Black Hole Problem with OLSR Protocol in MANETs

Ankur Thakur
Department of Computer Science Engineering
RIMT, M.G.G, Punjab, India

Anuj Gupta
HOD, Department of Computer Science Engineering
RIMT, M.G.G, Punjab, India

Abstract - In this paper, we studied the optimized link state routing protocol, how it works, how malicious node attack the Protocol & we discuss various method that how we protect it from the attacker. All protocol has a problem of black hole. So we should have to protect it from the best routing protocol which having a less effect of black hole problem. We implement OLSR protocol with the help of OPNET tool & we find out that how attacker affects the nodes. The Simulation results show that how hello packet exchanges between the nodes & effect of black hole nodes in OLSR Protocol.

Keywords: MANETSs, OLSR, Malicious Nodes, OPNET.

I.INTRODUCTION TO MANETS

Mobile Ad-hoc Network is a collection of mobile nodes which are moving freely in the network. Manets is a self building dynamic wireless network. Wireless network is in very much demand in the last decade. Mobile Ad hoc network is a major area for the business environment these days. In Manets the nodes can act as a host/router or both at the same time. These nodes have the ability to configure themselves & they are deployed urgently without the need of any infrastructure [1]. MANETSs work without a centralized network where the nodes communicate with each other without any security. So security is the major issue for the mobile Ad-hoc nodes.

Securing an Ad-hoc network is very important these days. All the organisations focus on the security of Manets. Securing a mobile ad-hoc network is done by securing the routing protocol in the network layer. Routing Protocol tells about the topology and discovers the route for the nodes.

Routing protocol can be classified into three categories: Reactive Protocol (e.g AODV, DSR). In reactive protocol the route creation process will be asked only at the demand time. So, it reduces the control traffic. In proactive protocol the nodes exchange information with each other. So, route will be easily available at all the time. Proactive protocol is based on the periodic exchange of control message. Hybrid protocol is a combination of both reactive and proactive protocol. Hybrid protocol is adaptive in nature & user changes it as per his requirement [2][3].

II.OPTIMISED LINK STATE ROUTING PROTOCOL (OLSR)

The optimised link state routing protocol is a proactive protocol. In OLSR, the routes will be created with the help of nodes. Within the network all the routes will be maintained by the nodes. The nodes exchange information periodically when sending data or moving from one network to another network. OLSR is a table driven protocol & its main purpose is to update & maintained the table which having information regarding the control traffic generated & received by the nodes. OLSR protocol is not responsible for route traffic its mainly Purpose to maintain the routing table [4]. The OLSR Protocol is based on the two major concerns. First, HELLO message & second the topology control message. The neighbour nodes are finding with the help of exchanging HELLO message between the nodes. HELLO message also gives information about the topology used by the nodes. HELLO message also selects MPR (Multipoint Relay) from the neighbour. Second, the TC (Topology Control) message, the TC message contains the information of the MRP node that retransmits the data to further nodes. From MPR nodes all the nodes received the TC message. So that all the nodes having the information of the network topology and route will be created with the help of nodes [5][6].

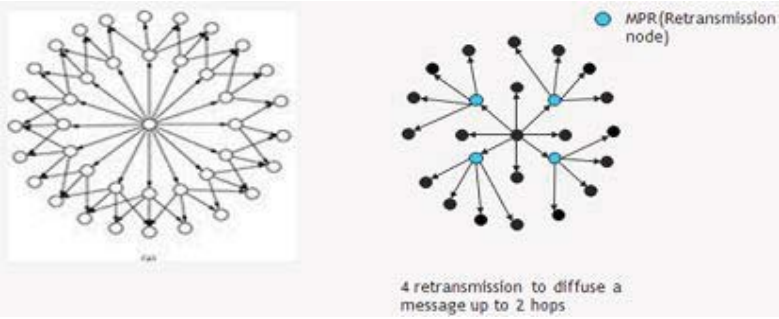

Fig 1.Multipoint Relay

III.BLACK HOLE ATTACK

In Black hole attack, an attacker sends a false routing information to the neighbour node that it is having the shortest path to reach the destination. So, the other nodes send information through the malicious nodes. Therefore, all the data will be captured by the attacker. An attacker destroys the data packet or modifies the data packet coming from the source node and sends it to the destination. The destination node cannot get that the data will be modified by the attacker [7].

IV.BLACK HOLE ATTACK IN OLSR

In OLSR, the information is exchanged between the nodes with the help of HELLO & TC message. The attacker sends a false HELLO message to the nodes & tells that they have a multiple nodes to send further data. In other word, the malicious node shows that it is having the multiple neighbour nodes for retransmitting the data. So the source node creates that node as a Multipoint Relay. When malicious node is selected as a MPR then all the information which is sent through the neighbour nodes of the MPR will pass through them & all the data will be captured [8].

V. SIMULATION

We have created a network with OLSR protocol in OPNET & checked that how black hole attack affects the OLSR protocol. In this, we create two scenarios. In the first scenario, as shown in Fig 2, we create a simple network with the OLSR protocol & check that hello message packet is exchanged between the nodes.

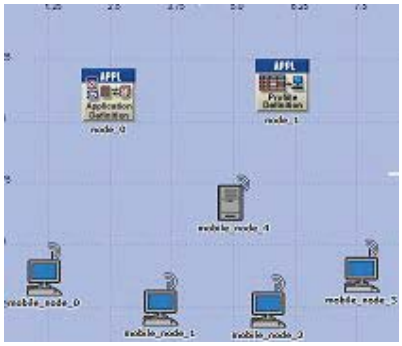

Fig 2. Mobile Nodes exchange Hello bit

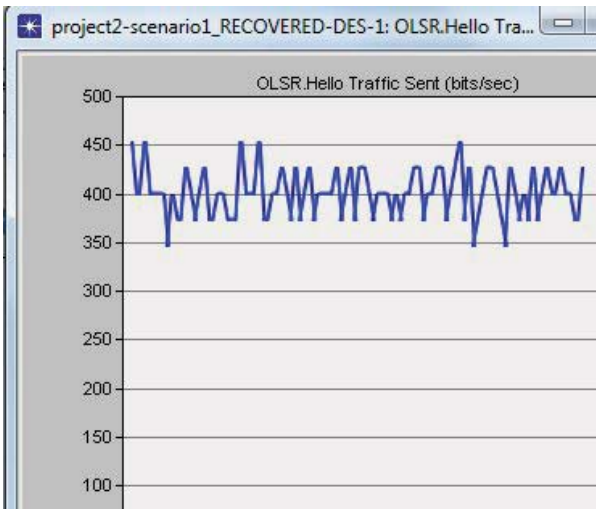

Fig 3. Hello Packet Exchange bits/sec

Fig 2. Manets network with 5 nodes and a mobile server is created in which all the nodes are connected to them. In this, two other nodes such as Application Configuration & Profile Configuration have been used. These are used to define the application definition & profile definition. OLSR protocol manages a network & shows how hello packet travels in the network. The result of scenario 1 is shown in fig 3 in which the hello message packet travels in the network with the 400b/s.

In scenario 2, a black hole attack is created in nodes to check how black hole affects our network. In scenario 2 a Manets network with OLSR protocol is created & a black hole effect was applied on it to check the HELLO packet exchange.

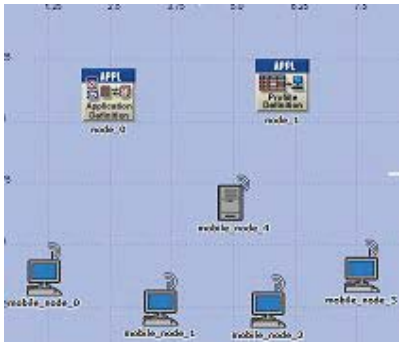

Fig 4 Manets Network with Black hole attack on node

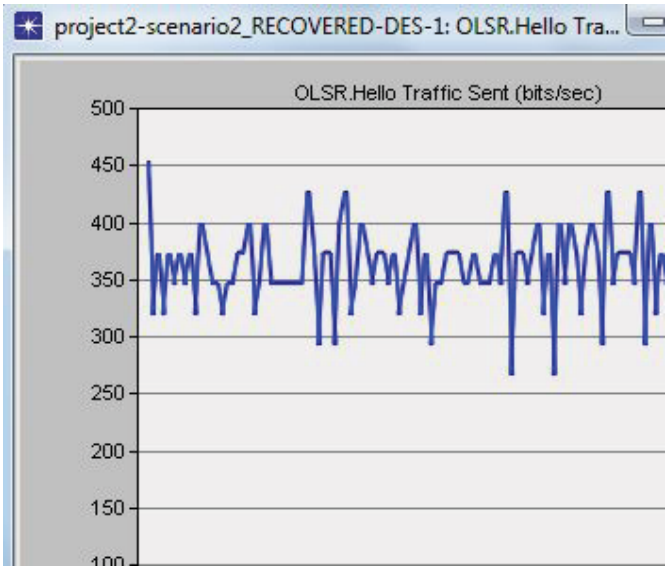

Fig5.Hello Packet Excahnge bits/sec with Black Hole

As it can be seen from fig 4, the node 3 acts as a Black Hole node in scenario 2. The node 3 increases its willingness to make MPR node & increases HELLO packet speed in the network. It has been checked that how black hole effects HELLO message packet in the network. In Fig 5 it is been shown that how the packet bit rate will be decreased. The data rate of HELLO message is 350b/s. The following table illustrate the both the scenario.

S.No	Factor	Scenario2(Black Hole)	Scenario 1
1.	Willingness	High	Default
2.	Hello Interval(sec)	4.0	2.0
3.	TC(sec)	10	5
4.	Neighbour Hold Time	6	6

The comparison of the results of both the scenarios it has been find out that the packet bit rate decreased on applying the black hole attack on the nodes. The difference between both the scenarios is shown in Fig 6.The data rate of HELLO packet is decreased from 400b/s to 350b/s. So the data can be protected from the attackers by applying Protection scheme on the Protocols.

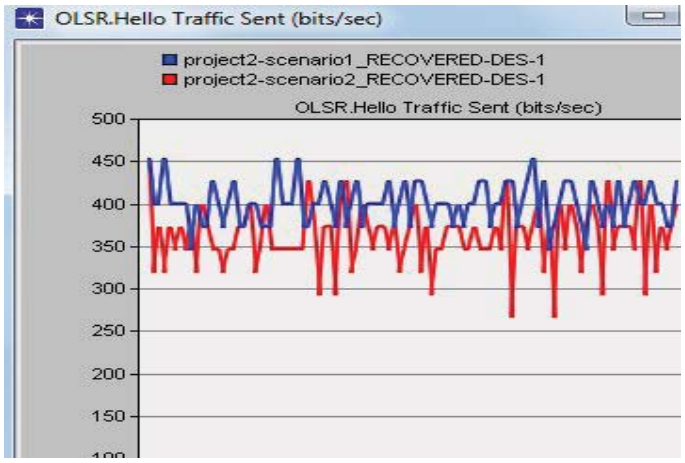

Fig 6. Comparison btw Simple & Black Hole Nodes for exchanging Hello Packet Interval(bits/sec)

VI. CONCLUSION

It can be seen that the performance of HELLO packet reduces when black hole attack is applied on node. Therefore, a network should be created which will have very less impact of attacks. In future scope, a work can be done on centralized network in manets for increasinge the performance of the network & reduced the black hole effect.

REFERENCES

[1] Anjaly Joy et al "Black Hole Attack & its Mitigation Techniques in AODV & OLSR", International Journal of computer Science & Technology , Vol 4, No.6, Pg. 740-745, June-2013.

[2] Manjeet Gupta ,Sonam Kaushik "Performance Comparison Study Of AODV ,OLSR and TORA Routing Protocol for MANETSS" International journal of Computational Engineering Research, Vol 2,issue 3, Pg. 704-711, May-June 2012.

[3] Devashish Rastogi, Sachin Ganu ," A Compartive Study of AODV & OLSR on the Orbit Tested", WINLAB,Rutgers University Technology Center of New Jersey North Brunswick, NJ 08902-3390, Pg. 1-7.

[4] C Jeyalakshmi et al, "An Experimental Study on Optimized Link State Routing Protocol for Underground Mines", Int. J. Computer Technology & Application ,Vol 3(6), Pg. 1886-1893, Nov-Dec 2012.

[5] P.Jacquet et al," Optimised Link State Routing Protocol For Ad Hoc Network", Hipercom Project , INRIA Rocqencourt, BP105, 78153 Le Chesnay cedex, France, Pg 1-7.

[6] Banoth Balaji et al, "Enhanced OLSR for Defense against Node Isolation Attack in Ad Hoc Networks", International Journal of Computer Science and Information Technology , Vol 4(6), 2013, Pg 1004-1009.

[7] Harjeet Kaur , Manju Bala , Varsha Sahni , "Study of Black Hole Attack Using Different Routing Protocols in MANETSS" International Journal of Advanced Research in Electrical Electronic and Instrumentation Engineering , Vol 2 , Issue 7, Pg. 3031-3039, July 2013.

[8] L. Sridhara Rao, MD.Ali Hussain , K.Satya Rajesh , "A Study on Black Hole Attack Against OLSR Based MANETSS" International Journal of Computer Networking, Wireless & Mobile Communication ,Vol 3 , Issue 1, Pg.157-164, Mar 2013.