ANALYZING THE IMPACT OF EAVES ON ENERGY CONSUMPTION OF AODV ROUTING PROTOCOL FOR MANETS

Dr. K.Soumya and Prof. S. P. Setty

Dept. of Computer Science & Systems Engineering, Andhra University, Visakhapatnam, India

ABSTRACT

In this dynamic world, communication is a sine qua non for development. Communication represents sharing of information which can be local or remote. Though local communications may occur face to face between individuals remote communications take place among people over long distances. Mobile ad hoc networks (MANETs) are becoming an interesting part of research due to the increasing growth of wireless devices (laptops, tablets, mobiles etc.) and as well as wireless internet facilities like 4G/Wi-Fi. A MANET is any infrastructure-less network formed by independent and self-configuring nodes. Each node acts as router. In order to send data, the source node initiates a routing process by using a routing protocol. The nature of the wireless medium is always insecure. So, during routing many attacks can take place. The main objective of an eavesdropper is to grab the confidential information in the network. This secret information is used by a malicious node to perform further attacks. Here, the entire problem lies in identifying the eavesdropper because the eavesdropper acts a normal node in the network. In this paper, we analyzed the impact of eavesdropper while executing an Ad hoc On Demand routing (AODV) protocol in MANETs. All the simulations are done using QualNet 5.1 network simulator. From the results, it is found that the network performance degrades in presence of an eavesdropper.

KEYWORDS

MANETs, AODV, eavesdropper, energy consumption, QualNet

1.INTRODUCTION

The wireless networks can be classified into two categories - infrastructure based and infrastructure less. The best suitable networks under infrastructure based networks are cellular networks. This is because, these networks are set up and run based on infrastructure (example cell tower). Another example of infrastructure based network is the use of Wi-Fi in homes or office or railways stations etc. In this also, a Wi-Fi router (access point) is needed to make nodes connected to the internet. The infrastructures less wireless networks are called as “ad hoc” networks or peer to peer networks. These networks work without any additional infrastructure and make nodes connected to them. For example, a laptop can be used to set up ad hoc network with a user name and password. All other nodes (laptops or PDA’s) can be connected to this laptop by turning on ad hoc node in the nodes and by providing correct password. If the laptop has an internet, this will be shared to the other nodes also. This sharing of internet to other nodes and enabling all nodes to share information method is being used in present days ShareIt application in mobile phones. All operating systems ranging from Windows XP to Windows 10, support ad hoc networks in the “Network and Sharing Center” category under control panel.

DOI: 10.5121/ijwmn.2019.11101

A mobile ad hoc network (MANET) is a special kind of wireless ad hoc network in which autonomous mobile nodes connected by wireless links. A sample MANET is shown in figure 1. These nodes require minimum human intervention to configure the network.

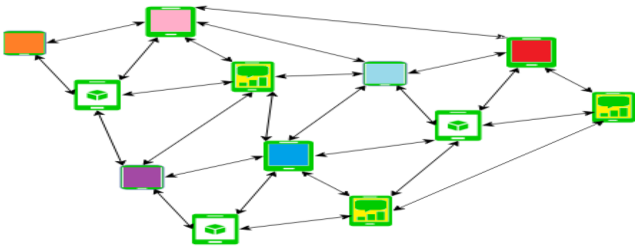


Figure 1: MANET scenario

Due to the self-organizing nature present in the wireless mobile ad hoc networks, all the nodes can join or leave the network at any time. The high mobility among the nodes in the network possesses dynamic change in the topology. As the network operates in peer to peer fashion, each node acts as both host and router. This means that, every node forwards packets and thus every node participates in routing process. In MANETs, node's resources like battery life time, processor processing capabilities are very limited. Generally, the wireless channel is also not secure. Due to these characteristics, routing securely is difficult.

Basically routing is to find a path from source to destination in order to send data. One of the challenging problem in the MANET [1][2] is to route the packets from source to destination safely in presence of attackers. The MANET routing protocols [3][4][5][6] can be classified into various types -proactive , reactive and hybrid. In the proactive routing protocols, a route is already found. So, simply sending of data in the route is enough. All the proactive routing protocols are table driven and static which are unsuitable to MANET's characteristics. Due to this reason reactive protocols are invented. In reactive routing protocols, when a source has data to send it initiates a route discover process to find a route. Once the route is found, on demand, the data is transferred in the route to the destination. The advantages of proactive routing an reaactve routing are both taken and placed in hybrid routing.

In this paper, we studied an Ad hoc On-demand Distance Vector (AODV) routing protocol [7] [8] routing protocol in presence of an unsecured environment. The simulations are done for 20, 40 and 60 number of nodes using QualNet [9] 5.1 network simulator.

In this paper section1 deals with introduction to MANETs and its characteristics. The famous existing routing protocol – AODV, security, attackers and QualNet is given in section 2. Our simulation environment is placed in section 3. Our results are graphically represented along with simulation tables are given in section 4. The future scope of our work is given Section 5.

2. REVIEW OF LITERATURE

2.1 AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

The Ad hoc On-demand Distance Vector (AODV) routing protocol is a reactive routing protocol. Whenever a node wants to send a packet it initiates a route discovery process. The source node sends a route request RREQ to its neighbors. Each intermediate node forwards the request. When the destination is found, a route reply RREP is sent from that node to the source node. When the link fails, that erroneous node sends a route error RERR to the source node. This prevents other nodes in the network from using the failed path.

2.2 Security Attacks

The attacks [11] in MANET can roughly be classified into two major categories-passive attacks and active attacks, according to the attack means [12] [13]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, there Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. The active attacks modify the data and hence they can be identified easily. Whereas, the passive attacks do not modify data and therefore identification is difficult.

2.3 Eavesdropper

Eavesdropping [14] is the intercepting and reading of messages and conversations by unintended receivers. The goal [15] of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes. There are two types of eavesdropping attacks in wireless ad hoc networks: 1. Passive Eavesdropping, in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium; 2. Active Eavesdropping, where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly node.

2.4 E-AODV (Eavesdropper in AODV)

The eaves dropper automatically gets into the network. Initially, this attacker also participates in the route discovery process. Later, this eavesdropper attracts network traffic by advertising itself having the path to the destination. That is, a RREP is sent to source says that is has the route to the destination. This process of attracting network traffic simply and not changing routing information is eaves attack. As these are no secure boundaries, no central administration to look, the eavesdropper simply gets all the information in the network it is residing. Further , this eavesdropper in advance stages drops all packets (blackhole attack) [16] or tunnels the packets from one location to another (wormhole attack)[17]. When an eavesdropper is present the packet will go to some other nodes, rather than the intended node.

2.5 QualNet network simulator

The QualNet [9] simulator imitates the behavior of a real network through planning, testing and training tools. The users can design new protocol models, optimize models, analyze the performance of networks. This simulator scales well to all types of wired and wireless networks.

3. RESEARCH METHODOLOGY

The majority of the secure ad hoc routing protocols proposed so far tend to focus on the protection techniques rather than computational cost and energy consumption. The main objectives have been to investigate the applicability of the existing secure schemes for MANETS by minimizing the energy consumption to enhance the network life and contribute to the development of resource efficient and secure to enhance the network. Several researchers have proposed several solutions to support QoS in the dynamic MANET environment. But they are not taking care about the provisioning of security requirements in hand held devices, where the resources are scarce. This is because the security provision will cost more resources and minimizes the network life. It may also adversely affect the QoS. Thus, it may be necessary to consider provisioning of security to minimize the energy consumption so as to provide network life in an integrated manner. To evaluate the designs proposed in this work and to choose the most suitable evaluation methodology, three evaluation methodologies were identified namely - simulation, experimental and mathematical.

Simulation is chosen, as experimental methodology is not practicable while mathematical methodology is highly restrictive. This simulation method is to evaluate the collection of the results. The results are analyzed and compared with E-AODV along with AODV.

3.1 SIMULATION SCENARIO

All the simulations are carried out in QualNet simulator, for various numbers of nodes like 20, 40, 60 and 100. One of the given nodes, a single node acts as an eavesdropper. This eavesdropper has the same simulation parameters like other normal nodes as listed in table 1. A random node placement model is selected, in which all the nodes move randomly with speeds ranging from 1 m/s to 10 m/s. A constant bit rate (CBR) [19] traffic model is used to generate constant traffic at a deterministic rate The packets size of 512 bytes used in the entire experiment. A two-ray model or the two-path model [9] captures the signal reached to the receiver through multiple paths. According to this model, the received power is given by:

$$\mathbf{P_r=P_tG_tG_r(h_th_r/d^2)^2} \qquad \ldots \text{ eq.(1)}$$

Where Pt is the transmitted power, Gt and Gr are the transmitter and receiver antenna gains, respectively, in the direction from the transmitter and receiver, d is the distance between the transmitter and receiver, and ht and hr are the heights of the transmitter and receiver, respectively.

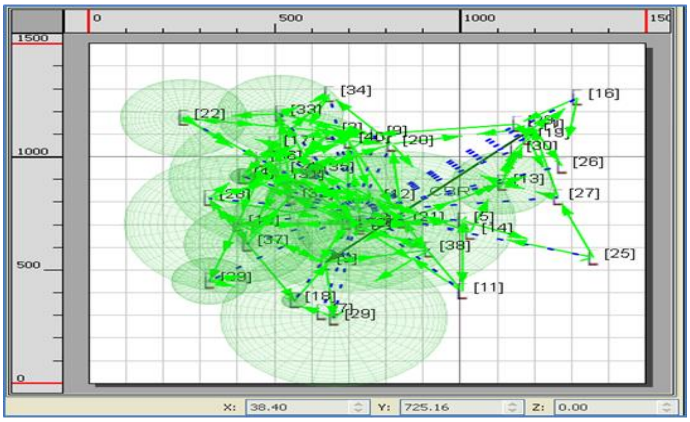
Initially, scenarios for 20,40,60,80 and100 number of nodes is run using AODV protocol in the absence of an eavesdropper under the scenario properties as listed in table 1. All the results pertaining to different metrics are noted. Later, a particular node is chosen as an eavesdropper. All the scenarios are carried out in presence of an eavesdropper for 20,40,60,80 and100 number of nodes under the same scenario properties as listed in table 1. All the results related to this newly simulated protocol E-AODV (Eaves-Ad hoc On-demand Distance Vector routing protocol) are considered. In AODV and E-AODV all the nodes are highly mobile.

Table 1. Scenario Parameters

Routing Protocols	AODV & E-AODV
Terrain	1500 m x 1500 m
Simulation Time	120 sec
Mobile Nodes	20,40, 60,80 & 100
Placement Model	Random
Propagation Model	Two ray
Mobility Model	Random Way Point
Pause Time	0 sec
Minimum Speed	1 m/s
Maximum Speed	10 (m/s)
Traffic	CBR
Packet size	512 bytes
MAC layer	802.11
Antenna Type	Omni-directional

The QualNet simulation scenario for 40 nodes under the parameters is show in figure 2.

Figure 2: Simulation scenario for 40 nodes



4. RESULTS AND ANALYSIS

Firstly, we present QOS metrics – throughput, average end-to-end delay and average jitter. Lastly, we present metrics related to energy consumption [18].

4.1 THROUGHOUT (BITS/S): It is the rate of successfully transmitted data per second in the network during the simulation. The variation of throughput with different nodes is shown in figure 3. The results are tabulated in table 2.

Figure 3: Variation of throughput with different nodes

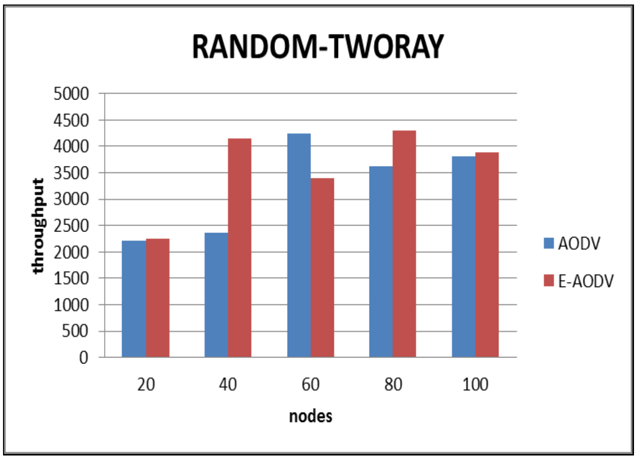


Table 2: Variation of throughput with different nodes

throughput	No. of nodes				
Protocol	20	40	60	80	100
AODV	2208	2353	4238	3620	3808
E-AODV	2252	4148	3391	4293	3882

The results show that, the throughput increases along with network size in E-AODV, except for 20 and 100 nodes.

4.2 AVERAGE END-END DELAY(S): It is the time taken for a packet to travel from a source to destination. The variation of average end-end delay with different nodes is shown in figure 3. The values are presented in table 3.

Figure 4: Variation of Average end-end delay with different nodes

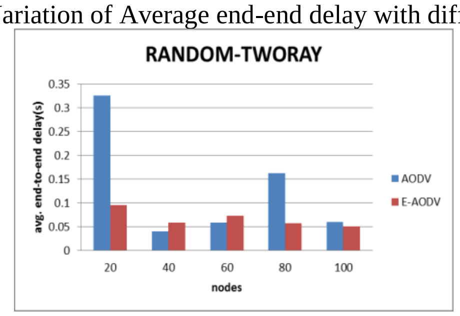


Table 3: Variation of Average end-end delay with different nodes

Average end-end delay	No. of nodes				
Protocol	20	40	60	80	100
AODV	0.325739	0.0409617	0.0584267	0.162352	0.0601867
E-AODV	0.0962007	0.0591429	0.0726921	0.0573371	0.0506981

From the result, it is observed that the average end-to-end delay increases along with network size in E-AODV, except for 60 nodes. This is not advisable for any network.

4.3 AVERAGE JITTER (S): It is the variance of minimum and maximum delay. The variation of average jitter with different nodes is shown in figure 5 and is tabulated in table 4.

Figure 5: Variation of Average jitter with different nodes

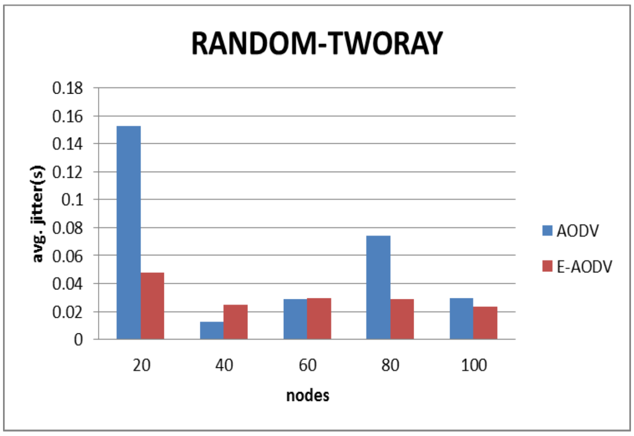


Table 4: Variation of Average jitter with different nodes

Average jitter	No. of nodes				
Protocol	20	40	60	80	100
AODV	0.152782	0.0125734	0.028561	0.0739777	0.0296098
E-AODV	0.0476167	0.0248356	0.0295323	0.0291724	0.0236499

The results indicate, the average jitter increases along with network size in E-AODV, except for 20 and 60 nodes. This is not advisable for a network.

4.4 ENERGY CONSUMED IN TRANSMIT MODE: The nodes require energy to transmit data packets. This energy is called Transmission Energy (Tx). The variation of energy consumed in transmit mode with different nodes is shown in figure 6 and the metric values are given in table 5.

Figure 6: Variation of energy consumed in transmit mode with different nodes

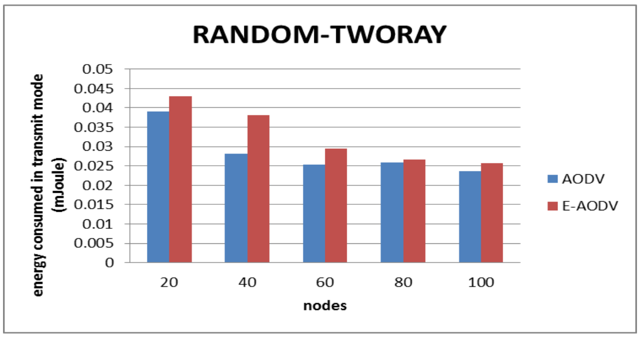


Table 5: Variation of energy consumed in transmit mode with different nodes

energy consumed in transmit mode	No. of nodes				
Protocol	20	40	60	80	100
AODV	0.0391125	0.0282068	0.0252639	0.0258141	0.023612
E-AODV	0.0429347	0.038067	0.0295051	0.0266319	0.0256251

From the results, it is found that, in E-AODV energy is consumed a lot in transmit mode. This is because, an eavesdropper attracts traffic. So, the energy consumed in transmit mode is more for all nodes in E-AODV.

4.5 ENERGY CONSUMED IN RECEIVE MODE: When a node receives a data packet from other nodes certain amount of energy is consumed. This energy taken to receive packet is called Reception Energy (R_x). The variation of energy consumed in receive mode with different nodes is shown in figure 7 and the data values are given in table 6.

Figure 7: Variation of energy consumed in receive mode with different nodes

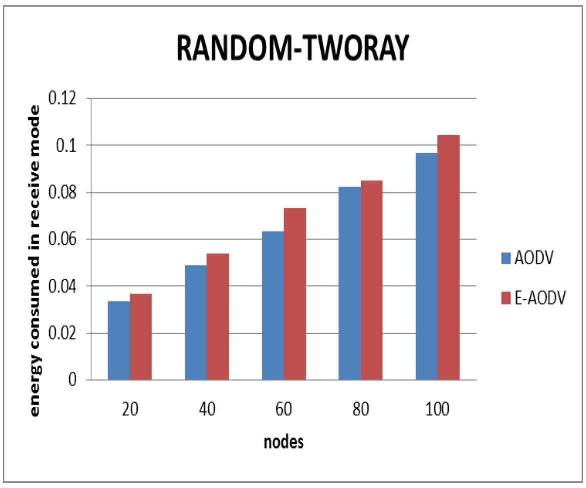


Table 6: Variation of energy consumed in receive mode with different nodes

energy consumed in receive mode	No. of nodes				
Protocol	20	40	60	80	100
AODV	0.0335119	0.049095	0.0634596	0.0823396	0.0967015
E-AODV	0.0366444	0.0538067	0.0735712	0.0850931	0.104673

From the results, it is found that, the energy in receive mode is high in E-AODV. This is because the eavesdropper should receive the packet speedy. Otherwise the actual packet will be received by the destination. . So, the energy consumed in receive mode is more for all nodes in E-AODV.

4.6 ENERGY CONSUMED IN IDLE MODE: In this mode, generally a node is neither transmitting nor receiving any data packets. But this mode consumes power because the nodes have to listen to the wireless medium continuously in order to detect a packet that it should receive, so that the node can then switch into receive mode from idle mode. The variation of energy consumed in receive mode with different nodes is shown in figure 8.

Figure 8: Variation of energy consumed in idle mode with different nodes

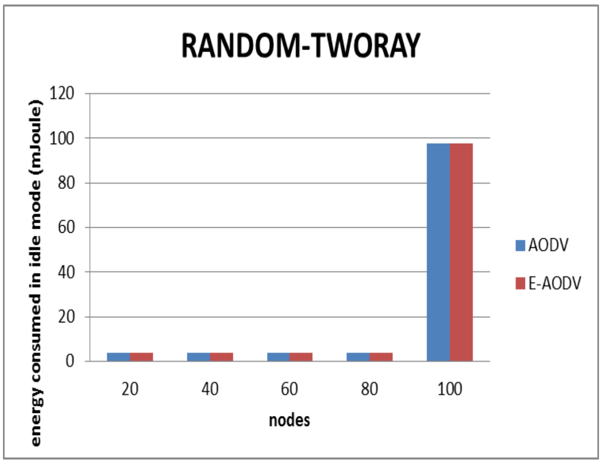


Table 7: Variation of energy consumed in idle mode with different nodes

energy consumed in idle mode	No. of nodes				
Protocol	20	40	60	80	100
AODV	3.9658	3.95232	3.93931	3.92184	97.7191
E-AODV	3.96259	3.94776	3.92962	3.91923	97.5309

From the results, it is observed that, the energy consumed in idle mode less more in E-AODV. This is a special case.

4.7 TOTAL ENERGY: It is the sum of energy consumed in transmit mode, receive mode and idle mode. The variation of energy consumed in all the three modes with different nodes is shown in figure 9 and the data values are given in table8.

Figure 9: Variation of total energy consumption with different nodes

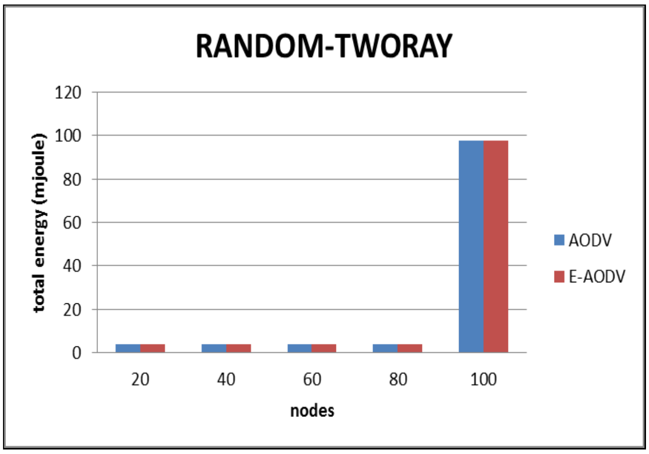


Figure 8: Variation of total energy consumption with different nodes

total energy consumption	No. of nodes				
Protocol	20	40	60	80	100
AODV	4.0384244	4.0296218	4.0280335	4.0299937	97.8394135
E-AODV	4.0421691	4.0396337	4.0326963	4.030955	97.6611981

The total energy consumed is more for all nodes, except for 100 nodes in E-AODV.

5. CONCLUSION AND FUTURE SCOPE OF WORK

This paper makes an attempt in knowing the amount of energy consumption in presence of an eavesdropper for different number of nodes ranging from 20,40,60,80 and 100. From the experimental results, it is found that as throughput increases in E-AODV, the end-to-end delay also increases. This is not acceptable in any network. Moreover, the total energy consumption increases. These high metric values indulge in degrading the network performance and thereby decrease the network lifetime. So, it is understood that in presence of an eavesdropper, the performance of AODV routing protocol falls. This is because the existing AODV routing protocol is not scalable. This paper purely focuses on identifying the impact of increase in the energy consumption of AODV routing protocol in presence of an eavesdropper. This is done by simulating E-AODV routing protocol in QualNet simulator. The limitation of this work is that, we are not considering either the protection in the network or minimizing the energy consumption or to increase the battery life of the node. In future work, we present a fuzzy-based solution which improves the performance of the protocol by providing security and minimizing the energy consumption in presence of an eavesdropper.

REFERENCES

[1] D. P. Agrawal and Q-A Zeng. "Introduction to Wireless and Mobile Systems," Brooks/Cole Publishing, ISBN No. 0534-40851-6, 436 pages, 2003.

[2] S. Giordano and W. W. Lu, "Challenges in mobile ad hoc networking," IEEE Communications Magazine, vol. 39, no. 6, pp. 129–181, June 2001.

[3] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. "Multi-Hop Wireless Ad Hoc Network Routing Protocols." ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'98), pages 85-97, 1998.

[4] Latiff, L. A. and Fisal, N. 2003. 'Routing Protocols in Wireless Mobile Ad Hoc Network – A Review'. The 9th Asia-Pasific Conference on Communication (APCC 2003), vol. 2, pp. 600- 604.

[5] S. Lee, M. Gerla, and C. Chiang. "On-Demand Multicast Routing Protocol." IEEE Wireless Communications and Networking Conference (WCNC'99), 1999.

[6] J. Broch, D. Maltz, D. B. Johnson, Yih-Chun Hu, J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing protocols."Proceedings of the Fourth Annual ACM/IEEE on Mobile Computing and Networking, MOBICOM 98, October 1998.

[7] C.E. Perkins, E.M. Royer & S. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, IETFInternet draft, draft-ietf-manet-aodv-08.txt, March 2001

[8] C. E. Perkins, and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999

[9] QualNet 5.1 Developer Model Library, Scalable Network Technologies, Inc., http://www.scalable-networks.com

[10] Jiejun Kong, Xiaoyan Hong. AODV: anonymous on demand routing with untraceable routes for mobile adhoc networks. MobiHoc'03, June 1–3, 2003, Annapolis, Maryland, 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.) pp.,2006 Springer

[12] 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.

[13] R. Oppliger, Internet and Intranet Security, Artech House, 1998.

[14] Qiu Wang and Hong-Ning Dai and Qinglin Zhao, "Eavesdropping Security in Wireless Ad Hoc Networks with Directional Antennas"

[15] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour2, 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

[17] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS", 2008 IEEE

[18] Neeraj Tantubay,Dinesh Ratnam Gautam and Mukesh Kumar Dharjwal , "A Review of Power Conservation in Wireless Mobile Ad hoc Network (MANET)",IJCSI Vol.8, Issue 4, No.1 , July,2011