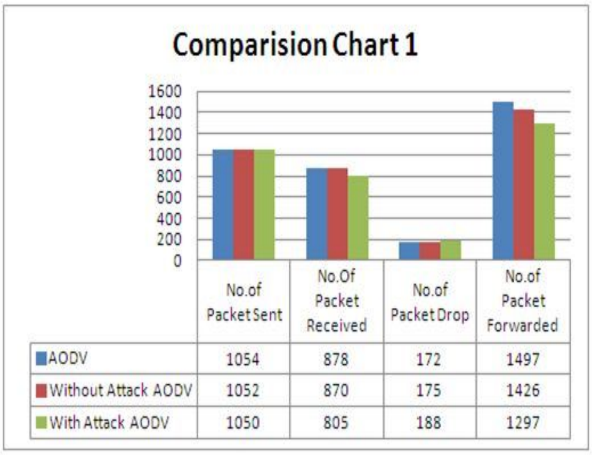
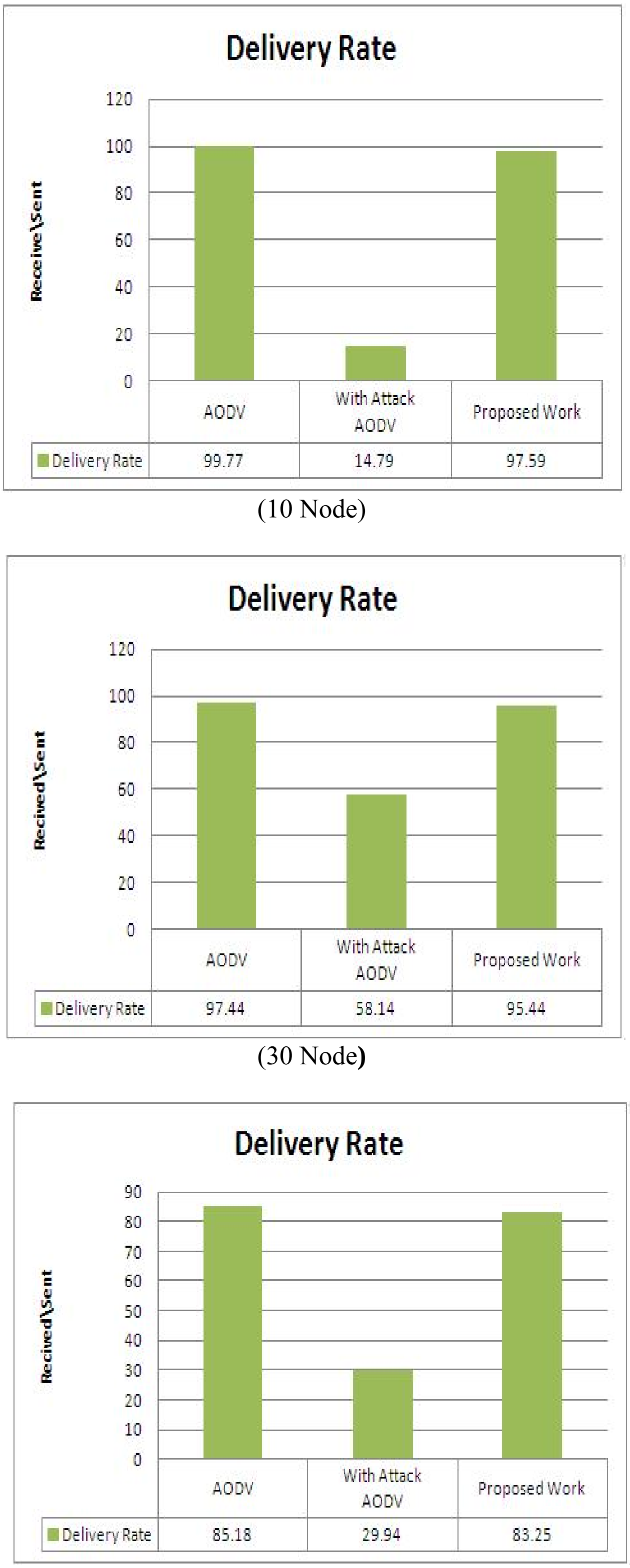


Fig 4 Data Traffic (CBR) Comparison

B .Data Traffic Delivery Rate

Delivery rate for each protocol can be counted by calculating Received/Sent Packets. Below graph shows delivery rate: From the below figure it can be concluded that in case of proposed AODV without attack the delivery rate is decreasing marginally, which is a good indication.



(10 Node)

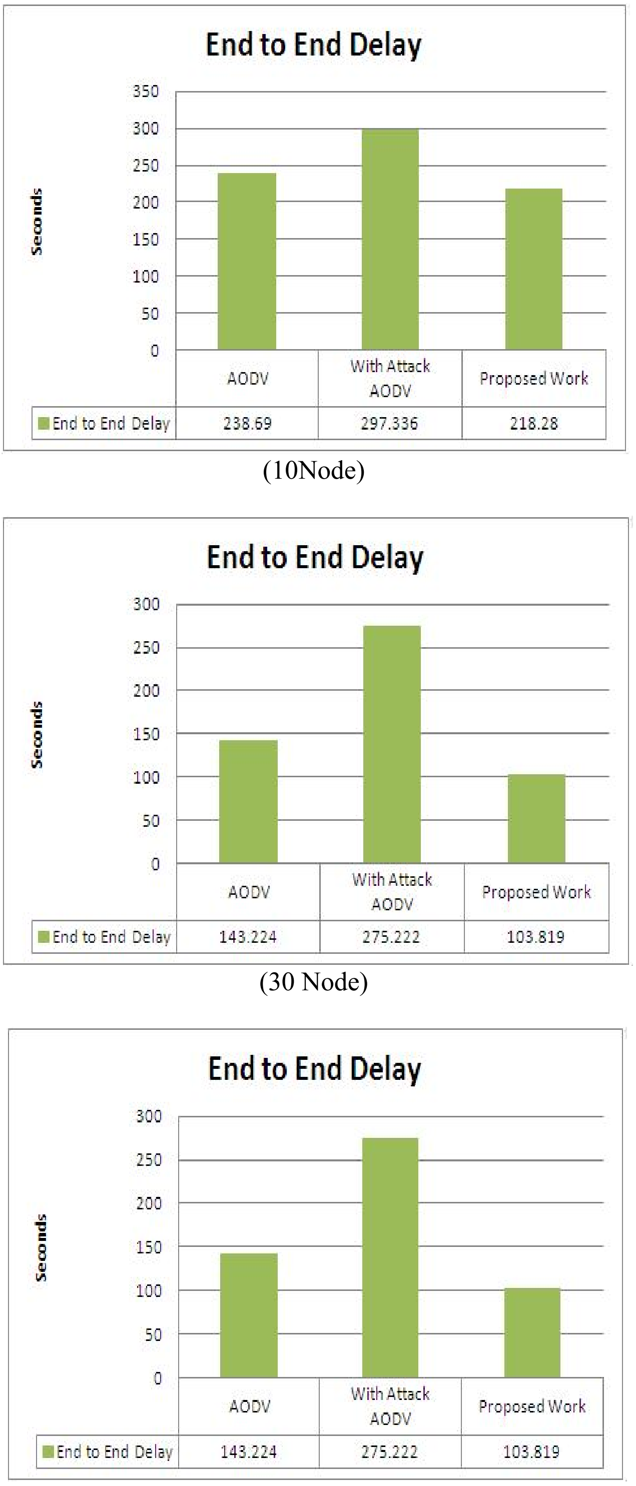
(30 Node)

(60 Node)

Fig 5 Data Traffic (CBR) Delivery Rate

C .Average End-to-End Delay

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. In this experiment, the average end-to-end delay is being measured for the Normal AODV, Proposed AODV and AODV with attack.



(10Node)

(30 Node)

(60 Node)

Fig 6 Average End to End Delay

.

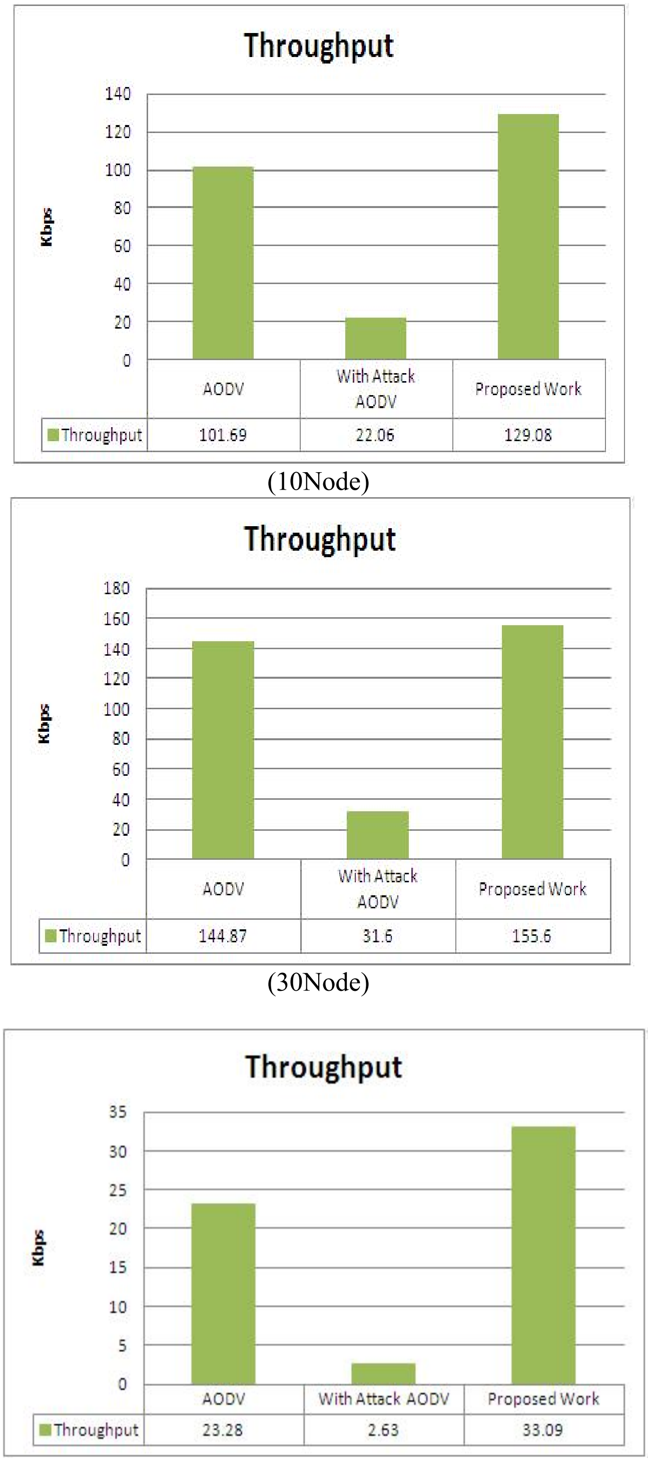
D .Average Throughput

It is defined as the total number of packets delivered over the total simulation time.

Mathematically it is defined as,

Throughput= N/1000

Where N is the number of bits successfully received by all destination node.



(10Node)

(30Node)

(60Node)

Fig 7 Average Throughput

V. CONCLUSION

There is rapid grow and change in the field of MANETs. While there are still many challenges that need to be met, it is likely that such networks will observe widespread and extensive use within the next few years. One of these challenges is security. Security of mobile ad hoc networks has recently gained momentum in the research community. Security solutions for MANET have to cope with a challenging environment including limited energy and computational resources. To my knowledge, there is no previously published work on detecting and defending against malicious and unauthenticated nodes together in the field of MANETs' routing protocols using double digest symmetric key distribution based algorithm.

With the above charts of the different parameters, we can see that there are improvements and network can still able to deliver the packets though there is the attack in the network. There are degradation in the parameters because of security inclusion in the protocol.

In future, we will further propose some ideas that can be integrated to the proposed scheme and they are presented as follows: This mechanism can also be used to secure other routing protocols like DSR, DSDV, TORA etc. Even the performance factor improvement of other protocols by optimization between different layers is in line up.

REFERENCES

[1] Davide Cerri and Alessandro Ghioni, CEFRIEL — Politecnico di Milano, "Securing AODV- The A-SAODV Secure Routing Prototype", IEEE 2008

[2] Jan Van Mulert, Ian Welch, Winston K.G.Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", JNCA(Elsevier 2012)

[3] Mr. Bhaumik A. Patel, "Improvement in Routing for MANET using Double Signature Security Scheme." Paripex-IJR 2013

[4] Jayashree.A.Patil, Nandini Sidnal, "Survey - Secure Routing Protocols of MANETs" IJAIS, FCS, New York, USA, Vol. 5– No.4, March 2013

[5] Carlos T. Calafate†, P. Pablo Garrido‡, José Oliver†, Manuel P. Malumbre "Mobile ad hoc networks", 2000.

[6] Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," New Orleans, LA, Feb. 1999, pp. 90–100.

[7] M. Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," Proc. 1st ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[8] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc on-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[9] Irshad, A.; Gilani, S.M.; Khurram, S.; Shafiq, M.; Khan, A.W.; Usman, M., "Hash-chain based peer-peer key management and establishment of security associations in MANETS", DOI: 10.1109/ICIET.2010.5625727, 2010

[10] Li-Li Pan, "Research and simulation for secure routing protocol based on Ad hoc network", DOI: 10.1109/ICETC.2010.5529947, 2010

[11] P. Papadimitratos and Z. J. Haas, ―Secure Link State Routing for Mobile Ad hoc Networks,‖ Proc. IEEE Wksp. Security and Assurance in Ad hoc Networks, IEEE Press, 2003, pp. 27–31.

[12] K. Sanzgiri et al., ―A Secure Routing Protocol for Ad hoc Networks,‖ Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), IEEE Press, 2002, pp. 78–87.

[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, ―Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks,‖Proc. 22nd Ann. Joint Conf. IEEE Comp. and Commun. Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976–86.

[14] Y.-C. Hu, D. B. Johnson, and A. Perrig, ―SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc works,‖ Proc. 4th IEEE Wksp. Mobile Comp. Sys. and Applications, Callicoon, NY, June 2002, pp. 3–13.

[15] P. Papadimitratos and Z. J. Haas, ―Securing the Internet Routing Infrastructure,‖ IEEE Commun. Mag., vol. 10, no. 40, Oct. 2002, pp. 60–68.

[16] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002, pp.70–75.

[17] M. Joa-Ng and I. T. Lu, "A Peer-to Peer Zone-Based Two Level Link State Routing for Mobile Ad hoc Networks," IEEE JSAC, vol. 17, no. 8, Aug. 1999, pp. 1415–25.

[18] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," Proc. IEEE Wksp. Mobile Computing Systems and Applications, Dec. 1994.

[19] D. B. Johnson and D. A. Maltz, "Dynamic Sources Routing in Ad Hoc Wireless Networks," Mobile Computing, 1996.

[20] Y. KO and N. H.Vaidya, "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," Proc. ACM MOBICOM 1998, Oct. 1998, pp. 66–75.

[21] L. Lamport, "Password Authentication with Insecure Communication," Commun. ACM, vol. 24, no. 11, Nov. 1981.

[22] L. Lilien, "Developing Pervasive Trust Paradiam for Authentication and Authorization," Cracow Grid Wksp. (CGW'03), Cracow, Poland, Oct. 2003.

[23] W. Liu and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM 2004, 2004.

[24] D. A. Maltz, "Resource Management in Multi-hop Ad Hoc Networks," CMU School of Computer Science Technical Report CMU-CS-00-150,Nov. 21, 1999.