Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Analysis of Black Hole Attack in OLSR Routing Protocol

[1]Hamela K and [2]Kathirvel Ayyaswamy,
[1]Research Scholar, MTWU, Kodaikanal and Assistant Professor, Government First Grade College, KGF, India
[2]Professor, Department of CSE, M. N. M. Jain Engineering College, Chennai, India

***Abstract*—** Routing is a standout amongst the most imperative difficulties with respect to portable unplanned nodes (MANETs). Having no fixed framework nodes with continuous topology changes, require routing conventions to work under participation of all nodes. In case, lack of co-operation of the node will reduced the performance and also leads to denial of service. Uncooperative conduct of nodes can result in form of attack against the network. One of the destructive attacks of MANET which will reduce the performance of the network is Black Hole Attack. The work of black hole attack is to deviate the network traffic towards the fake node and to drop the received data packets. In this paper we would like to analysis about Black hole attack in one of the proactive routing protocol namely optimized link state routing (OLSR) protocol.

Keywords— *MANET, OLSR, Black Hole attack*

I. INTRODUCTION

Mobile adhoc Networks (MANET) is self-making, self-managing and self-sorting out network structure, where an arrangement of self-inspired portable node can dynamically transfer information among themselves even without a fixed infrastructure. Each node in MANET also acts as a router allowing other nodes to communicate through them using their resources. The communication range of each device in MANET is very limited and therefore, most of the time an user can exchange packets only with any one of the devices in its transmitting or receiving range. These features are important for potential use in a wide variety of disparate situations like battlefield communications, emergency situations like earthquakes, vehicular traffic management [2 - 4].

It is further divided in Proactive Routing protocol, Reactive Routing protocol and Hybrid protocol. Reactive routing will recover the route when needed and it will be suitable for large scale applications. In proactive routing protocol, every node in a network topology keeps up at least one routing tables which are refreshed frequently. Each node sends a communicate message to the whole network get updated information from the neighbor nodes. Notwithstanding, it causes extra overhead cost because of keeping up-to-date information and therefore; throughput of the network might be influenced yet it gives the real data to the accessibility of the network. Hybrid routing protocols with hold the characteristic of both reactive routing protocol and pro-active routing protocol.

In this paper, we would like to focus on black hole attack in OLSR, which is one type of proactive routing protocol. In section II we discuss about literature review of related work and section III we describe the overview of OLSR. Section IV contribute towards the concept of black hole attack in MANET and we conclude with our future work in Section V.

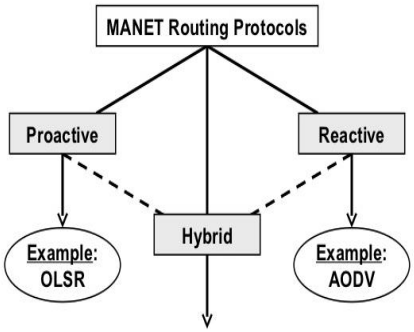

Fig 1. Types of MANET routing protocol

II. LITERATURE REVIEW

K. Sivagurunathan et al, analyzed the nature of black hole attack and wormhole attack in MANET. They propose a new mechanism called Advanced OLSR (AOLSR) protocol is acts as the proactive routing protocol as its nature. The experiment results show that our protocol achieve routing security with 22% increase in packet delivery ratio, 27% reduction in packet loss rate, 42% increase in throughput and 69% reduction in packet end to end delay than standard OLSR. This proposal was implemented in NS2.

Hancy Bhambri et at, proposed a method to prevent black hole attack in OLSR. The proposal was performed using fuzzy logic and Support Vector Machine algorithm. The simulation was done in MATLAB. The result shows that black hole exist in the network which can be optimized by using fuzzy logic and SVM algorithm.

Ankur Thakur et al, the proposal shows the implement of OLSR & effect of black hole nodes in OLSR Protocol. The result show the performance of hello packets during black hole attack. This model was implemented by OPNET simulator

III. OLSR: AN OVERVIEW

In OLSR, routes are immediately available when required by the nodes. It is a proactive routing protocol. OLSR deals with two kinds of control messages. One is Hello Message and another is Topology control message. Information about link states and the neighbor of the host's node is maintained in the Hello message. Neighbor node information of entire network topology is maintained by Topology control message. Multi Point Relay (MRP) plays a vital role in maintaining Hello messages in all the nodes . MRP is also constructed along with the Hello Message. Topology control maintains MPR selector information among the nodes.

A. Hello Message packet

A hello packet sends all the nodes in the wireless network, so that each node can maintain neighboring information and their state of their link to its neighbors. For these purpose hello packets are used. Every node has 1 hop and 2-hop neighbors. Using this information, MPR is selected. In neighbor table, each

node records the information about its one-hop neighbor and a list of two hop neighbors. It also contains holding time, sequence number values which specifies most recent MPR set.

B. MPR Selection Algorithm

One of the MPR selection[1] has two steps to be performed. Consider each point u has to select its set of MPR. Here one-hop neighborhood and two-hop neighborhood .

Step 1: Select the nodes of one-hop neighbor which covers isolated points of two hop neighbor.

Step 2: Select the nodes which was not selected in Step 1. Try to identify the node which covers highest number of points of two-hop neighbor and continue on till every points of two-hop neighbors are covered.

For a larger network, the selection of MPR will be very much useful, since it can avoid transmitting the same packets again and again. Multiple copies of packets for transmission can be avoided if we chose a particular node as MPR node. And using that MPR node we can transmit to all other neighboring node. Fig. 2 shows MPR selection for larger network [3].

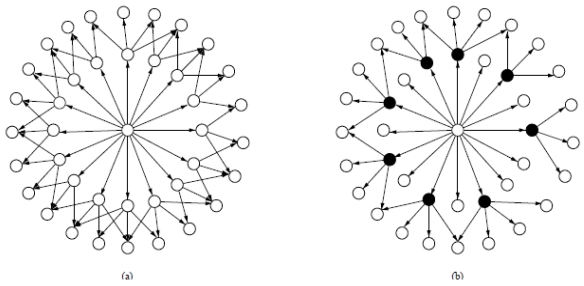

Fig. 2 Two neighbors and 'multipoint relays' (the solid circles) of a node. (a). Illustrates the situation where all neighbors retransmit a broadcast (b). Illustrates where only the MPRs of a node retransmit the broadcast

C. Topology Control Message

MPR selector data must be communicate to all nodes in the network, this should be possible by a Topology control message. The work of Topology control message is to construct intra-sending database. TC messages are sent just by MPR nodes periodically. TC message contains MPR selector, destination address, sequence number and holding time.

D. Routing Table

Every node keeps up a routing table to every recognized nodes in the network structure. Routing table will hold data with respect to neighbor table and the topology table. Routing table contains data like destination node address, next hop address and distance between nodes. Routing table is recalculated after each changes in the neighbor table or in topology table. Since OLSR is a proactive routing convention, routing table will hold data about all the existing nodes in the network structure.

IV. BLACK HOLE ATTACK IN OLSR

Nodes which go about as black hole send wrong hello messages. This black hole node extend themselves as node with more connections to its neighbors. By which, black hole node will be chosen as MPR node. There by black hole node will focus for TC message and attempt to catch the course of the network structure[7].

Activity performed by attacker nodes are

- attacker node broadcast fake route in the network to receive all the packets
- after receiving all the packets, then it will start dropping the packets.

Table 1: Hello message broadcasted to one-hop neighbor

Nodes	One-hop nodes
A	B,D,F
B	A,C,D,E
C	B,D
D	A,E
E	C,D
F	A

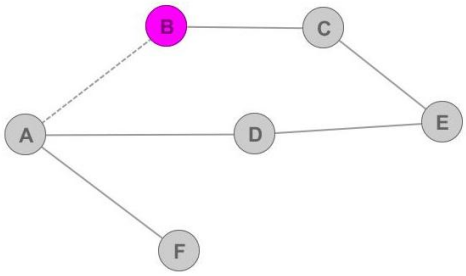

Figure 3: Black Hole attack in OLSR

Consider a network structure with B as attacker node and A as target node as shown in the figure. If hello message has being broadcasted to its one hope neighbor of all the nodes(Table 1). Since B is the attacker node, it will send a fake hello message to target node A and will inform that it has got many nodes as its one hop neighbor. Considering the message received from B node, target node A will select attacker node B as MPR. Since A node does not select D as MPR, these node will send TC messages not containing node A. And also the data packets send to E through D from node A will also be send through the attacker node B. There by attacker node B will totally block all the data packets broadcasted from A. Thus attacker node was able to capture the route and gain control over the connection from A to C and D.

CONCLUSION

In this paper, we have analyzed the Black hole attack on OLSR. 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 to overcome black hole attack in OLSR.

References

[1] P. Jacquet, P. Muhlethaler, T. Clausen, A.Laouiti, A. Qayyum, L. Viennot", Optimized Link State Routing Protocol for Ad Hoc Networks",*IEEE INMIC Pakistan 2001*, pp. 62 - 68.

[2] Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks", International Journal of Communication Networks and Distributed Systems, Vol. 7, No. 1 / 2, pp. 153 – 187, 2011.

[3] Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc

Networks", International Journal of Network Management, Vol. 21, No. 5, pp. 341 – 359, 2011.

[4] N.Kirubakaran and A.Kathirvel, "Performance Improvement of Security Attacks in wireless Mobile Adhoc Networks", Asian Journal of Information Technology, Vol. 13, No. 2, pp. 68 – 76, 2014.

[5] Ankur Thakur and Anuj Gupta, "Black Hole Problem with OLSR Protocol in MANETs", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4. Pp, 1-4, Sept 2014.

[6] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao,"A survey of black hole attacks in wireless mobile ad hoc networks",Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4

[7] K.Sivagurunathan , K.Manojkumar , D.Sounder , Midhun Sebastian,"Performance Evaluation of Advanced OLSR against Black Hole Attack and Wormhole Attack", International Journal of Innovative Research in Computer and Communication Engineering, ISSN ONLINE(2320-9801) PRINT (2320-9798),2017

[8] Hancy Bhambri and Gurinder Kaur Sodhi ijesird,"Preventation Of Black Hole Attack In Manet Over Olsr Protocol", International Journal of Engineering Science Invention Research & Development; Vol. III Issue I July 2016/1

[9] Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das,"A Survey of Black Hole Attack Detection in Manet",978-1-4799-2900-9/14/$31.00 ©2014 IEEE 202