Improve AODV Protocol For MANET Black Hole Attack Minimization

Rahul Rajendra Patil[1], Sunil G.Tamhankar[2]
[1]Dept of Electronics
[2]Assistant Professor, Dept of Electronics
[1, 2] Walchand College of Engineering, Sangli, Maharashtra 416415, India

Abstract- *Over the past few years wireless sensor networks has seen a tremendous growth with more and more use of mobile phones, smart devices leading to a growth in ad hoc network. Mobile Ad-hoc Network is an accumulation of the mobile nodes that does not have any fixed infrastructure. The MANET is self-configurable network, in which there is a constant connections and disconnections among the nodes of the network automatically at any point of time. In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its effect in the network for Minimization we modifying AODV Protocol.The proposed mechanism is implemented in NS-2.35.*

Keywords- AODV, Black hole, MANET, Performance Parameter

I. INTRODUCTION

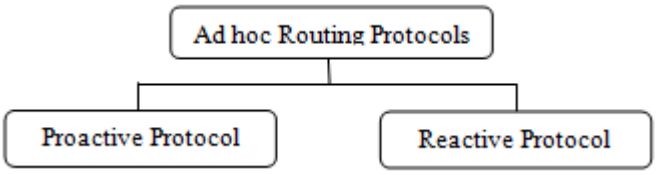
Mobile Ad-hoc Network is an accumulation of the mobile nodes that does not have any fixed infrastructure. The MANET is self-configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Routing of the data in the MANETs are done on the basis of the node discovery and then transmission i.e. the node receive the request message and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination and with help of route reply message the communication takes place. Each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network. For the connection between the nodes the routing protocols are required.In MANET these are such as AODV (Ad-hoc On Demand Routing protocol), OLSR (Optimized Link State Routing), DSDV (Destination-Sequenced Distance-Vector) etc.

MANET suffer from security attacks because of its features like open medium, dynamic change in topology, lack of central authority for the management and monitoring, distributed operation, lack of infrastructure. So MANET is susceptible to various attacks. In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it.

In this paper, We have suggested a solution to by pass the black hole node from the network. In particular, AODV protocol is most widely used in MANET for communication between the nodes. This solution route provides protection mechanism against black hole attack to improve the performance of the network. The analysis shows the impact of attack on MANET.

II. ROUTING PROTOCOLS USED IN MANET

Routing protocols are used to decide the path of the message packets from source to destination in a network by some set of rules. In MANET, various routing protocols are implemented as per the network circumstances and applications.



The two important routing protocols in MANET are **Proactive** and **reactive**. Proactive protocols have fresh lists of destinations with their routes and they periodically distribute routing table throughout the network. While the reactive protocol looking for a route only when needed by the network and they do so with the help of Route Request message.

AODV(Ad Hoc On-Demand Distance Vector Routing Protocol)

In AODVs, protocol development procedure is began by the node that wants to connect with the other node, it shows a HELLO idea after a particular time frame, thus a node keeps paths of only its next hop (Kumar & Sharma, 2013). Whenever a node want to connect with a node that is not its next door neighbor, it basically transmitted route request message (RREQ) massage that contain RREQ ID, location IP deal with, location sequence number, resource IP deal with, resource sequence number, and hop depend (Kumar & Sharma, 2013). It is designed to reduce needing network-wide, while showing it excessive. AODV does not sustain paths from every node to every other node in the network rather they are found as and when needed and are managed only provided that they are needed [5].

AODV is explained in RFC 3561 [6]. Its reactive protocol, when a node wishes to start communication with another node in the network to which it has no route; AODV will provide topology information for the node. AODV employ control messages to discover a route to the destination node in the network.

There are three kinds of control messages in AODV that are discussed as following:

1. RREQ:

When source node needs to communicate with another node in the network, it sends RREQ message. AODV broadcasts RREQ message, using spreading out ring technique. In every RREQ message, there is a time-to-live (TTL) value; the value of TTL expresses the number of hops the RREQ should be sent.

2. Route reply message (RREP):

A node that have a requested identity or any mediatory node that has a route to the requested node creates an RREP message and sends it back to the originator node.

3. Route error message (RERR):

During active routes, each node in the network keeps monitoring the link status to its neighbor's nodes. When the node discovers a link crack in an active route, RERR message is created by the node in order to inform other nodes that the link is down.

III. BLACKHOLE ATTACK IN MANETS

Wireless Ad-hoc Network has lack of infrastructure; it is easily attacked by various hackers or viruses. There are various type of attacks identified in Ad-hoc network. One of the attack is Black-Hole Attack. In black hole attack hacker or attacker target one of the nodes in the network and try to mess-up the whole communication. In this type of attack, the malicious node absorbs all the data directed towards it; starts dropping the packets and does not allow the data packets to pass through it. Black hole attacker node tries to pretend that only it has the fresh route to transfer data packets. But actually it is a hacker who hacks all packet data and starts dropping it in the network. As route discovery process in Ad-hoc network, source node is finding fresh path to destination with shortest distance and fastest route. At this time attacker node immediately gives response to the source node that it has the fastest and shortest path to destination with secure transmission. By pretending like this in front of source node, source node believes that it has the fresh path and trusts that node. Then it starts transferring all data packets to attacker node and assumes that it will deliver them to destination node as it has a true path for communication. This node intercept all the packet data as well as damage the node interface. In the black hole attack the malicious node wait for the neighbors to broadcast route request control message. As it receive the RREQ message it send a false RREP packet with the modified sequence number. After receiving the RREP message the source assumes that node is having the fresh route for the destination node.

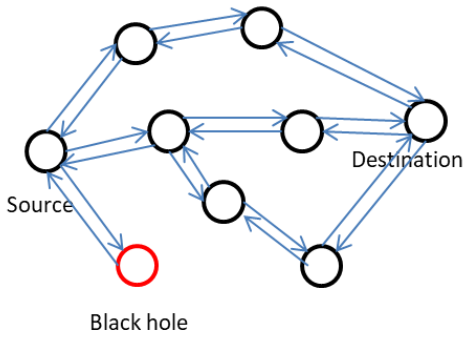


Fig. Black hole Attack in MANET

IV. IMPLEMENTATION

NS Network Simulator

NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols applications and traffic source behavior.

Implementing blackhole AODV protocol

In [7] Implementation of a New Manet Unicast Routing Protocol in NS-2 is described. To implement our contribution we have used the details explained in this paper. In our work, we have used the nodes that exhibit black hole behavior in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Black Hole they have to use a new routing protocol that can participate in the AODV messaging.

All routing protocols in NS are installed in the directory of "ns-2.35".We start with duplicating aodv folder in the folder ns-allinone-2.35/ns-2.35. Then we rename all the files in the folder as blackhole aodv instead of aodveg aodv.cc as blackholeaodv.cc.,aodv.h as blackhole aodv.h and so on. Then we change all classes, functions, structs, variables and constants from aodv to blackhole aodv names in all the files in the directory.

First modify recvfucntion **blackhole AODV::recv(Packet *p, Handler*)**

```
Void blackholeAODV::recv(Packet*p,Handler*) {
structhdr_cmn *ch=HDR_CMN(p);
structhdr_ip *ih=HDR_IP(p);
assert(initialized());
if(ch->ptype()==PT_AODV){
ih->ttl_ -= 1;
recvblackholeAODV(p);
return;
 }
if((u_int32_t)ih->saddr()==index)
forward((blackholeaodv_rt_entry*)0,p, NO_DELAY);
else
        drop(p, DROP_RTR_ROUTE_LOOP);
}
```

Second we change recvRequest function **blackhole AODV::recvRequest(Packet *p)**by doing modification at the end of this funcitonc hange paramameters eqno in function send Reply to some very large number as given below

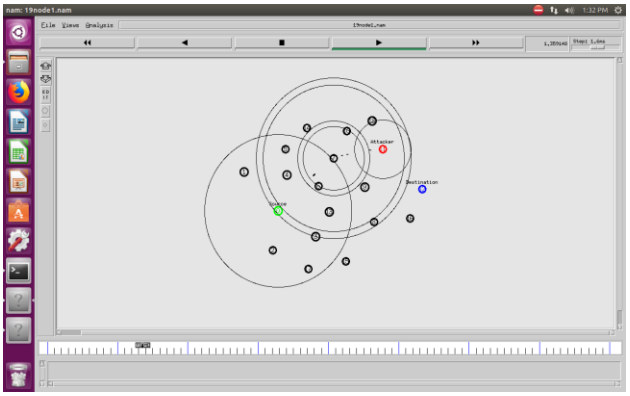
```
sendReply(rq->rq_src,     // IP Destination
 1,          // Hop Count
index,      // Dest IP Address
          4294967295,//HighestDest Sequence
        MY_ROUTE_TIMEOUT,  // Lifetime
rq->rq_timestamp); // timestamp

  Packet::free(p);
```

We added a blackhole agent in the scenario using the function

```
blackholeAODV {
setragent [$self create-blackholeaodv-agent $node]
}
```

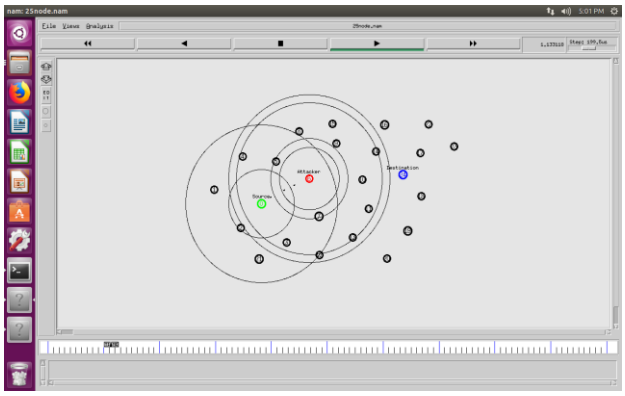
This function is predefined in NS-2.35 and can be used whenever we want to add a blackhole agent to create a blackhole attack. Further, we made changes to the ns-2.35/Makefile by adding prerequisite files. The changes are necessary for the above function to work. After all changes recompile ns2 open terminal go to ns-2.35 folder and type following commands and press enter make clean, make. We have now installed a new protocol in ns2. After implementation of blackhole AODV protocol. we have create some wireless scenarios with changing number of nodes 8,14,19 and 25. These are some wireless scenario with blackhole attack.

19 node wireless scenario with one blackhole node



This is 19 Node wireless scenario with blackhole node. In which blackhole node attract all the traffic towards blackhole node and drop it down without forwarding to destination. Green color node is Source node and Blue color node is destination node and Red color node shows blackhole node in this scenario. Figure shows that CBR packets are Dropped at Blackhole node.

25 node wireless scenario with one blackhole node



In this 25 Node Wireless scenario with Black Hole node. Figure shows that CBR packets are Dropped at the blackhole node as expected.

Implementing the solution in NS 2 by Modifying AODV Protocol

The Mechanism used for by pass the black hole attack is the process to ignore the first establishment route is added to the logical expression in routing update process. The main strategy is that when the network is under attack, multiple RREP from a different path is generated. This protocol assumes that the first RREP message that arrived at a node is from a malicious node, and hence the mitigation method in IDSAODV is to ignore this RREP to avoid false route entry being updated to the routing table. The implemented solution Minimize the effect of black hole attack on network performance instead of detection.

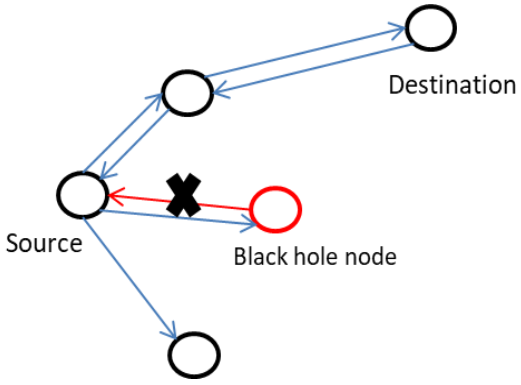


Fig. Black hole node respond to RREQ

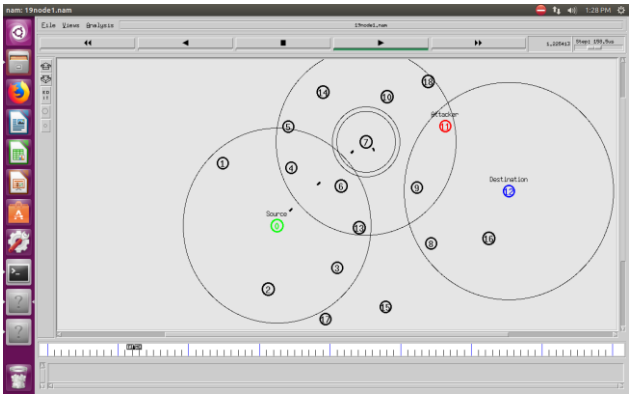
To evaluate effects of the proposed solution, we first needed to implement it in NS-2. Therefore, we cloned the "aodv" protocol, changing it to "idsaodv" as we did "blackholeaodv" before. To implement the black hole we changed the receive RREP function (recvRequest) of the blackholeaodv.cc file but to implement the solution we had to change the receive RREP function (recvReply) and create RREP caching mechanism to count the second RREP message.

In the "recvReply" function. It show show the receive RREP message function of the ids aodv is carried out.

```
idsAODV::recvReply(Packet *p) {
idsBroadcastRREP*r=rrep_lookup(rp->rp_dst);
if(ih->daddr()==index){
if(r==NULL){
count=0;
rrep_insert(rp->rp_dst);
} else {
r->count ++;
count = r->count;
}
}
else
{
Forward(p);
}
}
```

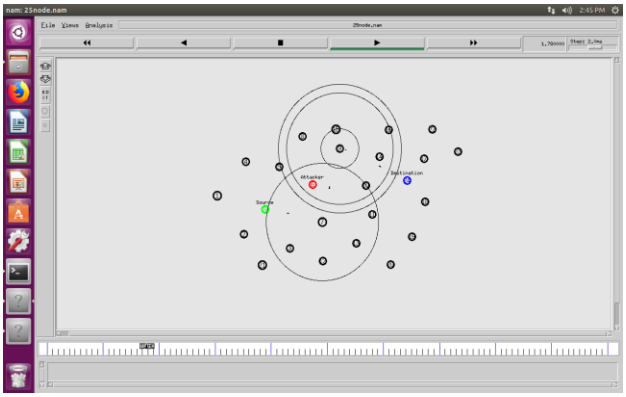
After all changes in idsaodv.cc file. We implement the some scenarios using idsAODV protocol. They provide the solution to blackhole attack in wireless network.

19 node ids AODV scenario with one blackhole node



Having implemented the ids AODV protocol in NS-2, we tried it in a tcl simulation. In the scenario of the simulation there are 19 nodes scenario. In this simulation ids AODV protocol is used instead of AODV for all nodes except the Red color black hole node. To change the AODV protocol to ids AODV we only change "*$ns node-config -adhocRoutingidsAODV*". When the simulation is compiled, we saw that sending node is sending the messages to Destination node properly. Figure shows that CBR packets are reaching the destination node as expected in which black hole attack node by pass and minimizes the result of attack on network performance.

25 node ids AODV scenario with one blackhole node



In this 25 Node Wireless scenario with Black Hole node. Using ids AODV protocol. Figure shows that CBR packets are reaching the destination node as expected.

V. SIMULATION RESULT

Different scenarios are used in our work: 8,14,19 and 25 AODV nodes without black hole attack; 8,14,19 and 25 blackhole AODV nodes with one black hole node; and 8,14,19 and 25 nodes using Modified AODV protocol. UDP connections are established between nodes. In all of the scenarios, the sending node is Green color node and the receiving node is Blue color node and packets send from sending node to receiving node. In all Scenarios Number of Generated packets is 250 depends on dropped packets received packet may varied in different scenarios.

Table 1. Total Drop Packets Comparison

Number of Nodes	8	14	19	25
Without Blackhole	0	0	0	0
With One Blackhole	250	250	250	250
With Modified AODV	10	11	2	12

A] Packet Delivery Ratio:

It is defined as the ratio of the number of packets received at the destination as compared to the number of packets sent by the source node. It is calculated on the basis of the data packets generated and received in trace files. The awk script is used to process the trace file ang the result is generated.

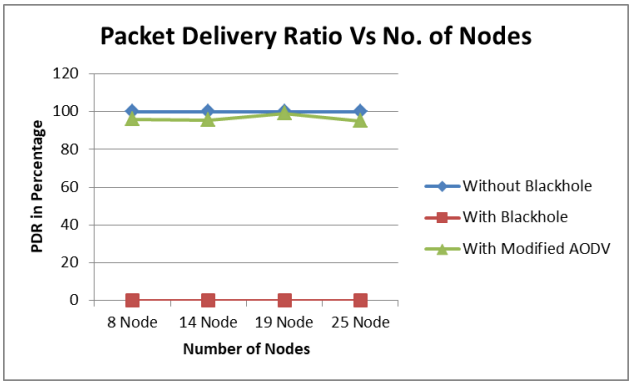
Packet Delivery Ratio= Σ Number of packets received / Σ Number of packets send

The comparison of AODV, Black hole Attack and Detection Mechanism is evaluated on the basis of Packet delivery ratio.

Table 2Packet Delivery Ratio(%)Comparison

Number of Nodes	8	14	19	25
Without Blackhole	100	100	100	100
With One Blackhole	0	0	0	0
With Modified AODV	96	95.6	99.2	95.2

Table 2.compares packet delivery ratio (PDR). As it shows, PDR is almost 100% before black hole attack that it means almost total packets sent by sender node are received by receiver node, but for network with black hole node PDR reduces to 0, that means almost whole of the packets sent by sender node are dropped by black hole nodes.



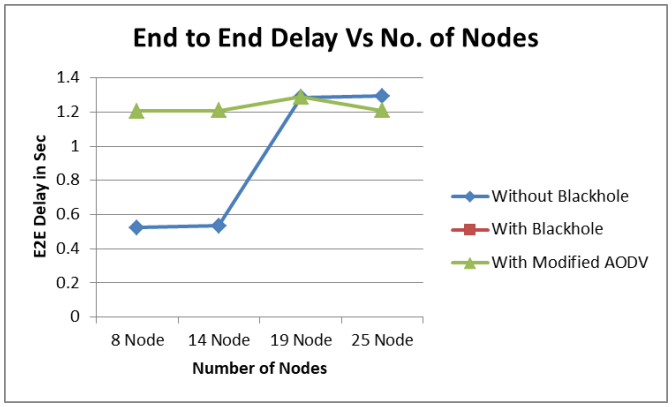
B] End to End delay :

It is described as the average time taken by the data packet to be transmitted from source to destination. It means that how much time the data packet is needed to be transmitted between source and destination across the network. The end to end delay is calculated for the successfully received packets at the destination. All values in Second.

Table 3 End-to-End Delay Comparison

Number of Nodes	8	14	19	25
Without Blackhole	0.5224	0.5345	1.2846	1.2923
With One Blackhole	∞	∞	∞	∞
With Modified AODV	1.2050	1.2086	1.2884	1.2076

Table 3. shows average end-to-end delay in different scenarios, as we can see average end-to-end delay infinite in scenarios with black hole attack, it is because of not a single packets received at Destination node during blackhole node. As no. of nodes increases then end to end delay also increased in the result.

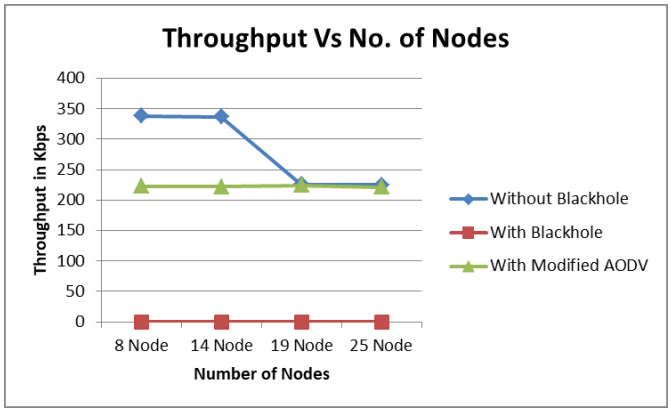


C] Throughput:

Throughput means the amount of data packets transmitted across the network from one end to another end in a given amount of time. It is calculated as the time taken on the average of the number of bits that are transmitted from the source to its destination. The throughput of detection mechanism is improved as compare to the black hole attack in AODV. The awk script is used to calculate the throughput using trace files. All values in Kbps.

Table 4 Throughput Comparison

Number of Nodes	8	14	19	25
Without Blackhole	338.0433	336.6175	225.7000	225.0546
With One Blackhole	0	0	0	0
With Modified AODV	223.1602	222.1959	224.1471	221.6495



V. CONCLUSION

In this Paper, Blackhole Attack are Simulated and performance of the different scenario is analyzed on the factors like packet drop, packet delivery ratio, end to end delay and throughput. The tool used is Network Simulator version 2.35. The simulation is carried out using AODV protocol, for different scenario and is compared for different number of nodes. Simulation results show the difference between the number of packets dropped 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. Implementing Modified AODV on the network decreases drop packets and improves packet delivery ratio. IDSAODV solution requests minimum modification on AODV.

VI. FUTURE SCOPE

In this system simulated the Single Black Hole Attack in the Ad-hoc Networks and investigated its affects when going for Multiple Black Hole attack in the Ad-hoc Networks will be future scope.

REFERENCES

[1] A survey of black hole attacks in wireless mobile ad hoc networks Fan-
Hsun Tseng Li-Der Chou and Han-Chieh Chao.

[2] H. Deng, W. Li, and D. Agrawal, Routing security in wireless ad-hoc network,IEEE Communications Magazine, vol. 40, no. 10 (2002).

[3] Ranjeet Suryawanshi, Sunil Tamhankar, "Performace Analysis and Minization of Black hole Attack In Manet" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue4, July-August 2012, pp.1430-1437

[4] Sushil Kumar, Deepak Singh Rana, Sushil Chandra Dimri, "Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.1, August 2015

[5] Gupta, N., & Shrivastava, M. (2013). An evaluation of MANET routing protocol. InternationalJournal of Advanced Computer Research, 3(1), 165_170.

[6] Ullah, I., & Rehman, S.U. (2010). Analysis of black hole attack on MANETs using different MANET routing protocols. A Mater Thesis, Electrical Engineering, Thesis No. MEE, 10, 62

[7] F. J. Ros and P. M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", December, 2004, http://masimum.dif.um.es/nsrt-howto/pdf/nsrthowto.pdf, 25 July 2005.