Performance Analysis of AODV and OLSR under Black Hole Attack in MANET

Nancy Mittal
M.Tech Student
Department of Computer Engineering,
Punjabi University,
Patiala, India

Er.Lal Chand
Assistant Professor
Department of Computer Engineering
Punjabi University,
Patiala, India

Abstract- **MANET is Mobile Ad-hoc network, which is an infrastructure less network. MANET networks are vulnerable to various types of attacks and threats. MANETs has unique characteristics like dynamic topology, shared physical medium, distributed operations and many more. There are many attacks which effect the functioning of mobile ad hoc network. Security becomes the major issue with these attacks. Denial of Services which is commonly used to affect the network is one of the types of the network. Black hole attack is one of the major attacks in MANETs. Main goal of BH attack is not to send the packets to the destination. Comparison analysis of AODV and OLSR protocol under BH attack can be done on NS3 by using various design parameters.**

Keywords: MANET, Black hole Attack (BH), AODV, OLSR, NS3.

I. INTRODUCTION

MANET is Mobile Ad-hoc network, which is an infrastructure less network. The Latin meaning of Ad-hoc is “for this purpose” and Infrastructure less means that the network has no structure. A mobile ad hoc network (MANET) is a self-configuring network of mobile nodes. It lacks any fixed infrastructure and centralized administration. All network services of ad hoc network are configured and created on the fly [1]. Thus due to wireless link and the lack of infrastructural support, security in ad hoc network becomes weak.

II. ROUTING PROTOCOLS

A. Ad hoc on-demand Distance Vector routing protocol (AODV)

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes from source to destination on demand. AODV defines three types of control messages (Route Request (RREQs), Route Replies (RREPs), and Route Errors (RERRs)) for route discovery and route maintenance. It supports both unicast and multicast routing.

B. Optimized Link State Routing Protocol (OLSR)

It is a proactive routing protocol and a table driven protocol because it stores and updates its routing table permanently. In order to provide a route, OLSR keeps track routing table if needed. This protocol works in collaboration with other nodes in a WMN through the exchange of topology information. This exchange of information is done periodically. This protocol optimizes the flooding process and reduces the control message overheads by marking subset of neighbors as multi-point relays (MPRs). Two types of messages in OLSR, periodically broadcasts by each node: HELLO messages and Topology Control (TC) messages.

III. BLACK HOLE (BH) ATTACK

A black hole attack is an attack where the malicious node forcibly obtains the route with greatest sequence number and less hop count and subsequently overhears or drops all data packets [2]. Black hole attack is of two types:-

A. Single black hole attack:- A single black hole problem arises when one malicious node which utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets and does not forward packets to its neighbors.

B. Collaborative black hole attack:- A collaborative black hole problem occurs when more than one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets and does not forward packets to its neighbors or forward the packet to only malicious nodes.

IV. SIMULATION ENVIRONMENT

To justify our work we simulate mobile ad hoc routing protocols AODV and OLSR under BH attack using NS3. It is a very sophisticated tool and gives very user friendly Graphical User Interface. We are using the simulation scenarios with 25 no. of nodes.

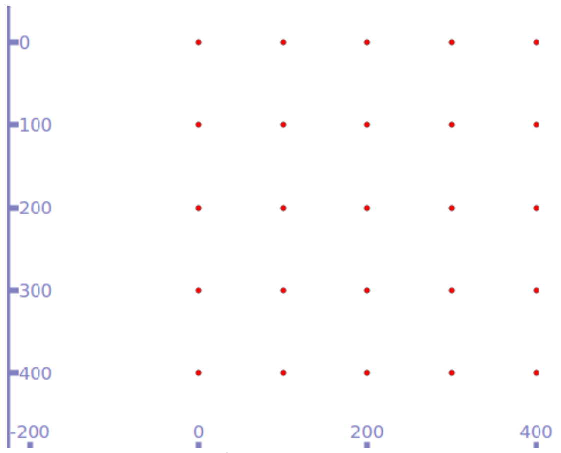

Figure 1: Scenario of network with 5*5 grid (25) nodes.

V. EXPERIMENT DESIGN AND RESULTS

A. Design Parameters

Parameters	Value
Simulator	NS3
Area	400*400 sq. units
Network size	25 nodes
Mobility model	Constant
Topology	Grid
Traffic Type	Packet sent
Address Mode	IPv4
Ad Hoc Routing Protocols	AODV and OLSR
Performance Parameters	Throughput, average delay, Packet Drop
Duration	49 secs
Value per Statistics	100

Table 1: Simulation Parameters

B. Results with Simulation parameters

1) Throughput: It is the total number of packets delivered over the total simulation time. It is represented in mbps.

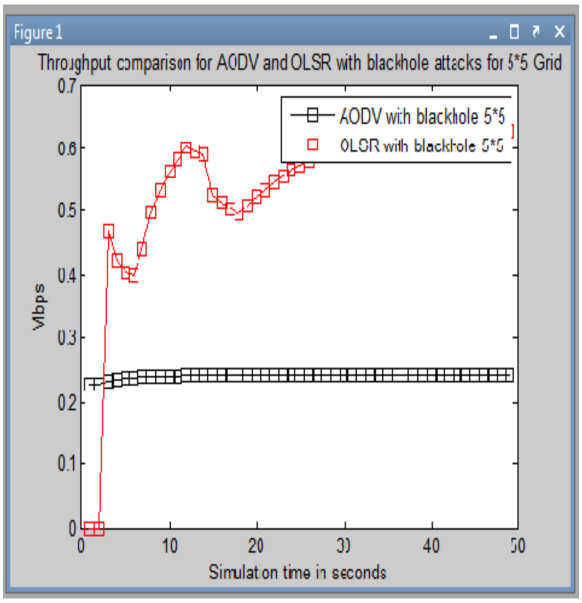

Figure 2: Throughput comparison of AODV and OLSR under black hole attack for 25 nodes.

Figure 2, shows that the throughput of the OLSR is more than the AODV protocol so AODV is more affected under Black hole attack.

2. Average Delay: It is the average end to end delay and the time taken by the packets to reach to the destination from the source node.

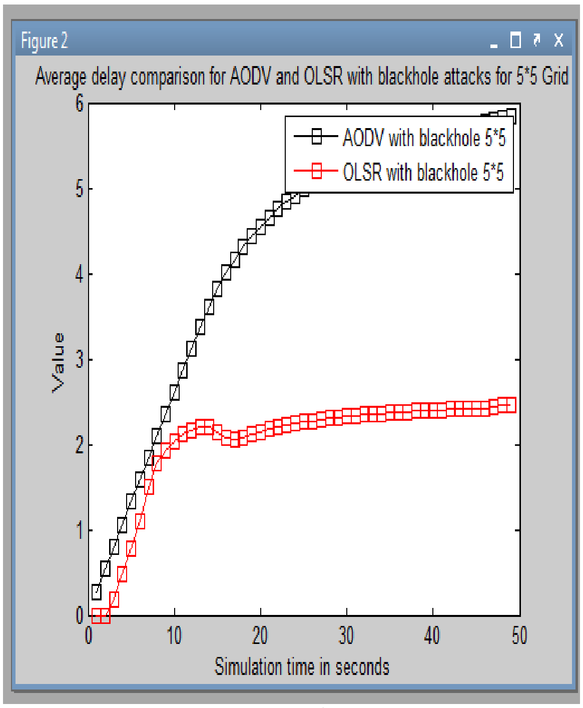

Figure 3: Average Delay comparison of AODV and OLSR under black hole attack for 25 nodes.

Figure 3, shows the Average Delay of the OLSR is less than the AODV so the packets send by OLSR protocol under black hole attack reaches fast to destination than the AODV.

3. Packet Drop: Packet drop is measured as a percentage of packets lost with respect to packets sent. This lost is due to the denial of service attack.

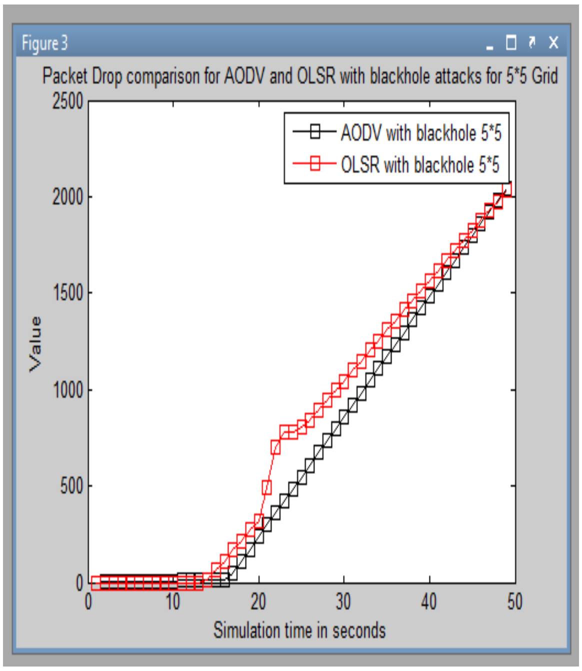

Figure 4: Packet Drop comparison of AODV and OLSR under black hole attack for 25 nodes.

Figure 4 shows the packet drop of OLSR is less than the AODV so packets in OLSR under black hole attack reaches more to destination.

VI. CONCLUSION

Effect of BH nodes on the performance of AODV and OLSR routing protocol is analyzed with the help of three parameters throughput, average delay and packet drop. From the results it is concluded that AODV adversely affect with the black hole attack.

OLSR performs better than the AODV with our simulation parameters.

VII. FUTURE SCOPE

In future we want to check the performance with more parameters for different protocols to get the better result.

REFERENCES-

[1] Aarti and Dr. S.S. Tyagi " Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and software Engineering, Volume 3, Issue 5, May 2013.

[2] NakkaNandini, ReenaAggarwal, "Prevention of black hole attack by different methods in MANET." Published in: International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015.

[3] Shilpi Jain, Sudhanshu Ranjan Choudhary, Shubham ," A Survey Of Single Black Hole Attack And Collaborative Black Hole In Manet", International Journal Of Science Technology And Management,volume no 6, issue no 4,2017.

[4] aPraveen K S, bGururaj H L*, cRamesh B, "Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols", International Conference on Computational Modeling and Security (CMS 2016),pp.325-330,2016.

[5] Arathy K Sa*, Sminesh C Na, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST), pp 264-271, 2016.

[6] Mohammad Hammoudeh, Fayez Al-Fayez, Huw Lloyd, Robert Newman, Bamidele Adebisi,Ahcène Bounceur, and Abdelrahman Abuarqoub, "A Wireless Sensor Network Border MonitoringSystem: Deployment Issues and Routing Protocols," ieee sensors journal, VOL. 17, NO. 8, pp.2572-2582, APRIL 15, 2017.

[7] Lovepreet Singh, Navdeep Kaur and Gurjeevan, "Analysis the Performance of MANET Protocol under Black Hole Attack for E-Mail Application", International Journal of Computer Applications (0975 – 8887) Volume 103 – No.12, October 2014.

[8] Neelam Janak Kumar Patel, Dr. Khushboo Tripathi,"Prevention and Detection of Black hole Attack in MANET using Modified AODV Protocol", International Journal of Advance Engineering and Research Development Volume 4, Issue 4, April -2017.

[9] Alamsyah, Mauridhi Hery Purnomo, I Ketut Edy Purnama, Eko Setijadi," Performance of The Routing Protocols AODV, DSDV and OLSR in Health Monitoring Using NS3", International Seminar on Intelligent Technology and Its Application, IEEE, 2016.

[10] Sathish M#1, Arumugam K#3, S.Neelavathy Pari#4 and Harikrishnan V S#2, "Detection of Single and Collaborative Black Hole Attack in MANET", IEEE WiSPNET conference, pp 2040-2043, 2016.

[11] Network simulator, Inc. "Network Simulator", Internet-www.ns3.com.