Varying Number of Nodes Based On Black Hole Attack For Routing Protocol In MANET

Payal Jain[1], Ashish Chaurasia[2], Ashok Verma[3]

[1]M. Tech Student, Dept of CSE, [2]Assistant Professor, Dept of CSE, [3]HOD, Dept of CSE

Gyan Ganga Institute Of Technology & Sciences, Jabalpur

Abstract - A mobile ad hoc wireless network is an autonomous system of mobile nodes connected through wireless links. The mobile nodes in the network coordinate among themselves for communication. Hence each nodes in the network is also expected to route packets for other nodes in the network. Due to unique nature of the network ad hoc networks are vulnerable to various attacks, Black Hole attack is one of the passive attack on ad hoc network. In this paper we compare the effect of Black Hole attack on two routing protocols which are AODV(Ad hoc On-demand Distance Vector routing protocol) and OLSR(Optimized Link State Routing protocol). These two routing protocols are based on routing information and update mechanism. OLSR is also known as a type of table driven routing protocol. AODV is also known as a type of on-demand routing protocol.

Keywords: MANET, AODV routing protocol, OLSR routing protocol, Black hole Attack, simulation.

I. INTRODUCTION

The security of an ad hoc network is very important phase of communication. The lack of any security thread makes the network weak for attack from malicious nodes. Black Hole attack is one of these attack, it is a passive attack. Black Hole attack uses the concept of dropping the data by generating the false route. It performs in following way: Black Hole node makes other nodes to believe that it is having a fresh routing path. Once Black Hole attack attracts other nodes then it starts dropping the data. In our study, we simulate Black Hole attack in MANET and compare their effect on the network performance. For simulation purpose we choose AODV and OLSR protocols.

A. AODV Protocol

AODV is an abbreviation of Ad hoc On-demand Distance Vector routing protocol. AODV uses an on demand routing approach for finding paths from source node to destination node. That means the route established only when needed. In AODV protocol the nodes stores the information about next node corresponds to each flow of data transmission.

In AODV protocol, the source node floods the Route-Request packets in the network when a route is not available for destination node. It may obtain multiple routes to destination from a single Route-Request packet. A node update its path information towards destination node only if the destination sequence number of the current packet received is greater than the last destination sequence number stored at the node. Destination source number shows the freshness of the route. When an intermediate node receives a Route-Request packet it either forward it to the next node or prepare for Route-Reply packet to the source node. The destination also sends a Route-Reply to the source node, in this case source receives multiple Route-Reply packets then source node itself decides the shortest path towards the destination node. All the intermediate nodes between the path from source to destination node needs to update their route information if it leads to shortest path.

The main advantage of this protocol is that the connection setup delay is less because route is established on demand whenever needed.

B. OLSR Protocol

The optimized link state routing (OLSR) protocol is a proactive routing protocol. Proactive protocols are also known as table driven protocol because there is a need of routing table which maintains the list of information of each nodes inside the network. This protocol employs an faithful link state packet forwarding mechanism which is called multi-point relaying. Optimization in this protocol is done by reducing the size of packets and the number of links used to forward the packets. The reduction of packets and links are done by declaring only a subset of the link in the link state update. This subset of links updates and assigned the task of packet forwarding are called multi-point relays. This optimization provides the facility of periodic link state update. The link state update optimization mechanism achieves greater efficiency when operating in highly complex network.

OLSR uses three types of control packets which are as follows:

1. Hello

   This control message is forwarded for sensing the neighbor node and for calculation of multi-point relays.

2. Topology Control

   It is a signal for link state and used by multi-point relay for optimizing messages.

3. Multiple Interface Declaration

   This message consist a list of all IPs used by nodes in the network. This message can be transmit on one or more interfaces.

C. Black Hole Attack

Black Hole attack is a network layer attack. It can also be categorized as an active attack. In this attack a malicious node falsely promotes a good or fresh path to the destination node during the path finding process in the AODV protocol or in the route update messages in OLSR protocol. The intention of the malicious node could be block the path finding process or to intercept all data packets sent to the destination node.

II. RELATED WORK

In [1], Harjeet Kaur, Manju Bala and Varsha Sahni compares reactive routing protocol AODV, proactive routing protocol OLSR and hybrid routing protocol ZRP. In this comparison they found that AODV protocol is more effective than other two protocol without any black hole node. The performance parameter they choosen were throughput, end-to-end delay and packet drop ratio.

Irshad Ullah and Shahzad Anwar, in [2], the black hole attack is analyzed with four scenario with respect to end-to-end delay, network load, throughput. They found AODV is 10% more vulnerable to the black hole attack than other routing protocols.

The solution proposed in [3], D.B.Roy, R.Chaki and N.Chaki focuses on the requirement of source node to wait until it receives multiple Route-Reply packets. Its drawback is the existence of time delay because of waiting for multiple packets before checks for the authentication of nodes.

In research paper [4], Vandana Dahiya analyze the impact of Black Hole attack on various routing protocol to check the performance of the network. For simulation purpose NS-2 (version 2.35) network simulator has been used. The parameters used for performance measurement are end-to-end delay, network load and throughput.

The previous work done on security issues were based on reactive routing protocol. Very small attention is given on other routing protocols to study the effect of black hole attack in MANET. In previous researches only theoretical part can be shown, no implementation part has been done. Hense we have to implement the theory that AODV protocol is more vulnerable than OLSR protocol. There is a need to know the effect of black hole attack on both reactive (AODV) and proactive (OLSR) protocols. In previous simulation NS-2 simulator is used. In this study we use NS-3 (version 3.23) network simulator for simulation and python language is used as back end.

III. ANALYSIS

1. Black hole attack in AODV

In AODV, Black Hole node waits for neighboring node to forward the Route-Request message. When it receives that Route-Request message it immediately sends a false Route-Reply message to the source node giving the information that it has a fresh route towards the destination node. Hence the source node assumes that the route finding process is now complete and it starts sending the data packets to the malicious node by assuming that either the malicious node itself is a destination node or it forwards those data packets to the next node towards the destination but it doesn't forward the packets anywhere.

2. Black hole attack in OLSR

In Optimized Link State Routing (OLSR) black hole attack, a malicious node forcefully selects itself as Multi-Point Rely. Malicious node keeps its forwardness field to constantly in its HELLO message. So in this case, neighbors of malicious node would always select it as Multi-Point Route. Therefore the malicious node earns a favored position in the network which it efforts to carry out the denial of service attack.

IV. PERFORMANCE MATRICS

For the comparison of the two protocols under security issues, various performance parameters are needed. Few of them are mentioned as follows:

A. Transmitted bytes (Tx)

It is the number of bytes transmitted by the source node.

B. Received bytes (Rx)

It is the number of bytes received by the destination node.

C. Throughput

It is the ratio of number of packets received by the sink to the number of packets sent by the source node.

V. SIMULATION

The simulation is done with the help of NS-3(V-3.23) network simulator. NS-3 provides accurate implementation of the different network protocols. Implementation of routing protocols in NS-3 is written in python language in the backend and fore-end is Ubuntu linux12.04. For comparison between AODV and OLSR routing protocols we change the number of nodes in the network as 10, 20 and 30. Simulation time has been taken as 100 seconds. Transmission range of our network has been fixed to 250 meters. Mobility module in our program is constant mobility module.

Various simulation parameters are mentioned in the following table:

Simulator	NS-3(version-3.23)
Simulation time	100(s)
No. of nodes	10, 20, 30
No. of malicious nodes	5
Protocols	AODV, OLSR
Transmission range	250 meters
Data rate	1Mbps
Traffic	UDP
Channel	Wireless channel

VI. RESULT AND CONCLUSION

In the comparative studies of reactive routing protocol AODV (Ad hoc On-demand Distance Vector) and proactive routing protocol OLSR (Optimized Link State Routing) with black hole attack using performance parameter transmission bytes, received bytes, throughput, the performance of OLSR is best in presence of black hole attack as compare to AODV protocol. Figure 1 shows the comparative result of throughput in AODV and OLSR protocol when number of nodes are increased in the network.

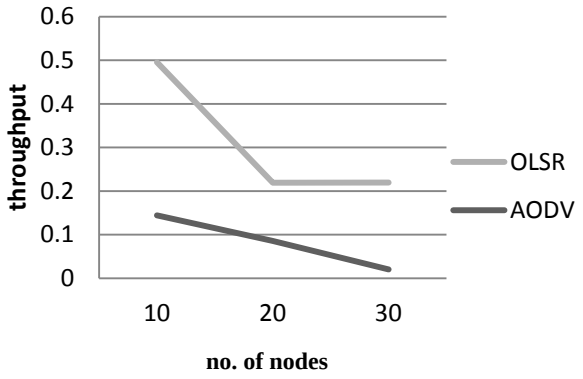

Figure1: Throughput in AODV and OLSR

Figure 2 shows the result of Received bytes (Rx) in AODV and OLSR protocol while increasing the number of nodes in the network.

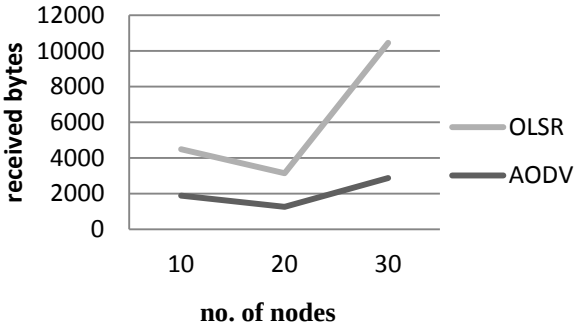

Figure: Received bytes (Rx) in AODV and OLSR

VII.FUTURE WORK

In this paper we study about the performance of AODV and OLSR protocol in the presence of black hole nodes by using the throughput , transmitted bytes, received bytes parameters. In our future work we enhance this study using other parameters as well such as packet drop ratio, end-to-end delay, network load.

REFERENCES

[1] Harjeet Kaur, Manju Bala and Varsha Sahni, ”Performance Evaluation Of Aodv, Olsr And Zrp Routing Protocols Under The Black Hole Attack In Manet”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, June 2013.

[2] Irshad Ullah and Shahzad Anwar, “Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols”, International Journal of Computer Science, May 2013.

[3] 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),April, 2009.
[4] Vandna Dahiya, "Analysis of Black Hole Attack on MANET Using Different Routing Protocols", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), October 2014.
[5] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",IEEE International Conference on Advance Information Networking and Application, April,2010.
[6] Vivek Thaper, Bindiya Jain and Varsha Sahni "PERFORMANCE ANALYSIS OF ADHOC ROUTING PROTOCOLS USING RANDOM WAYPOINT MOBILITY MODEL IN WIRELESS SENSOR NETWORKS" (IJCSE)International Journal on Computer Science and Engineering, August 2011.
[7] Raj Shree, Sanjay Kr. Dwivedi and Ravi Prakash Pandey "Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks",International Journal of Computer Applications, March 2011.
[8] Himani Yadav and Rakesh Kumar "Identification and Removal of Black Hole Attack for Secure Communication in MANETs",International Journal of Computer Science and Tele-communications, September 2012.
[9] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad "Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks" Emerging technology Trends in Electronics, communication and networking,IEEE First international Conference ISBN, 2012.
[10] Prem Chand and MK Soni "Performance Comparison of AODV and DSR on-Demand Routing Protocols for Mobile Ad-Hoc Networks" International Journal of Computer Applications, July 2012.
[11] Monika Verma, Dr. N. C. Barwar, "A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole Attacks in MANET", International Journal of Computer Science and Information Technologies, 2014.
[12] Neeraj Arora, Dr. N.C. Barwar, "Performance Analysis of Black Hole Attack on different MANET Routing Protocols", International Journal of Computer Science and Information Technologies, 2014.
[13] Neeraj Arora, Dr. N.C. Barwar, "Performance Analysis of DSDV, AODV and ZRP under Black hole attack", International Journal of Engineering Research & Technology (IJERT), April 2014.