Volume 3, Issue 9, September 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET

N. Satheesh*
Research Scholar in Department of CSE,
Karpagam University, Coimbatore, India

Dr. K. Prasadh
Mookambika Technical Campus,
Muvattupuzha, Kerala, India

Abstract*— In recent years, ubiquitous computing using Mobile Ad Hoc Networks (MANET) created many researches in all the application areas. Since the nodes in MANET are small with limited resources, highly mobile and has no centralized administrative control, it is used for tracking and monitoring in unattended environments. Dynamic topological changes due to the high mobility of the nodes make challenges in routing and making secure communication. In this paper, the impact of wormhole attack is analysed with Ad Hoc on demand Distance Vector Routing protocol in the presence of wormhole attacks. The parameters such as throughput, end to end delay and the number of cache replies were used to evaluate the performance. Result shows that throughput and the number of cache replies are increased up to 50% in the presence of malicious nodes and the end to end delay is increased randomly.

Keywords*— MANET, Wormhole attack, AODV, Protocol, Cache Replies, Ad Hoc, Throughput, End to End delay.

I. INTRODUCTION

The nature of ubiquitous communication in Mobile wireless networks increases the demand in many application areas. Mobile Ad hoc Network (MANET) has a huge number of nodes that use no fixed infrastructure or fixed connectivity among them. Each node has small processing unit, memory, communication interface and limited residual power. Infrastructure of MANET is reconfigurable whenever the node changes its location. Communication among the nodes is possible by multi hop paths by using a number of intermediate nodes. Mobility of the nodes, available power and signal inferences make frequent topology changes [1]. In the protocol architecture of MANET, the functions for controlling media access and power, routing and transporting are needed. The transmission and power control are the factors that control the transmission capacity, consumption of the residual energy and end to end delay of the network [2]. But the transmission and power control are limited by the interference of the communication signals. MANETs are mostly used for environmental monitoring, tracking and rescue operations. Since all the nodes have limited range of wireless communication and mobility of nodes, all the nodes must cooperate with other nodes to yield maximum possible performance. When comparing to the wired networks MANETs are vulnerable to attack because of open access medium, no centralized access control and mobility nature of nodes [3]. Therefore, some risk management system is needed to identify risks and take necessary security related actions with cost effective manner.

II. ROUTING PROTOCOL

Each node of MANET has small communication range by wireless medium. Nodes within communication range transfer the data directly. Nodes with farther distance communicate by multi hop paths. Finding a shortest path between two farther nodes is the most important task in MANET. Many routing protocols are used in MANET. To improve the reliability of the network, routing protocols must be distributed. Power efficient, secure and QoS aware routing is needed to improve the performance of the entire network [4]. Major categories of routing are proactive, reactive and hybrid routing protocols [5]. Proactive routing protocols are based on the routing tables derived from the current topology of the network. Each node maintains the possible routes to all of its reachable nodes. The routing information in the table are checked and updated periodically. Whenever a new route has to be found, the contents of routing table are used. So new route is found easily, but the maintenance of routing table increases the overhead of the network. Reactive protocols are on-demand algorithms and route finding is done at the time of starting the communication. This is a reliable method, but route finding will increase the overhead. Hybrid protocols combine the methods of proactive and reactive protocols.

There are two possible ways to deliver the data from the source node to the destination node. They are unicast routing and multicast routing. In unicast routing information is sent from a single source to a single destination. In multi-cast routing, information is sent from a single source to many numbers of destinations, and all the destinations belong to a same group. Two types of routing are possible in multi-cast routing. They are mesh based routing and tree based routing. Mesh based routing has several routes to reach a destination, and tree based routing has only one path from the source node to reach a destination. Ad Hoc On-Demand Distance Vector Routing (AODV) is a reactive on demand routing protocol [6].

III. ATTACKS IN MANET

There are two major categories of attack. They are active and passive attacks [7].

a. Active attacks:

Active attack does not affect the operations of the network. The attacker just collects the data being transferred in the network. Finding this type of attack is difficult since the operations of the network are not affected. For example, snooping attack is done on another person's data by an unauthorized user.

b. Passive attacks:

In passive attack, attacker gathers data from the network and tries to alter or drop the information being transferred in the network. The attack may be initiated either internally or externally. Internal attack is more dangerous than external attacks. External attacks can be controlled by using firewalls. Passive attacks are categorized according to the functionalities in layers in the protocol stack.

1)**. Network Layer Attack:**

Wormhole attack: Malicious node gets data from one location and tunnels them to another location in the network, so that packets are resent into the network. The attackers may create a worm hole for the packets not addressed to them.

Black Hole Attack: Malicious nodes monitor the routing request in the network and advertise themselves as the intermediate nodes that have shortest paths to the destination nodes. When the reply from the malicious nodes reaches the source, a false route is created. Then, if the communication is started then malicious nodes get the data from the source node and data can be dropped or altered. Byzantine Attack: Any intermediate node is compromised to perform attacks such as creation of loops in the routes, forwarding the data in non efficient paths and selective data dropping. Information Disclosure: Any node is compromised to leak the critical information such as status, location, private and security keys of the nodes. Routing Attacks: Compromised node may create routing table overflow, routing table poisoning, packet replication, route cache and rushing attack.

2)**. Transport Layer Attack:**

Session Hijacking: Usually, session setup is done to start an authenticated communication between two nodes in the network. Attacker spoofs the target machine's IP address and the correct sequence number. Then the attacker uses them for creating new sessions and act as a legitimate user.

3)**. Application Layer Attack:**

Repudiation is one of the major application layer attacks. Some nodes may behave as selfish nodes by denying the communication.

4)**. Multilayer Attack:**

Multilayer attacks are not associated with single layer in the protocol stack.

Denial of Service attack: Denial of service is the most important multilayer attack. It prevents the services given by the network to the authorized users. This attack is done by flooding the request to the centralized resource, and it makes the failure in the resource. Jamming, SYN flooding, Distributed DOS are some of the denial of service attacks in the MANET. Impersonation: Any node is compromised by the attacker and the compromised node acts as a special user to get some important privileges.

5)**. Wormhole Attack**

Wormhole attack is created by two colluding nodes which are far away from each other and they create an illusion that they are neighbour nodes by creating a tunnel. When any one of the colluding node receives RREQ message from any source node, colluding node transfers to other colluding node via the tunnel. Then the RREQ message is resent from the other colluding node. These two colluding nodes will perform multipoint relay that leads to interpret topology control messages and data passed via the wormhole tunnel [8]. Once the topology control message is interpreted by the colluding nodes, the incorrect topology information is forwarded which prevents the participation of honest nodes to forward the data and control messages. There are two types of wormhole attacks. They are in band wormhole attack and out of band wormhole attack [9]. In band wormhole attack use the existing wireless medium to create the tunnel. There are two types of in band attacks. 1) Self-sufficient wormhole attack - The attack is done by the two colluding nodes of the wormhole tunnel. 2) Extended wormhole attack- The attack is extended beyond the colluding nodes of the tunnel. In the out of band wormhole attack, a special hardware is needed to connect the two colluding nodes. This attack may be a hidden type or exposed type. Figure 1 shows the example of wormhole attack. In the figure 1 nodes M and N are colluding nodes that create wormhole tunnel. When finding the route from the node S to D, node M receives RREQ packet and creates an illusion that node N is a neighbour node of node M that has shortest path to the node D.

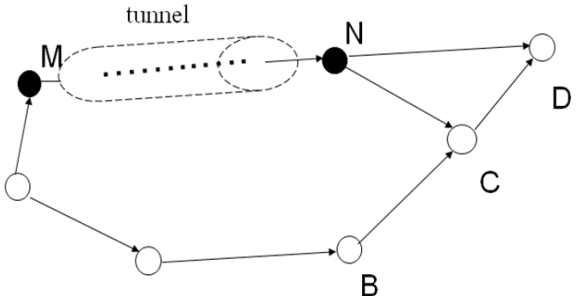

Figure 1: Example of Wormhole attack

IV. RELATED WORKS

Manickam, et al., [10] presented performance comparisons of routing Protocols in mobile ad hoc networks. Using simulator tool three different routing protocols in MANET such as DSDV, AODV and DSR were analyzed. By using various numbers of nodes, and simulation time performance was compared. DSDV was proved as best one when the network size is small and mobility of nodes is low. AODV performed best in packet delivery ratio but increased the end to end delay. DSR performed better when there was a moderate mobility of nodes with moderate traffic. Xu, et al., [11] developed an analytical framework to analyze the behavior and the performance of proactive and reactive routing protocols in MANETs. To measure the performance of the routing operation, model was synthesized with the operation of MAC protocol. Using different traffic patterns and mobility nature performance was analyzed. Using the unified model the relationship between the packet delivery ratio and type of flows was derived. Huang and Handurukande [12] presented an autonomic MANET routing protocol. Timers were mostly used when maintaining the routing information. In automated routing protocol timer was adjusted based on the dynamic nature of the network. A model was developed to compare the performance of routing algorithms such as DSDV and OLSR with fixed and adaptive tuner. Results showed that automated tuning of timer improved the performance of the network. Upadhyay and Bajpai [13] presented a statistical approach to avoid Wormhole Attack in MANET. To detect worm hole in MANET, the statistical information such as the number of incoming and outgoing packets, time needed for finding a new route, number of retransmission attempts and end to end delay were used. When there was an abnormal change in these parameters based on the node, where change occurred and percentage of the change wormhole attack was detected. Proposed algorithm proved that it was successful in detecting when sufficient information was available.

Maulik and Chaki [14] presented a study on Wormhole Attacks in MANET. Simulations were conducted with the presence of wormhole attack. Routing protocols such as AODV and DSR were used. Different mobility scenarios were created by the models random way point and Reference Point group mobility. Quality of Service (QoS) parameters such as packet delivery ratio, end to end delay, consumption of power and density of nodes were used to evaluate the performance with the presence of wormhole attack. Results showed that AODV performs better than DSR routing algorithm. Rana and Shekhar [15] presented the consequences and measures of wormhole attack in MANET. The effects of wormhole attacks and multi-mode wormhole attacks were analyzed with different scenarios. Comparison of result showed that multi-mode attack dropped a number of packets in multiple numbers of times when compared to the normal ad-hoc network. Thalor and Monika presented a review on Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks [16]. This work gave a survey of existing routing algorithms with worm-hole attack problem. There was no single solution for all situations. Based on the number and density of the nodes in the network, type of data to be transferred and specific to the application synchronization, QoS can be fixed. Jain and Jain [17] presented a novel trust-based scheme to identify and separate the colluding nodes that create a wormhole tunnel in the MANET. Without using any cryptography, simulations were conducted with the presence of colluding nodes. Trust based scheme avoids colluding nodes and does not create any unwanted conditions in the network, when establishment and operation of the network. Bouhorma, et al., [18] presented a performance comparison of Ad hoc Routing protocols such as AODV and DSR. Two important properties such as Qualitative and quantitative properties were used to measure the performance. Some of the qualitative properties were degree of operation distribution, freedom of loops, security and demand based routing. Some of the quantitative properties of routing were end to end delay, throughput, packet delivery ratio, memory requirement and route finding time. Since many of the routing protocols used qualitative parameters to evaluate the performance, recently many simulation studies use quantitative properties to compare the performance of routing protocols.

V. MATERIALS AND METHODS

In this work, the impact of wormhole attack is observed in MANET. AODV routing protocol is used for finding paths between source and destination nodes. Whenever a source node tries to send a packet to a destination node, source node broadcast route request (RREQ) packet. The neighbor nodes of the source node gets RREQ packet and broadcasts to their neighbor nodes. This forwarding will continue until the RREQ reaches the destination. While forwarding all the intermediate nodes record the information in their routing tables. Then the destination node sends a reply in the reverse path by using the information stored in the intermediate nodes. To maintain the routes, if a source node moves again RREQ packet is sent. Whenever the intermediate node moves, link failure information is sent to the source node.

To identify the nodes involved in wormhole attack some of the parameters used are strength, length, attraction and robustness.

- Strength: It measures the amount of traffic forwarded by the tunnel which is advertised by the two colluding nodes.
- Length: Length is measured by the difference in number of hops between the genuine shortest path and the advertised path by malicious nodes.
- Attraction: Attraction means the reduction in the path length offered by the wormhole. When the attraction has low value, then the small improvement in the actual path may reduce its strength.
- Robustness: Robustness refers to the persistence of nodes creating wormhole even a small change in the topology of the network.
- Packet delivery ratio: It is the ratio between number of delivered packets and total number of dispatched packets.

The quantitative measures such as throughput, end to end delay and the number of cache replies were used to evaluate the performance. Throughput is calculated by the number of bits transferred successfully from the source to the destination divided by the amount of time taken for transmission. End to delay is the average time needed to transmit a single packet from the source node to the destination node.

VI. EXPERIMENTS AND RESULTS

The experiments are conducted with 25 nodes distributed over two square kilometers. AODV routing protocol is used. Two experiments are conducted the first without malicious nodes and the second with 20% of the nodes being malicious. Figure 2 to 4 shows the performance comparisons of two experiments.

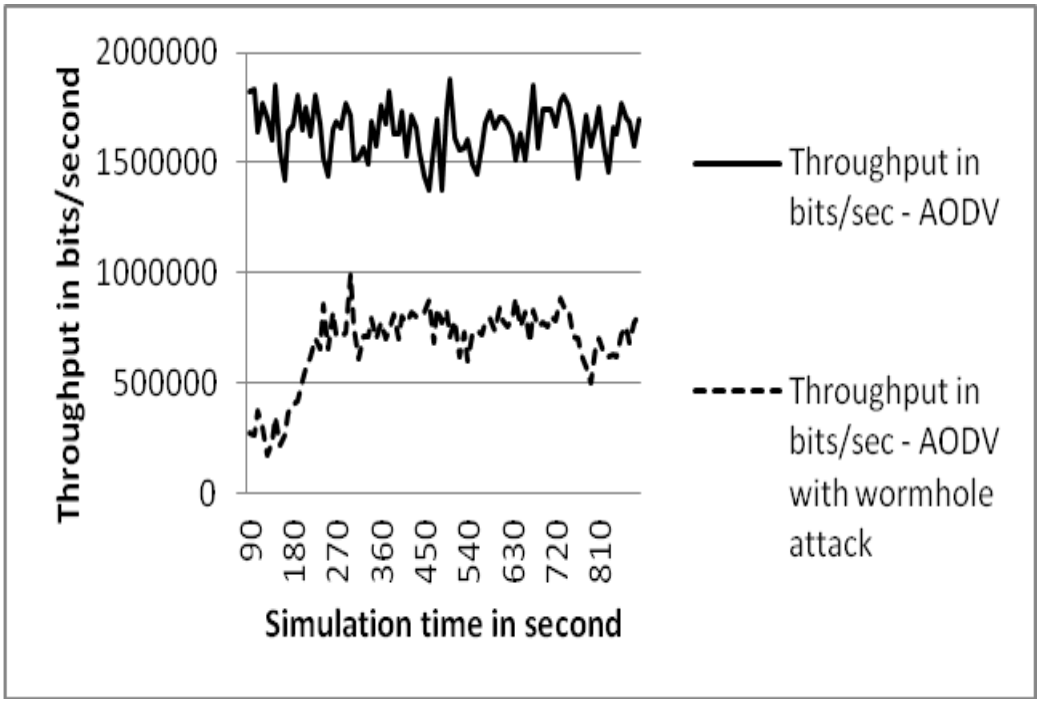

Figure 2: Throughput in bits/second

From the figure 2, it is observed that throughput is reduced up to 50% in the presence of 20% of malicious nodes in MANET.

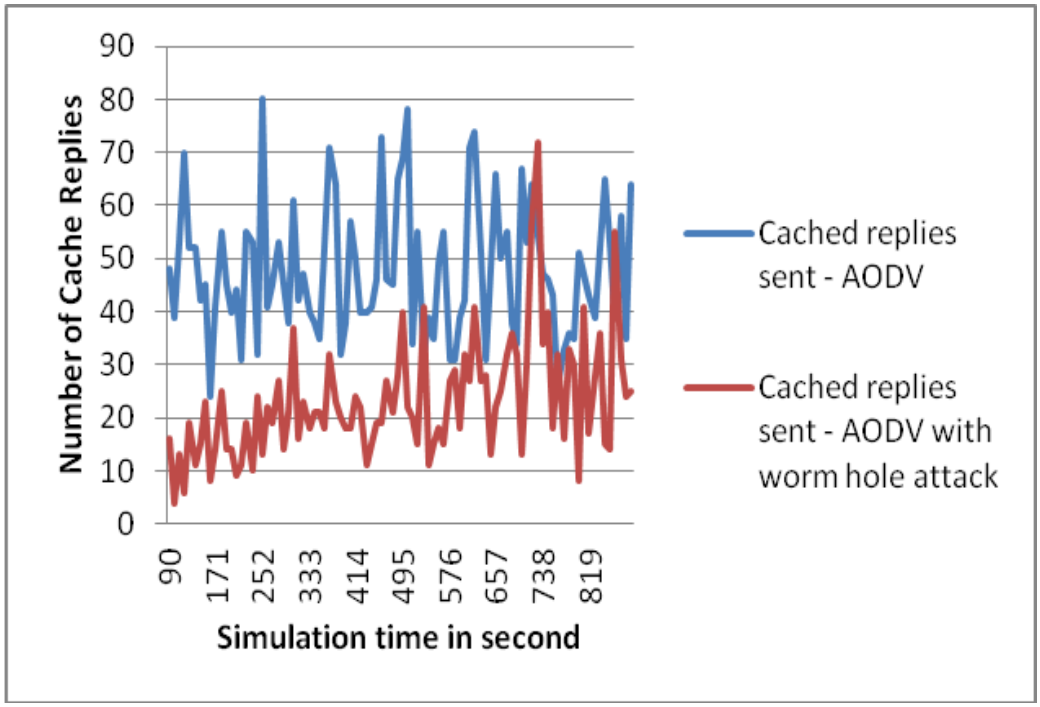

Figure 3: Number of cache replies

Figure 3 shows the number of cache replies sent in route discovery process. From the figure, it is observed that number of cache replies is three times more in the presence of 20% of malicious nodes.

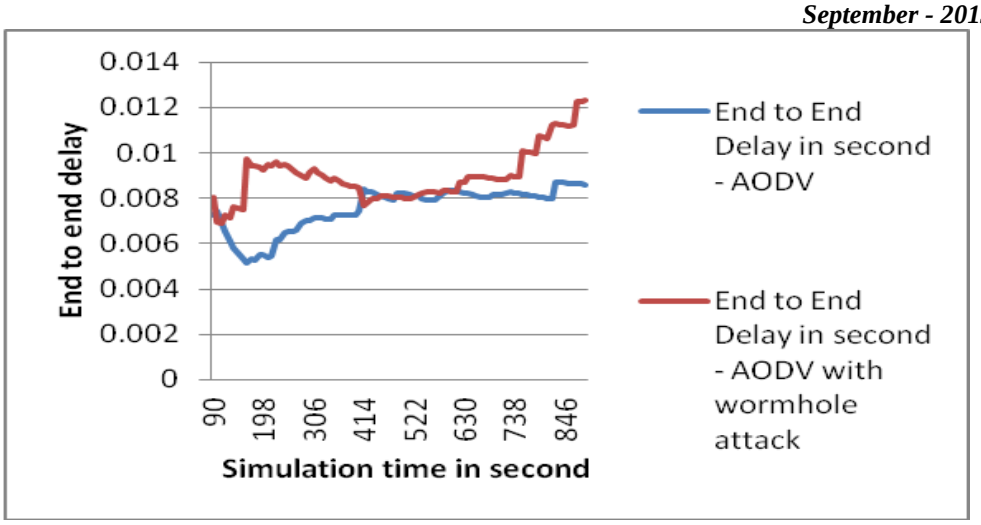

Figure 4: End to end delay

Figure 4 shows the comparison of normal and wormhole attacked MANET using the parameter end to end delay measured in seconds. Figure 4 shows that end to end delay is more variable in the presence of malicious nodes that create wormhole attack.

VII. CONCLUSION

In MANETs, to evaluate the performance variances in the presence of malicious nodes that create wormhole attack is analyzed. The experiments are conducted with 25 nodes which are distributed within two square kilometers. Two experiments are conducted, the first experiment is conducted without the presence of malicious nodes and the second experiment is done with 20% of the nodes being malicious. The parameters such as throughput, end to end delay and the number of cache replies were used to evaluate the performance. Performance comparisons are shown by line charts. Graphical results show that the throughput and the number of cache replies are increased up to 50% in the presence of malicious nodes and the end to end delay is increased randomly.

REFERENCES

[1] G. Carofiglio, C.-F. Chiasserini, M. Garettoy, and E. Leonardi, "*Route Stability in MANETs under the Random Direction Mobility Model*", International Journal of Engineering, 1(9), 2003.

[2] C.S.R. Murthy and B.S. Manoj, "*Ad-hoc Wireless Networks Architectures and Protocols*", Prentice Hallm Communications Engineering and Emerging Technologies Series, 2004.

[3] Sevil Şen, and John A. Clark, "*Intrusion Detection in Mobile Ad Hoc Networks*", Department of Computer Science, University of York, York, UK, YO10 5DD.

[4] G.Vijaya Kumar, Y.Vasudeva Reddyr and Dr.M.Nagendra, " *Current Research Work on Routing Protocols for MANET: A Literature Survey*", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, 706-713.

[5] S. Baraković and J. Baraković, "*Comparative Performance Evaluation of Mobile Ad Hoc Routing Protocols*" , Proceedings of the 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2010), Opatija, Croatia, May 2010.

[6] Perkins CE, Royer EM, Chakeres "*Ad hoc On-Demand Distance Vector (AODV) Routing*", IETF , October, 2003.

[7] 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) 265.

[8] F. Nait-Abdesselam, B. Bensaou, T. Taleb. "*Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Network***s**", *IEEE Communications Magazine*, 46 (4), pp. 127 - 133, 2008.

[9] V. Mahajan, M. Natu, A. Sethi. "*Analysis of wormhole intrusion attacks in MANETs*". In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[10] P. Manickam, T. Guru Baskar , M.Girija , Dr.D.Manimegalai, "*Performance Comparisons of Routing Protocols In Mobile Ad Hoc Networks*", The International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011, DOI : 10.5121/ijwmn.2011.3109 98.

[11] Hui Xu, Xianren Wu, , Hamid R. Sadjadpour, and J.J. Garcia-Luna-Aceves, , *"A Unified Analysis of Routing Protocols in MANETs*", IEEE Transactions on Communications, VOL. 58, NO. 3, March 2010.

[12] Yangcheng Huang, Sidath Handurukande "*Autonomic MANET Routing Protocols*", Journal of Networks, VOL. 4, NO. 8, October 2009.

[13] Saurabh Upadhyay and Aruna Bajpai, "*Avoiding Wormhole Attack in MANET using Statistical Analysis Approach*", International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012.

[14] Reshmi Maulik and Nabendu Chaki,"*A Study on Wormhole Attacks in MANET"*, International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988 Volume 3 (2011) pp. 271-279.

[15] Rohit Rana, and Jayant Shekhar, "*Consequences and Measures of Wormhole Attack in MANET*", International Conference on Recent Trends in Engineering & Technology (ICRTET2012).

[16] Jyoti Thalor and Monika,"*Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[17] Shalini Jain, Dr.Satbir Jain,"*Detection and prevention of wormhole attack in mobile adhoc networks*", *In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1* February, 2010, pp.78-86.

[18] Mohammed Bouhorma, H.Bentaouit and A.Boudhir, "*Performance comparison of Ad hoc Routing protocols AODV and DSR*", IEEE 2009.

