PROPOSED SOLUTION TO PREVENT BLACK HOLE ATTACK IN MANET

Reena Karandikar*

Rashmit Kaur Khanuja**

Surendra Shukla**

ABSTRACT

Mobile ad hoc network is a kind of wireless network. It is dynamic in nature and vulnerable for several attacks to be arising in it. Mobile nodes frequently disconnect and join the network, they can arbitrarily moves from one place to another. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path, this kind of nodes are known as malicious node. One of the attack is Black hole attack, it is a kind of active attack, it drops all the incoming packet between one source and destination. Black Hole nodes actually send a fake RREP packet and advertise itself as the shortest route is found and sender starts transmitting packets. But packet do not reach the destination node on account of this attack and data loss is also caused.

In our work we tried to secure the AODV protocol, so that it can withstand the attack by adding new secure Reply function to AODV protocol, we have seen that packet drop ratio is decreased by desirable amount. This will help to improve the performance of Mobile Ad hoc network and decrease the Packet loss ratio, which increased due to the attack.

Keywords: *MANET, AODV, ns2, Black hole attack, Malicious Node, Secure Reply function*

*Lecturer, K. C. Bansal Technical Academy, Indore, Madhya Pradesh.

**Assistant Professor, Chameli Devi School of Engineering, Indore, Madhya Pradesh.

I. INTRODUCTION

Wireless networks can be classified in two types: - infrastructure network and infrastructure less (ad hoc) networks. Mobile Ad hoc network belongs to the category of infrastructure less network. The word Ad hoc is a Latin word which means “for these only”.Nodes in this network are autonomous in it self, that they are not dependent on any infrastructure[1]. In this way, ad-hoc networks have a dynamic topology such that nodes are mobile in nature, so that they can easily join or leave the network at any time.

A major characteristics of MANET is its fully distributed architecture[2]. It can be set up anywhere,as there is no infrastructure or minimum infrastructure facilities required. There are some major characteristics of MANET [3]are as follows:-

- Communication via wireless means
- Nodes can perform the roles of both hosts and routers
- No centralized controller and infrastructure, intrinsic mutual trust
- Bandwidth-constrained, variable capacity links
- Energy-constrained Operation
- Limited Physical Security
- Dynamic network topology
- Frequent routing updates
- It can set up anywhere
- Multi hop Routing
- Device Heterogeneity

II. UNDERSTANDING BLACK HOLE ATTACK

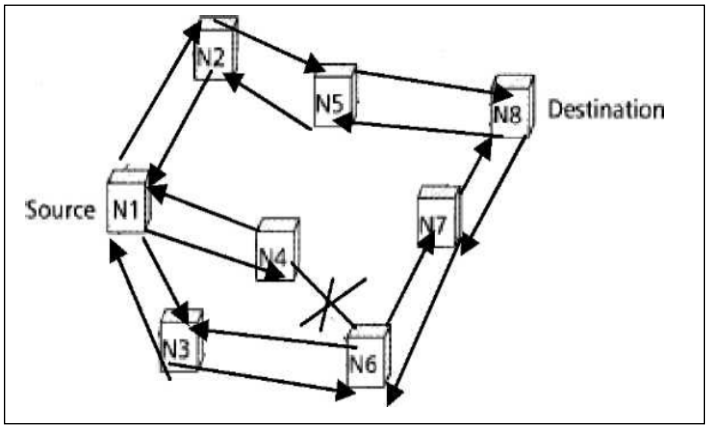
MANET is vulnerable for many attacks, one of them is Black hole attack. Black hole attack is a kind of active attack.In a black hole attack[4], malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, gives a high sequence number to make entry in the routing table of the victim node, before other nodes send a true RREP. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes access to all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole attack to real meaning which sucks all objects and matter.

There are two major behavior that Black hole node actually possess. They are as follows:-

- Black hole node advertise itself by showing larger or highest possible destination sequence no. as we know larger the sequence[5] no. means the route is fresh and latest for a particular destination. This way malicious node bluff the source node, who wants to initiate communication.
- It is a active DoS attack in MANET[5], which intercepts all incoming packets from an intended source. A black hole node absorbs the network traffic and drops all packets.
- The malicious node is supposed to be positioned in center of the wireless network.

To explain the black hole node behavior Fig.1 is drawn below.



In the Fig.1, we assume that node N4 is the malicious node[6]. Suppose node N1 has to send data packets to node N8, and starts the route discovery process. We assumed node N4 is a malicious node and according to the behavior of Black hole node which has no fresh enough route to destination node N8. However, node N4 claims that it has the shortest route to the destination whenever it receives RREQ packets, and sends the response to source node N1. The destination node and any other normal intermediate nodes that have the fresh route to the destination may also give a reply.

If the reply from a genuine node reaches the source node of the RREQ First, everything works as it is supposed to do; but the false reply RREP from malicious node N4 is probable to reach the source node first, in the case if malicious node is close to the source node. A malicious node does not need to check its routing table as it is known that it's sending a false RREP message; its response is probable to reach the source node first. This makes ensure the source node that the route discovery process is complete, then it discards all other reply messages, as it has got the shortest route reply(from malicious node) first and begin to send data packets over it. As a result, all the packets through the malicious node are intercepted or

dropped. The malicious node could be said to form a black hole in the network. In this way the malicious node can easily gulp a lot of network traffic to itself, and could cause an attack to the network with a big loss of data.

Proposed Solution for Black hole Attack- Mobile Ad hoc network is Vulnerable to many kinds of attack due to its dynamic nature, and the effect is actually taken up by any of the protocols being used for MANET. AODV protocol is among them, it is vulnerable to these kind of attacks. That's why we chosen AODV protocol to apply some preventive measure from Black hole attack. There are many other protocols that are being affected by these attack but AODV is major victim. To actually understand the proposed solution first we should know about the working of AODV protocol.

III. WORKING OF AODV PROTOCOL

AODV is basically on-demand routing protocol. Here nodes in the network do not maintain routing table prior to transmission start. When first packet is send, the routing table is updated because now it has got its first shortest path entry in routing table. AODV uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. AODV makes sure the route to the destination does not contain a loop and is the shortest path.

AODV builds routes using a route request / route reply query cycle.[6] When a source node require a route to a destination, it broadcasts a route request (RREQ) packet across the network. These broadcasted RREQ packet is received by each node present in the network during its travel each node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node simply reject the newly received RREQs. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node.

The RREP message is unicasted to the source node. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. It unicasts a RREP back to the source. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP having a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing table for that destination and begin using the better route.

IV. PROPOSED SOLUTION FOR BLACK HOLE ATTACK

In the proposed solution we have provided some addition features to SendReply function and ReceiveReply function of AODV protocol. which has a new valid route.For doing the changes we made a new function, named as sendSecureReply() and recvSecureReply().We have taken the idea from [7]the paper, where trust based defense mechanism is being used to prevent Mobile Ad hoc network from black hole attack. In the recvAODV function we have made some changes in type of incoming packet. We have changed recvReply (RREP) with recvSecureReply (SREP). The changes are shown as follows:

```
void
AODV::recvAODV(Packet *p) {
 struct hdr_aodv *ah = HDR_AODV(p);

 assert(HDR_IP (p)->sport() == RT_PORT);
 assert(HDR_IP (p)->dport() == RT_PORT);

switch(ah->ah_type) {

 case AODVTYPE_RREQ:
   recvRequest(p);
   break;
 case AODVTYPE_SREP:       // Adding secure reply
   recvSecureReply(p);          message type//
   break;
 case AODVTYPE_RERR:
   recvError(p);
   break;
---------------
------------
}
}
```

Fig.2 choosing secure message type in recvAODV function

After adding secure reply (SREP) we have made changes in send Reply and receive Reply function. There name will be then changed as sendSecureReply function and receivesecure Reply function. The changes we have made are as shown below:-

```
void
AODV::recvSecureReply(Packet *p) {
…….
…….
double delay = 0.0;
aodv_rt_entry *rtc;
aodv_rt_entry *rt0; // it is new path
rt0 = rtable.rt_lookup(rp->rp_dst);
if(rt0 == "0") {
   rt0 = rtable.rt_add(rp->rp_dst);
 }
if (rt0 == "nhn") {                    // for next hop node then valid route//
  rt0 =rtable.rt_add (rp->rp_dst);
}
if(rt0 == "inode") {                  // for intermediate node then valid route//
   rt0 = rtable.rt_add(rp->rp_dst);
 }

// I am not destination but check new route and shorter route
  if ((rt0->rt_seqno < rp->rp_dst_nhn ) ||   // newer route having next hop
node
       (( rt0->rt_seqno == rp->rp_dst_nhn) &&
       ( rt0->rt_hops > rp->rp_hop_count )))
```

Fig. 3 Adding new route to recvSecureReply function

In this function we have added a new route by adding new pointer to aodv routing table. The new route is actually the entry of that node which comes along the selected route. It is like if the request message is coming from the legitimate node (source) than definitely it is a secure request, but if message is coming from any other node which belong to the same route, may consist intermediate node, next hop node, companion node or any known node in the existing Ad hoc network . Then the route must be the secure route. But if a request message is coming from an unknown node which has never participated in any communication, then this route will not be the secure route, the request must be coming from a malicious node, selfish node or Black hole node.

V. RESULT

In this solution we have made three simulations. In first case we just understood how AODV works in Mobile Ad hoc network. Packet drop is generally happened in Ad hoc networks. When a mobile node become out of reach,then the packets will start dropping. Where percentage of packet drop is normally 20- 30%. In second simulation we made two tcl scripts.

These script take into account black hole aodv protocol, which we have added in ns directory. Here we have measured the packet loss due to black hole attack in MANET is increased by 40%. The graphs has drawn among three parameters send packets, received packets and dropped packets. Graph is shown in Fig.4 and data is shown in Table 1.

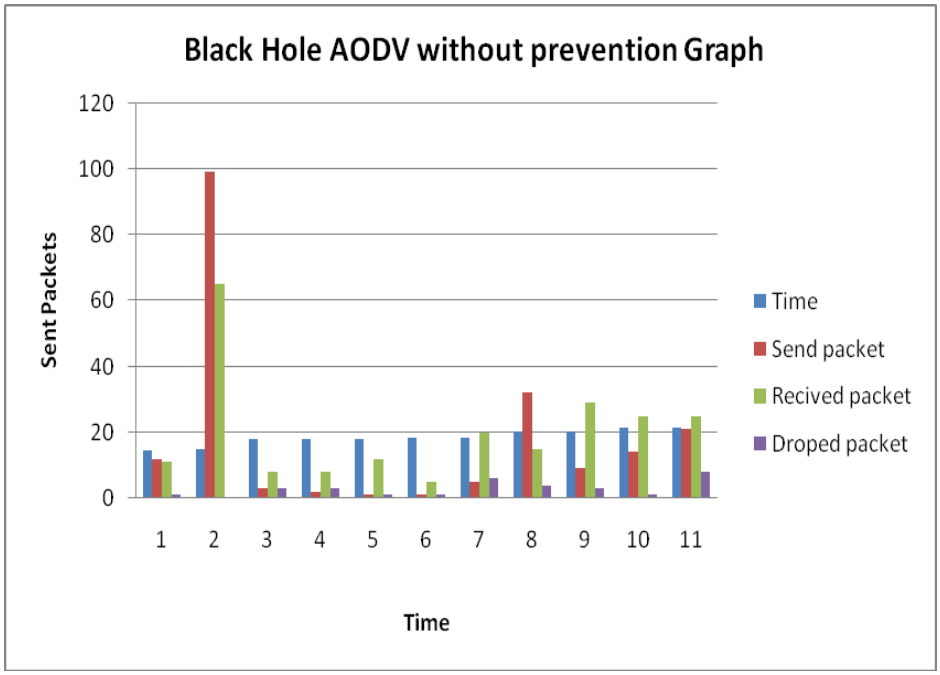


Fig.4 Showing graph to show black hole packet drop

Time(milli-seconds)	Send packet	Received packet	Dropped packet
14.34	12	11	1
15	99	65	0
17.88	3	8	3
18.111	2	8	3
18.112	1	12	1
18.33	1	5	1
18.4	5	20	6
20.26	32	15	4
20.27	9	29	3
21.56	14	25	1
21.57	21	25	8

Table 1. Data taken from blackholeaodv.tr file to draw Fig.4

Time(mili-Second)	Sent Packets	Received Packet	Dropped packet
2.556	3	1	0
2.557	0	2	0
2.558	2	0	0
2.559	0	2	0
2.562	2	1	0
2.563	5	1	0
2.57	11	8	2
2.573	15	10	5

Table 2. Data taken from blackholeaodv.tr file to show no. of packets send during attack

The data shown in Table 2 is, between very small fractions of time. As we can see where no. of sent packets are more, packet drop is high and where no. of sent packets are few, dropped packets are zero.

Total sent Packet	Total Received Packets	Total dropped Packets
1053	351	250
1108	397	275
1032	258	245
1052	407	199
1098	189	534

Table 5. Data taken from blackholeaodv.tr after prevention

In third simulation,we can see that after applying prevention mechanism black hole packet drop is reduced by 23%. This is half of black hole drops before prevention. So the prevention mechanism is working effectively to minimize number of packet drops in the Ad hoc network.

We can understand from the results; AODV network has normally 20 - 30 % data loss and if a

Black Hole Node is introducing in this network data loss is doubled to 50 - 65%. As 20 % data loss already exists in this data traffic, Black Hole Node increases this data loss by 20 %. When we used secureReply function in the same network, the data loss decreased to 23 %. These two results show that our solution reduces the Black Hole effects by 23 % as packet loss in a network.

VI.COCLUSION AND FUTURE WORK

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. Results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols should be tested as well to see the effect of black hole attack. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined. There are many techniques to prevent and investigate [8] AODV from the Black Hole attack. These could be tested to determine which one is the best to prevent the Black Hole.

We have analyzed effect of the Black Hole in an AODV Network. Our solution tries to eliminate the Black Hole effect by making an entry of secure route. This could be a possible solution to make secure entries in the routing table, where each node is known to rest of the nodes present in the Ad hoc network. If a new node wants to join this network, it has to ensure its authenticity. Then authenticity should be well tested and black hole must be detected at that point. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period.

REFERENCES

1. By http://www.dokurer.net/node/1
2. By Ankit jain, Arnika Jain, Pramod Kumar Sagar *"Various Security Attacks and Trust Based Security Architecture for MANET "* ,Global Journal of Computer Science and Technology,Page no.32, vol.10 Issue 14(Version 1.0) November 2010
3. Book Title "Ad Hoc Mobile Wireless Network- Age of Pervasive Mobile Computing and Networking" By C.K.Toh ,Chapter 1,2 Second Edition, Publisher Pearson

Education, 2002

4. The Ns-Manual By Kevin Fall and Kannan Vardhana , May 9, 2010
5. By Nital Mistry, Devesh C Jinwala, *Member, IAENG,* Mukesh Zaveri" Improving AODV Protocol against Blackhole Attacks" Proceeding of International MultiConference of Engineers and Computer Scientists 2010 Vol II, IMESC 2010, March 17-19 2010,Hong Kong
6. By Anu Bala, Jagpreet Singh and Munish Bansal "Performance Analysis of MANET under Blackhole Attack" First International Conference on Network and Communication 2009
7. By N.Bhalaji, Dr.A. Shanmugam "Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET" Journal of Advances in Information Technology, Vol.2, No. 2, May 2011
8. By Anu Bala, Rajkumari and Jagpreet Singh "Investigation of Black Hole Attack on AODV in MANET" Journal of Emerging Technologies in Web Intelligence, Vol.2, No.2, May 2010