ISSN 2319-2720

Volume 1, No.2, September – October 2012

International Journal of Computing,Communications and Networking

Available Online at http://warse.org/pdfs/ijccn03122012.pdf

Analysis of Wormhole Attack in AODV based MANET Using OPNET Simulator

ACHINT GUPTA[1], Dr. PRIYANKA V J[2], SAURABH UPADHYAY[3]

[1]Gurgaon College of engineering, India,achintgupta7792@gmail.com

[2]Gurgaon Institute of Technology and Management, India, jvp248@gmail.com

[3]Sarvottam Institute of Technology and Management,India,saurabh.cse.cs@gmail.com

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network formed with wireless links by a collection of mobile nodes without using any fixed infrastructure or centralized management. The mobile nodes allow communication among the nodes by hop to hop basis and the forward packets to each other. Due to dynamic infrastructure-less nature and lack of centralized monitoring, the ad hoc networks are vulnerable to various attacks. The performance of network and reliability is compromised by attacks on ad hoc network routing protocols. In a wormhole attack an intruder creates a tunnel during the transmission of the data from one end-point of the network to the other end-point , making leading distant network nodes to believe that they are immediate neighbors' and communicate through the wormhole link. In this paper we have analyzed the effect of wormhole attack on AODV routing protocol based Mobile Ad-hoc Network using OPNET simulator using parameter like number of hops, delay, retransmission attempt, and data dropped.

Key words: AODV, MANET, OPNET, Wormhole attack

1. INTRODUCTION

A mobile Ad hoc network is a collection of two or more devices or nodes using wireless communication and networking capabilities [1], [2], [3]. These nodes like laptop, computers, PDAs and wireless phones have a limited transmission range for direct transmission .If two such devices are located within transmission range of each other, they can communicate directly otherwise they will use intermediate nodes. Thus, a multi-hop scenario will occur in which several intermediate will be used before they reach the final destination. Each node performs the functions as a router. The success of communication depends on cooperation of other nodes. Since the transmission may use several nodes as intermediate nodes for transmission many routing protocols [3] have been proposed for the MANETS. Many of them assume that other nodes are trustable so they do not consider attack and security issues. The lack of can move randomly, freely in any direction they will organize themselves arbitrarily in the network. The network topology changes rapidly, frequently and unpredictably which changes the status of trust among nodes .However most of these attacks are performed by a single malicious node in the network. Many solutions exist to solve such attacks [5], [6],[7] but they cannot prevent from the attacks such as wormhole attack. Routing protocols is one of the interesting research areas. Many routing protocols such as AODV, OLSR, DSR etc has been developed for MANET.

The rest of the paper is organized as follows. Section 2 describes about routing protocol and AODV. Section 3 of presents the wormhole attack. In section 4, simulation configuration is presented. Section 5 provides simulation results and analysis. Section 6 concludes the work.

2. ROUTING PROTOCOL AND AODV

2.1 Routing protocol

The nature of MANET's makes simulation modeling an important tool for understanding the operation in these networks. Multiple Ad-hoc network routing protocols have been developed in the recent years, in order to find an optimized Routes between source and destination. To make data transmission possible between two nodes, multiple hops are required due to the limited transmission range of the nodes. Due to the Mobility of the nodes the situation becomes even more complicated. Routing protocols can be categorized in three category named as proactive, reactive and hybrid protocols. Proactive routing protocols are typically table-driven such as Destination Sequence Distance Vector (DSDV). Reactive routing protocol does not regularly update the routing information. Information is updated only when there is some data need to be transmitted. Examples of reactive routing protocols are Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols are the combination of both reactive and proactive approaches such as Zone Routing Protocol (ZRP).

2.2 AODV Routing Protocol

Ad hoc On-Demand Distance Vector (AODV) [4] routing protocol is a reactive routing protocol that creates a path between source and to destination only when required. Routes are not established until any node sends route discovery message that the node want to communicate or transmit data with other node in the network . Routing information is stored in source node and destination node, intermediate nodes dealing with data transmission. This Approach reduces the memory overhead, minimize of the network resources, and runs well in high mobility scenario. The communication between nodes involves main three procedures known as path discovery, Path establishment and path maintenance. Three types of control messages are used to run the algorithm, i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) [8]. The format of RREQ and RREP packet are shown in Table 1 and Table 2.

Table 1: RREQ Field

Source address	Source Sequence	Broadcast Id	Destination Address	Destination Sequence	Hop Count

Table 2: RREP Field

Source address	Destination Address	Destination Sequence	Hop count	Lifetime

When the source node wants to send some data to the destination node, Source will issue the route discovery procedure. The source node will broadcast route request packets to all its accessible neighbors'. The intermediate node receiving request (RREQ) will check the request whether he is destination or not. If the intermediate node is the destination node, will reply with a route reply message (RREP). If not the destination node, the request will be forwarded to other neighbor nodes. Before forwarding the packet, each node stores the broadcast identifier and the node number from which the request came. Timer is used by the intermediate nodes to delete any entry when no reply is received for the request. The broadcast identifier, source ID are used to detect whether the node has received the route request message previously or not. It prevent from the redundant request receiving in same nodes. The source node may receive more than one reply, in that case it will determine later which message will be selected on the basis of hop counts. When any link breaks down due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable because of loss of the link. Then it will create a route error (RERR) message. The node sends the RERR upstream to the source node. When the source receives the Route reply message, it may reinitiate route discovery if it still requires the route.

3. WORMHOLE ATTACK

In wormhole, an attacker creates a tunnel between two points in the network and creates direct connection between them as they are directly connected. An example is shown in Figure. 1. Here R and P are the two end-points in the wormhole tunnel. R is the source node and S is the destination node . Node R is assuming that there is direct connection to node P so node R will start transmission using tunnel created by the attacker .This tunnel can be created by number of ways including long-range wireless transmission ,With the help an Ethernet cable or using a long-range wireless transmission .Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. This attack compromise the security of networks For example, when a wormhole attack is used against AODV, than all the packets will be transmitted through this tunnel and no other route will be discovered. If the tunnel is create honestly and reliably than it is not harmful to the network and will provides the useful service in connecting the network more efficiently. A potential solution is to avoid wormhole attack is to integrate the prevention methods into intrusion detection system but it is difficult to isolate the attacker using only software based approach because the packets sent by the wormhole are similar to the packets sent by legitimate nodes [9]. Choi et al. in [11] said that all the nodes should monitor the behavior of its neighbor nodes. Each node sends RREQ messages to destination by using its neighbor node list. If the source does not get back the RREP message from destination within a stipulated time, it consider the presence of wormhole attack and adds that route to its wormhole list .on-demand routing protocol (AODV) is being used in dynamic wireless ad hoc networks, a new route will be discovered in response to every route break [10]. The route discovery requires high overhead. This overhead can be reduced if there are multiple paths and new route discovery is required only in the situation when all paths break.

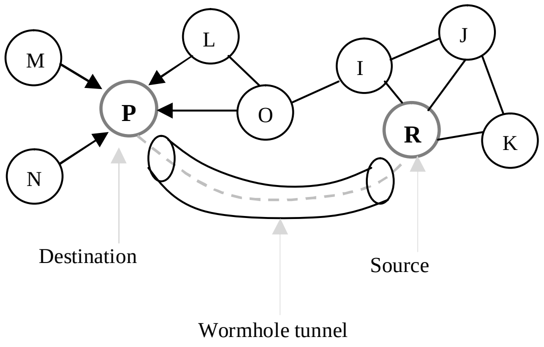

Figure 1: Warmhole Attack

4. SIMULATION CONFIGURATION

All the simulation work is performed in OPNET MODELER network simulator version 14.0.Simulation parameters are given in Table 3.

Table 3: Simulation parameters

Parameters	Description
Examined Protocol	AODV
Simulation Time	2000 sec.
Simulation Area	100×100 m
Seed value	191
Number of Nodes	16
Malicious Nodes present	02
Network traffic	CBR
Packet size	512 Byte

Table 3. Simulation parameters

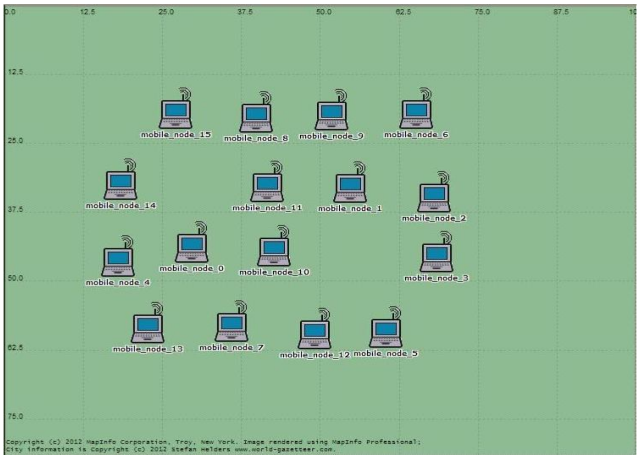

Figure : 2 Node distribution in a network

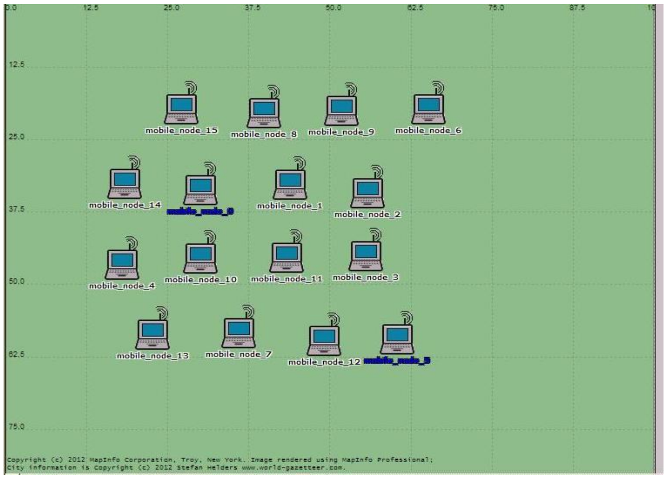

Figure 3: Node distribution affected by wormhole attack

Wormhole attack scenario is shown in Figure 3.Wormhole tunnel is created in between node 0 and node 5. Due to wormhole all the traffic between node 0 and node 5 will go directly while other intermediate nodes between them are presented in the network.

5. SIMULATION RESULT AND ANALYSIS

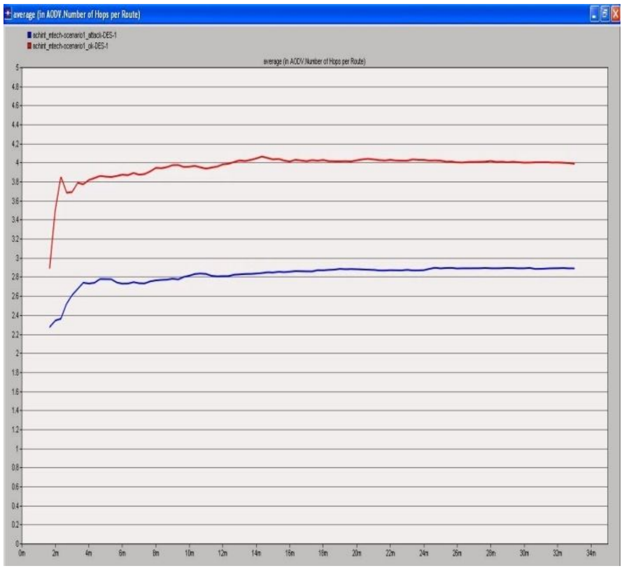

Figure 4: Average number of hops per route

Figure 4 shows the average route length using number of hops for the condition when there is no attack and when network is affected by wormhole attack'. The Simulation time is depicted by X direction and the number of hops by Y direction. No attack condition is depicted by red color where as attack condition is shown by blue color. Wormhole attack occurs in the network than wormhole affected node start sending packet by using the tunnel created by attacker without using intermediate nodes so number of hopes reduces as shown by blue color.

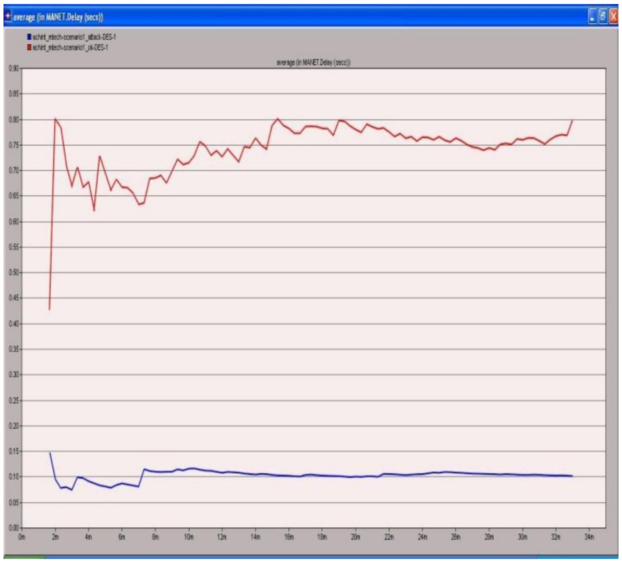

Figure 5: Average delay in seconds

Figure 5 shows the average route discovery time for wormhole attack and no attack conditions. X direction showing the simulation time while Y direction showing average delay. No attack condition is depicted by red color;

wormhole attack reduces the delay because the packets are delivered without using any intermediate nodes denoted by blue color.

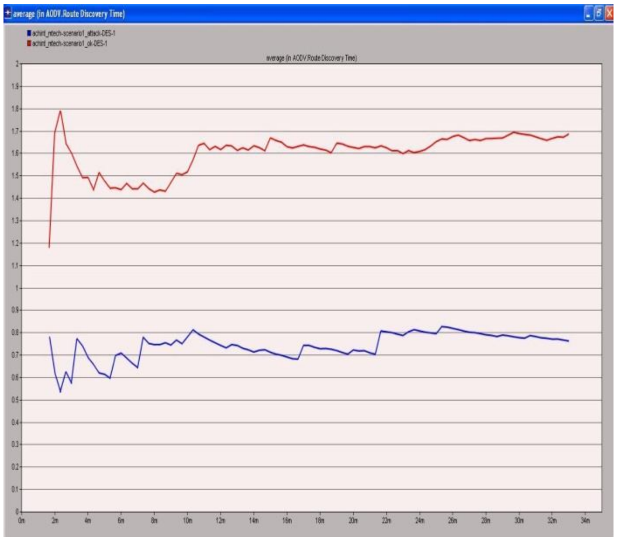

Figure 6: Average route discovery time

Figure 6 shows the average route discovery time. X direction shows the simulation time and Y direction shows the average route discovery time. Due to worm hole attack wormhole affected route will be selected most of the times so route discovery time will be reduced as depicted by blue color where as when there is no attack all the routes will be checked to find optimum routes so route discovery time will be higher as compared to the worm hole condition as denoted by red color

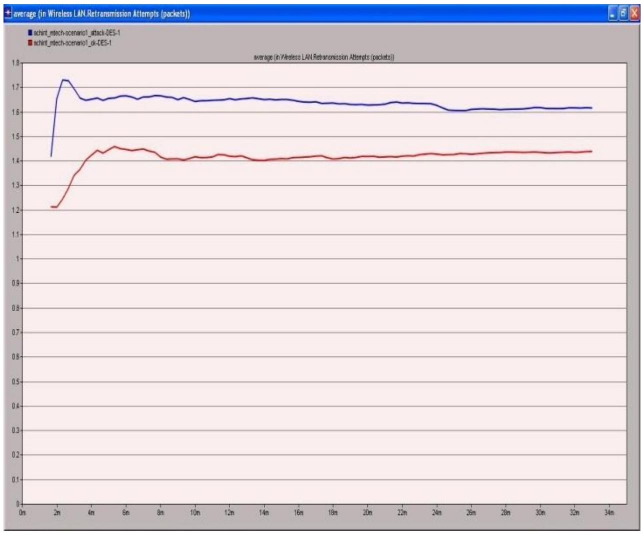

Figure 7: Average retransmission attempts

Figure 7 shows the retransmission attempt. X direction shows the simulation time and Y direction shows number of attempt for retransmission. Due to worm hole attack wormhole affected route will be selected most of the times so packet may not reach their destinations so number of retransmission will be increased as shown in red color where as when there is no attack most of packets will be delivered to destination so number of retransmission will be less denoted by blue color

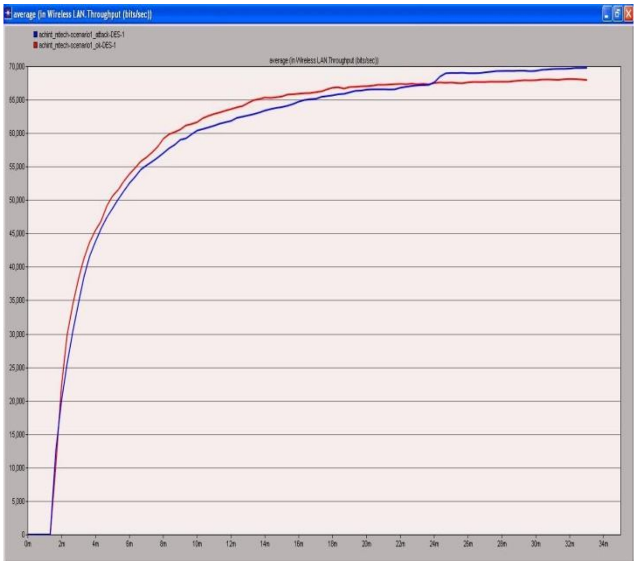

Figure 8: Average throughput

Figure 8 shows the average through put during the transmission. X direction shows the Simulation time and as Y direction number of packets transmitted. Due to wormhole attack the packets reaching their destination reduced so throughput also reduced as denoted by blue color. Whereas throughput without attack is denoted by red color

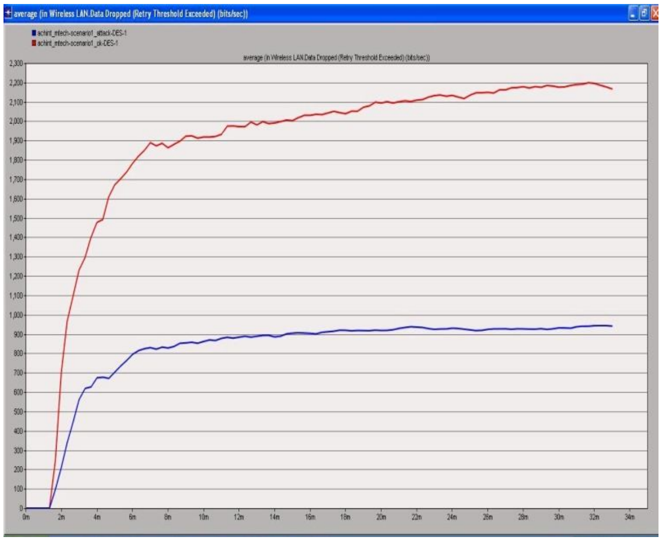

Figure. 9: Average data dropped

Figure 9 shows the average data dropped during the transmission. X direction shows the Simulation time and as Y direction depicts the number of packets loss during transmission When there is no attack in the system so packets had to travel number of hops and data will be dropped than could not find their destination as denoted by red color while when data is transmitted by using wormhole tunnel number of hops are reduced so only packets will be dropped as shown by blue color.

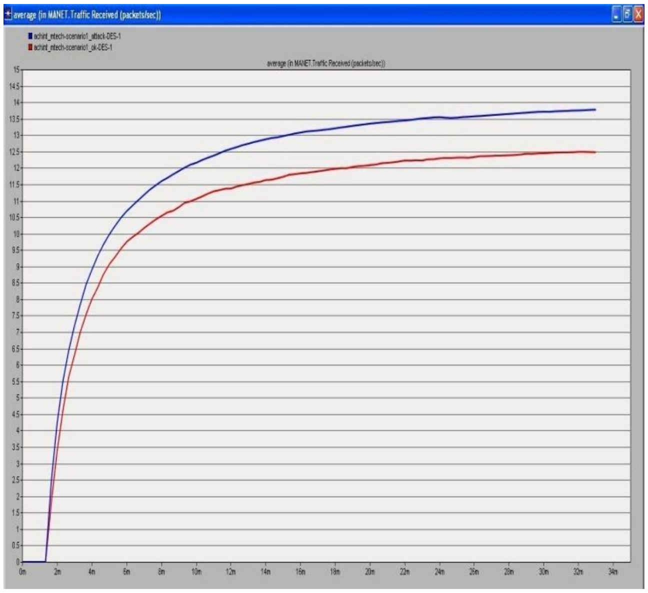

Figure 10: average traffic received

Figure 10 shows the average traffic received during the transmission. X direction shows the Simulation time and as Y direction depicts the number of packets received. Red color shows when there is no attack whereas due to wormhole attack number of packed received also increase as denoted in blue color.

6.CONCLUSION

MANETs is insecure and vulnerable to various attacks so it require a reliable, efficient and a secure protocol that can be rapidly deployed and use dynamic routing. AODV is prone to various attacks like modification in the sequence numbers or hop counts, source route tunneling, spoofing and fabrication in the error messages. Wormhole attack is a real threat against AODV protocol in MANET. Wormhole attack can be easily launched even in networks with provides confidentiality and authenticity. The malicious nodes usually target the routing control messages related to routing information. Therefore trustworthy techniques for detection and prevention of wormhole attack should be used. Some existing solutions cannot work well in the presence of more than one malicious node, while some other requires special hardware. So, there is still a lot of scope of research to provide security to the MANETs.

REFERENCES

1. Perkins C. and Bhagwat P. **Highly dynamic destination-sequence distance-vector routing (DSDV) for mobile computers,** In Proceedings of ACM Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM

2. Perkins C. and Royer E. **Ad hoc on-demand distance vector routing,** In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100 (1999)

3. Perkins.C.E. **Ad hoc Networking,** ***Boston, Addison Wesley*** (2001)

4 Harris Simaremare and Riri Fitri Sari. **Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks,** International Journal of Computer Science and Network Security, VOL-11, June 2011, pp.6.

5. Tamilselvan L. and Sankaranarayanan D. V. "**Prevention of impersonation attack in wireless mobile ad hoc Networks,** International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 3, p.118–123 (2007)

6. Papadimitratos P. and Haas Z. J. **Secure routing for mobile ad hoc networks,** In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (2002)

7. Hu Y.-C., Johnson D. B. and Perrig A. **SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,** In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13 (2002)

8. K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama and K. Thilagam. **Modified AODV Protocol against Black hole Attacks in MANET**, International Journal of Engineering and Technology Vol.2 (6), 2010.

9. S Upadhyay . and B.K Chaurasia. **Impact of Wormhole Attacks on MANETs,** International Journal of Computer Science & Emerging Technologies, Vol. 2, Issue 1, pp. 77-82 (2011)

10. R. Maulik and N. Chaki. **A Comprehensive Review on Wormhole Attacks in MANET.** In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010

11. S. Choi , D. Kim, D. Lee and J. Jung. **WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks,** International Conference on Sensor Networks Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.