International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 990 – 993

Preventing and Detecting Technique of Black Hole Attack in MANET AOMDV

Kavita Rani
M.Tech Scholar, Department of Computer Science & Engineering OITM Juglan Hisar (Haryana)

Surender Singh
Asst. Professor, Department of Computer Science & Engineering OITM Juglan Hisar (Haryana)

Abstract: **-** There are basically two types of black hole attack i.e. internal black hole and External black hole attack. Black hole is a malicious node that wrongly replies for some route requests without having active route to particular destination and drop all the getting packets. If these malicious nodes work jointly as a collection then the damage will be very risky. This type of attack is called cooperative black hole attack. Black hole attack is a type of active attack. Black hole attack can arise when the malicious node on the path attack the data transfer and purposely drop, delay or change the data transfer passing through it. Black hole node treats itself as a trusted node. Some attack drops the packets in the network and some are modify the packets. Study define the black hole node send false routing information, claim that it has a best route and cause additional good nodes to route data packets through the black hole node.

***Keywords*:-** *MANET, AOMDV , BLACK hole attack, MN-ID*

*****

I. INTRODUCTION

A mobile ad hoc network is a self-adjusting and dynamic network in which two or more nodes that can communicate with each other directly [8]. All the nodes leave or join the network anytime and anywhere without help of central control in the network [8]. Every node in an ad hoc network must be prepared to forward packets for other nodes. Thus, every node acts both as a router [11]. Each node finds a path to transfer the data using routing protocols [11]. The dynamic nature of MANET allows nodes to join or leave at any time that increase the chances of attack [7]. This network is decentralized in which nodes are adjusting everything like message delivery and network organization [39]. MANET is open medium network in which chances of attack is very high [37]. Some attack drops the packets in the network and some are modify the packets [39]. There are different characteristics which is a challenge in MANET include bandwidth issue, dynamic topology, restriction on the size of device [15].

Mobile ad hoc network is completely a wireless network that is very popular now days. Basically there are three types of wireless network that is ad hoc network, infrastructure network and hybrid network which is a combination of both networks [31]. An infrastructure network consists of wireless mobile device and one or more bridge, which attach the wireless network to the wired network. These bridges are called base stations. A mobile node within the network searches for the nearest base station (e.g. the one with the best signal strength), connects to it and communicates by it. The main fact is that all communication is taking place among the wireless node and the base station but not among dissimilar wireless nodes. While the mobile node is traveling around and all of a sudden gets out of range of the current base station, a handover to a new base station will let the mobile node communicate flawlessly with the new base station [3]. Infrastructure network is also called infrastructure basic service set. In this, we can communicate in two pass, in first pass frame are sent to access point and in second pass frame are sent from access point to target node.

II. AOMDV ROUTING PROTOCOL AND BLACK HOLE ATTACK

AOMDV is an ad hoc on demand distance vector routing protocol that is work on the basis of demand of route when it is required by the source node to the destination node [1]. AOMDV is improvement over Destination Sequence Distance Vector (DSDV) protocol. DSDV creating the small ad hoc network [11]. It requires universal distribution of connectivity information for right operation; it leads to frequent system-wide broadcast. so the size of DSDV ad-hoc networks is strongly restricted. When using DSDV, every mobile node also wants to maintain a whole list of routes for every destination within the mobile network. The benefit of AOMDV is that it tries to reduce the number of required broadcasts. It creates the route on an on-demand basis, as oppose to maintain a complete list of routes for each destination [11]. AOMDV does not maintain a routing table. This procedure is continuous until whether the destination node is found or the node that has a fresh enough route to the destination is found. Once finishing the route discovery process, the source node and the target node can be communicate and send the packets between them. When any node knows a link break or crash, Route Error (RERR) note is send to all other nodes [6]. Hello message is used for detecting and monitoring links to neighbors. Because of route error chances of attack is very high. Here we discuss the AOMDV Routing Protocol algorithm:

Step1: Source node sent RREQ to all neighbors.
Step2: Source node receives RREP from neighbors.

Step3: Source node select shortest and next shortest path based on the number of hops
Step4: Source node checks its routing table for single hop neighboring nodes only
Step5: If the neighbor node is in its routing table then sent data packet
Else
The node is malicious (black hole) and sends fake packets to that node.
Step 6: Invoke the route discovery notify all the neighboring nodes about the outsider.
Step 7: Add the status of outsider to the routing table of source node.
Step 8: Again send packet to neighboring node
Step 9: If step 5 repeats then broadcast the malicious node as black hole
Step 10: Update the routing table of source node after every broadcast
Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly. Black hole attack is a type of active attack [4]. Black hole attack can arise when the malicious node on the path attack the data transfer and purposely drop, delay or change the data transfer passing through it [9]. Black hole node treats itself as a trusted node. Black hole node send false routing information, claim that it has a best route and cause additional good nodes to route data packets through the black hole node. A black hole node drops all packets that it receives instead of normally forward those packets or message. There are basically two types of black hole attack i.e. internal black hole and External black hole attack [5]. Black hole is a malicious node that wrongly replies for some route requests (RREQ) without having active route to particular destination and drop all the getting packets. If these malicious nodes work jointly as a collection then the damage will be very risky. This type of attack is called cooperative black hole attack.

Black Hole

A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. We define the following conventions for protocol representation.

Internal Black hole attack

In this attack, malicious attack does not try to fit in to active route between source and destination [5]. It is present internally in the network, makes itself active route node in the network [3]. It will be able to attack as the data transmission start between nodes [5].

External Black hole attack

In this, malicious node is externally to the network and stay outside [3]. It creates congestion in the network and disturbs all the working of the network [3]. It can become an internal attack when it take control of internal malicious node and run it to strike other nodes in network [8].

III. PERFORMANCE PARAMETER

Throughput

Throughput is the rate of processing the data per second. In this, we count the transmission and receiving rate of data in the network per second. It can be calculated as:

Throughput = file size/ transmission time (bps)
Transmission Time = File size/ Bandwidth (sec)

Packet Drop Ratio

It is the total number of packet that is lost during simulation time. Lower value of packet drop ratio is improved the network performance. It can be calculated as:
Packet loss= no. of packet send- no. of packet received.

Packet Delivery ratio

It is the ratio of the no. of the delivered packet to the destination. Greater the value of pdr increase the network performance. It can be calculated as:

PDR= no. of packet receive/ no. of packet send.

IV. PREVENTION TECHNIQUE OF BLACK HOLE ATTACK

MN-Id Broadcasting Method

In this method, firstly we identify the malicious node (black hole) and once we recognize the malicious node then we save the MN- ID of this node and transmit to the whole network therefore whether the malicious node (black hole) take part in two or more path packets does not travel towards the malicious node (black hole) because whole nodes in the network should know about the malicious node (black hole). Therefore the packets transmitted through another path from source to destination [1].Here we shown the diagram which shows the concept of MN-ID method. In this MN-ID broadcasting method, here node 1 shows the source 1 and node 9 shows the target 1 and node 6 is represented as malicious node (black hole). When the source 1 transmit packets to target node 9. When packet reach on the node 6(black hole node), it will discard all the received packets from the node 1.

 ISSN: 2321-8169
990 – 993

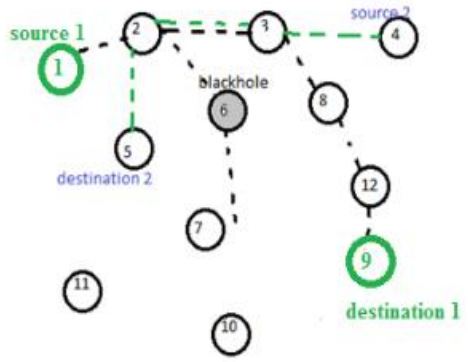

Fig. 1 MN-ID broadcasting method

Then the protocol discover an another path to target and broadcasting the MN- ID (that is node 6) to the whole nodes in the network. The actual shortest from node 4 to node 5 is 4-3-6-5. Whenever the packet transmit from node 4, the packets are not transmitted through the right shortest path because node 6 is a black hole (malicious node) and that particular node ID is broadcast to the whole network. Hence the packet broadcast takes place through the path 4-3-2-5 and arrive at right target node [1].

V. RESULT AND SIMULATION PARAMETER

The various parameters which are considered for network simulation is specified in the table 1.

Table 1. Simulation parameters

Number of nodes	9
Packet size	512bytes
Data rate	512b/s
No. of BH nodes	1

The result of various parameter are given below in which we compare the throughput vs. time; pdr vs. time etc which improvement on MN-ID method.

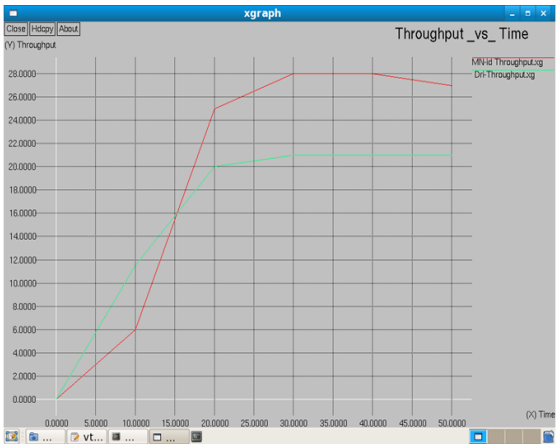

Figure 2. Throughput vs. time MN-ID broadcasting

As shown in figure 2 above as the time increase as well as throughput by MN-id broadcasting become better than DRI. That's why MN-id Broadcasting is better than DRI.

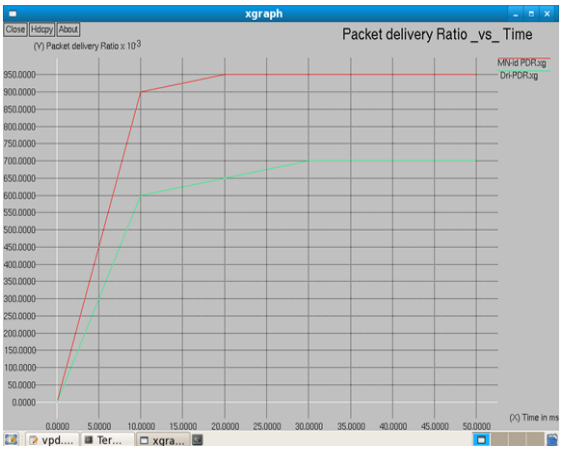

Figure 3. Pdr vs. time MN-ID broadcasting method

In this figure, the data routing information (DRI) received packet are decreased as compared with the MN-id broadcasting technique with respect to time. That means by this technique more data will be received by the receiver node, data packet will not be lost by the intermediate node by MN-id.

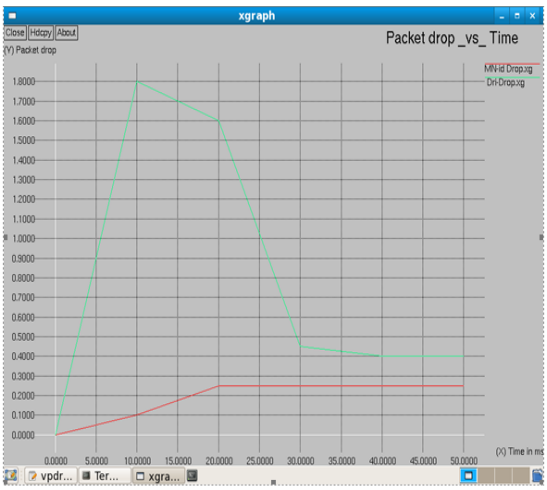

Figure 4 packet drops vs. time in MN-ID broadcasting method and DRI (existing method) method

As shown in figure 4, above that by the data routing information (DRI) packet drop ratio is increased as compared with the MN-id broadcasting technique with respect to time. That means by this technique more data will be losed by DRI.so MN-id is better than DRI.

VI. CONCLUSION AND FUTURE SCOPE

In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end to end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. The improved MN-ID broadcasting methods provide enhanced presentation of throughput, packet delivery ratio and decrease packet loss. Therefore improved MN-ID broadcasting method provides enhanced network performance and minimum packet loss in the packet transmission. After removing this attack from network, it will increase the packet delivery Ratio and decrease the packet dropping ratio and increase the security from black hole attack. In future, we try to more improve the MN-ID method which gives better results.

REFERENCES

[1] Funde N. A., Pardhi P. R., " Detection *& Prevention Techniques to Black & Gray Hole Attacks in MANET: A Survey*" , International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.

[2] Sharma R. , Shrivastava R. , " Modified *AOMDV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network*" , IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[3] Kalra J., Kaur R. , *" A Review Paper on Detection and Prevention of Black hole in MANET "* , International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 6, June 2014.

[4] Singh R. , Sharma A., Pandey G., " Detection *and Prevention from Black Hole attack in AOMDV protocol for MANET*" , International Journal of Computer Applications (0975 – 8887), Volume 50 – No.5, July *2012.*

[5] Baadache.A , Belmehdi.A , " Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks" , (IJCSIS) International Journal of Computer Science and Information Security, *Vol. 7, No. 1, 2010.*

[6] Phyu.T, Khin.E, " Impact Of black hole attack on AOMDV Protocol" , International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014

[7] http://ijcem.org/papers12011/12011_17.pdf

[8] Pooja, Kumar V. , " *A Review on Detection of Black hole Attack Techniques in MANET*" , International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 4, April 2014.

[9] Saini.A, Kumar.H, " Effect Of Black Hole Attack On AOMDV Routing Protocol In MANET" , IJCST Vol. 1, Issue 2, December 2010.