International Journal of
Science and Engineering Investigations vol. 2, issue 15, April 2013
ISSN: 2251-8843

The Effects of Black Hole Attack in Mobile Ad-Hoc Network using OLSR and AODV

Najiya Sultana [1], S. S. Saragdevot [2]
[1]Research Scholar
[2]Dean, Department of CS & I, JRN Rajasthan Vidhyapeeth University, Udaipur, India
([1]saara.sultan@gmail.com)

Abstract- Mobile Ad-Hoc network is an autonomous system, where nodes or stations are connected with each other through wireless links. To forward the data to the neighbors' nodes, a node can serve as a router. This kind of network is also known as infrastructure less networks. These networks have no centralized administration. MANETs are applied is emergency services such as disaster recovery and relief activities, where traditional wired network is already destroyed. The scope of this research is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc on Demand Distance Vector (AODV). For both protocols Comparative analysis of Black Hole attack is taken into account. On the performance of MANET the impact of Black Hole attack is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. In the light of throughput, end-to-end delay and network load the measurements were taken. Simulation is done in Optimized Network Engineering Tool (OPNET). The study focuses on analyzing the effects of black hole attack in the light of Network load, throughput and end-to-end delay in MANET. We simulate the black hole attack using Proactive and Reactive routing protocols and compare the results of both Proactive and Reactive protocols to analyze which of these two types of protocols are more vulnerable to Black Hole attack.

Keywords- *MAC, MANET, AODV, Black Hole Attack, Routing Protocols, OLSR .*

I. INTRODUCTION

In wireless networks users transmit and receive data using electromagnetic waves. Due to its mobility, simplicity and very affordable and cost saving installation, wireless networks are more popular. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Also routing protocols is one of the challenging and interesting research areas. For MANETS, (i.e. AODV, OLSR, DSR etc) many routing protocols have been developed. Due to ease of deployment and getting rid of wires it is adopted everywhere. No secure authentication process is here in order to make the MANETs more secure from malicious nodes. Mostly it is seen that the attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This type of attack is also known as spoofing attack [2]. The attacker in this attack hijack all the information that a source node sent to destination node, as the attacker node impersonate the destination node. The participating nodes communicate with each other In MANETs on blind mutual trust, the attacker exploits this weak point of the MANETs [3].

II. WIRELESS NETWORKS

In Wireless networks, computer devices communicate with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. In Wireless networks, computer devices communicate with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. In wireless networks Users transmit and receive data using electromagnetic waves. Due to its mobility, simplicity and very affordable and cost saving installation, wireless networks are more and more popular. Wireless wide area network (WWAN) cover geographically larger area than local area network [4]. The wide area networks almost consist of one or two local area networks.

A. MANETs Routing Protocols

To be implemented and to provide efficient better end-to-end communication MANETs created a new set of demands [5]. To provide the means of communication between communicating work stations MANETs works on TCP/IP structure. In order to compensate the MANETs mobility to provide efficient functionality Work stations are mobile and they have limited resources, therefore the traditional TCP/IP model needs to be refurbished or modified. So, the key research area for the researchers is routing in any network. In MANETs Routing protocols are challenging and attractive

tasks [6]. Routing protocols in MANETs are classified into three different categories according to their functionality.

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

B. Ad-Hoc on Demand Distance Vector Protocol (AODV)

AODV is described in RFC 3561 [7]. It is reactive protocol. It has no route when a node wishes to start transmission with another node in the network to which; for the node AODV will provide topology information. In the network AODV use control messages to find a route to the destination node.

C. Route Discovery Mechanism in AODV

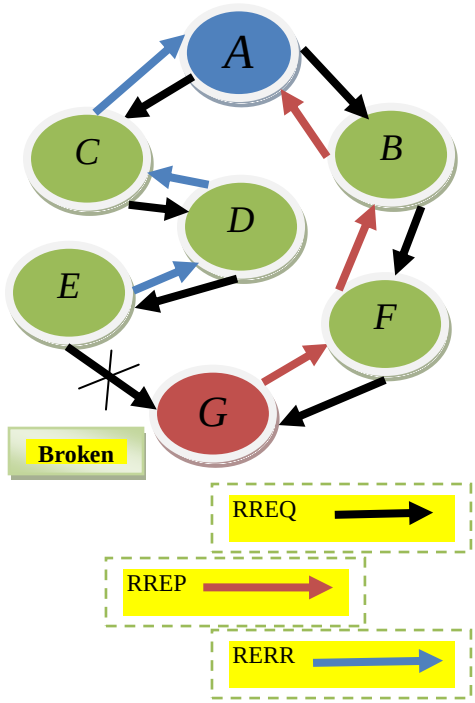

Fig.1 Route Error Message in AODV

When a node "A" wants to initiate transmission with another node "G" as shown in the figure, it will generate a Route Request message (RREQ)[7]. This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination node goes on until it finds a node that has fresh enough routes to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node [2]. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node [9]. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node. The scheme is shown in the above Fig.1.

D. Route Discovery Process

In the network when a source node wants to start data transmission with another node, it checks its routing cache. When there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any intermediate node that has fresh enough route to the destination node, RREP is generated [8]. When the source node receives the RREP it updates its caches and the traffic is routed through the route.

E. Route Maintenance Process

When the transmission of data started, it is the responsibility of the node that is transmitting data to confirm the next hop received the data along with source route. The node generates a route error message, if it does not receive any confirmation to the originator node. The originator node again performs new route discovery process [10].

F. Optimized Link State Routing Protocol

The Optimized Link State Routing (OLSR) protocol is described in RFC3626 [11]. OLSR is proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. OLSR diffuses the network topology information by flooding the packets throughout the network. The flooding is done in such way that each node that received the packets retransmits the received packets . These packets contain a sequence number so as to avoid loops. The receiver nodes register this sequence number making sure that the packet is retransmitted once. The basic concept of MPR is to reduce the duplication or loops of retransmissions of the packets.

III. BLACK HOLE ATTACK AND CLASSIFICATION

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack [12].

A. Wormhole Attacks

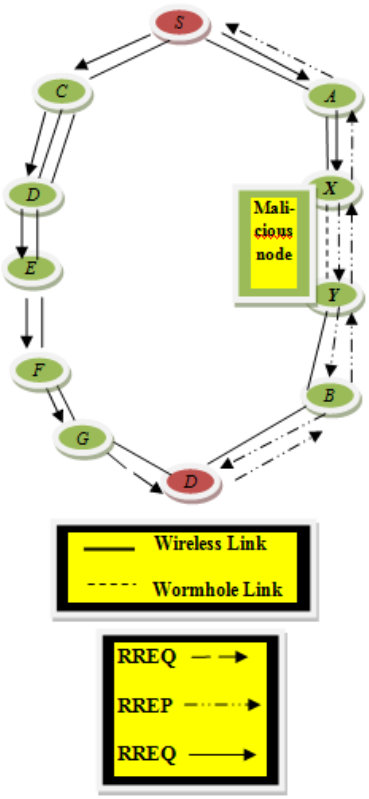

Fig.2 Wormhole Attack

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called "wormhole link". They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets [13].

B. Problems in MANETs

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are shown below.

3.2.1 Non Secure Boundaries

3.2.2 Compromised Node

3.2.3 No Central Management

3.2.4 Problem of Scalability

IV. PERFORMANCE ANALYSIS

Here we explain the various performance metrics required for evaluation of protocols. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End-to-end delay, Throughput and Network load. These matrices are important because of it performance analysis of network.

A. Performance Metrics

The performance metrics chosen for the evaluation of black hole attack are packet end-to-end delay, network throughput and network load.

In order to traverse the packet inside the network the packet end-to-end delay is the average time. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. Due to routing activities this includes the overall delay of networks including buffer queues, transmission time and induced delay. Different application needs different packet delay level. Voice and video transmission require lesser delay and show little tolerance to the delay level.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in packets per seconds or bits per second. Throughput is affected by various changes in topology, limited bandwidth and limited power in MANETs. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

The third parameter is network load, it is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. In entire network it indicates the quantity of traffic. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

V. COLLECTION OF RESULTS AND STATISTICS

TABLE I. SIMULATION PARAMETERS

Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11Mbps
Mobility Model	Random waypoint

In OPNET simulation two types of statistics are involved. Global and object statistics, global statistics is for entire network's collection of data and object statistic includes individual node statistics. Results are taken and analyzed, after the selection of statistics and running the simulation. In our case we have used global discrete event statistics (DES) [14].

VI. RESULTS

This part focuses on result and its analysis based on the simulation performed in OPNET modeler 14.5. Our simulated results are provided in Figures (3.1-3.4) gives the variation in network nodes while under Black Hole attack. To evaluate the behavior of simulated intrusion based black hole attack, we considered the performance metrics of packet end-to-end delay, throughput and network load.

A. Packet End-to-End Delay

We carried out two different simulations for packet end-to-end delay. The behavior of attack (Black hole) also depends on protocols, routing procedure and number of nodes involved. Fig. 3.1 shows the delay for AODV and OLSR in case of 16 nodes. This result was carried out when black hole attack was introduced and the graph is compared with the normal working protocol so as to observe the effect of attack on the whole network. In the network when there is no malicious node present the graph shows higher delay.

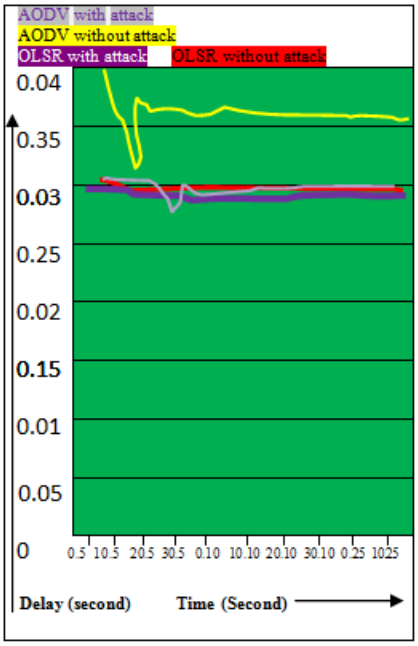

Fig. 3.1 End to end delay of OLSR and AODV with vs. without attack for 16 nodes.

B. Network Load

Similarly, simulation for large network in terms of more number of nodes e.g. in case 30 nodes were introduced with the presence of malicious node in the network. Fig 3.2 shows the delay for 30 nodes. Similar pattern was observed, the delay of both protocols was low when there is presence of malicious node. Also when both protocols i.e. AODV and OLSR was compared amongst each other to find out which has been more effected by the attack it shows that average delay of about 5 percent is increased when observed in comparison to less number of nodes which in our case is 16 nodes.

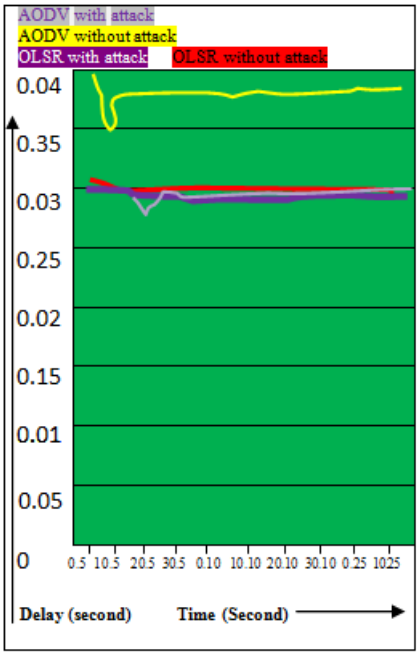

Fig. 3.2 End to end delay for OLSR and AODV with vs. without attack for 30 nodes.

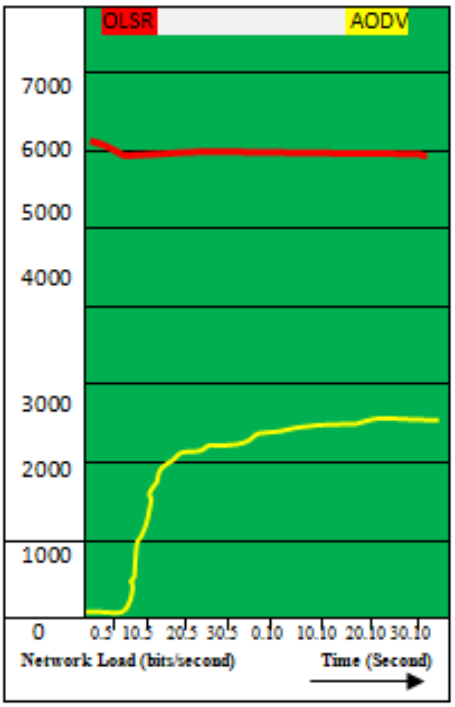

Fig. 3.3 Network loads 16 nodes AODV vs. OLSR with attack.

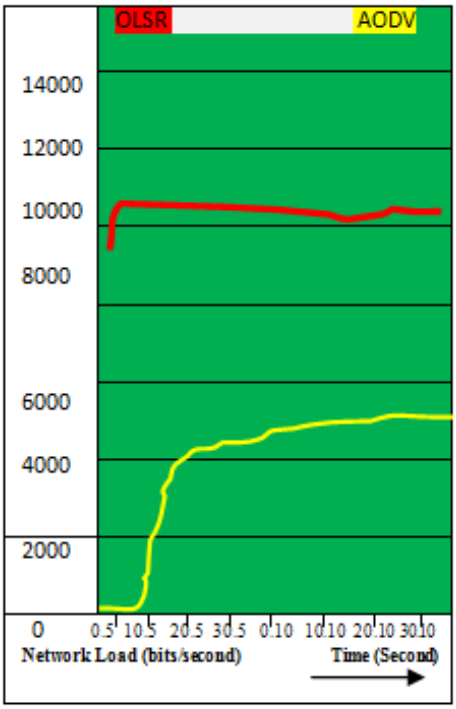

Fig. 3.4 Network loads 30 nodes AODV vs. OLSR with attack.

Like this when both protocols are compared with each other it was analyzed that In case of network load Fig. 3.3 and 3.4 OLSR has a high network load in presence of a malicious node as compare to that of AODV. In both 16 and 30 nodes network OLSR has high network load because the routing protocols are able to adjust its changes in it during node restart and node pausing. It is different at different speeds, at high speeds the routing protocols take much more time for adjusting and afterward sending of traffic to the new routes. In case of higher number of nodes AODV react more quickly as compare to OLSR which made the difference in network load much wider. As the node begins to pause and restarts and its mobility after the starting period having more stability make network load more pronounced.

VII. CONCLUSION

The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR. We conclude that AODV protocol is more vulnerable to Black Hole attack than that of OLSR protocol from our research. Many of the proposed solution claimed to be the best solution but still these solutions are not perfect in terms of effectiveness and efficiency. In the presence of single malicious node if any solution works well, it cannot be applicable in case of multiple malicious nodes. The intermediate reply messages if disabled leads to the delivery of message to the destination node will not only improve the performance of network, but it will also secure the network from Black Hole attack.

VIII. FUTURE WORK

In other MANETs routing protocols such as DSR, TORA and GRP, there is a need to analyze Black Hole attack. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. On the basis of how much they can be categorized, they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research. In the presence of single malicious node if any solution works well, it cannot be applicable in case of multiple malicious nodes. The intermediate reply messages if disabled leads to the delivery of message to the destination node will not only improve the performance of network, but it will also secure the network from Black Hole attack. Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

REFERENCES

[1] David B.Johnson and Dravid A. Maltz, "Dynamic Source routing in ad hoc wireless networks", *Technical report, Carneigie Mellon University*, 1996.

[2] 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, Page Number-6.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communication magazine, October 2002.

[4] Imrich Chlamtac, Marco Conti, Jennifer J. - N. Liu " Mobile ad hoc networking: imperatives and challenges ", School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.

[5] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Special Issue on Network Security, Vol-13, Nov-Dec 1999, Page Number - 24-30L.

[6] P. Ning and K. Sum, "How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol", Tech Rep, TR- 2003-07, CS Department, NC University, April 2003

[7] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks", Department of Computer Science and Electrical Engineering, University of Maryland.

[8] Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

[9] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 2002.

[10] M.Parsons, P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks", [Online]. Available: www.cse.buffalo.edu/srds2009/dncms2009_submission_person.pdf, [Accessed: April. 10, 2010].

[11] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[12] H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.

[13] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[14] S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265.

Najiya Sultana has 5 years teaching experience at degree level. She has completed MCA in 2005and M. Phil. in 2010. She is pursuing Ph. D. from Rajasthan Vidhyapeeth University, Udaipur. She has attended 5 international conferences and 2 national conferences. She is a member of CSI. Her Research areas of interest are Ad Hoc networks, network security and security protocols.

Prof. S.S. Sarangdevot is Dean, Department of CS & IT, JRN Rajasthan Vidhyapeeth (Deemed) University, Udaipur, India. Presently he is the Vice-chancellor of the university. He is Ph.D. in Computer Science and 26 years of teaching and 21 years of research experience. He has published 8 books and 78 research papers in journal of national and international repute. His research areas of interest are Artificial intelligence and networking.