Ranjeet Suryawanshi, Sunil Tamhankar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1430-1437

Performance Analysis And Minimization Of Black Hole Attack In MANET

Ranjeet Suryawanshi*, Sunil Tamhankar**
*(Department of Electronics, Walchand College of Engineering, Sangli,
Maharashtra 416415, India
** (Associate Professor, Department of Electronics, Walchand College of Engineering, Sangli,
Maharashtra 416415, India

ABSTRACT

A Wireless ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. We simulated the black hole attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations.

Keywords - MANET (Mobile ad hoc network), AODV(On-demand distance vector routing protocol), IDS(Intrusion detection system).

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battle field or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To Support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector) [1], DSR (Dynamic Source Routing) and DSDV(Destination-Sequenced Distance-Vector).

Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface.

II. AODV ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) [1] is an on demand routing protocol which is used to find a route between the source and destination node as needed. It uses control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from the source to the destination. Header information of these control messages are also explained in [1] . When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, and received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination in its routing table. Fresh enough means that the intermediate node has a valid route to the destination established earlier than a time period set as a threshold. Use of a reply from an intermediate node rather than the destination reduces the route establishment time and also the control traffic in the network.

Sequence numbers are also used in the RREP messages and they serve as time stamps and allow nodes to compare how fresh their information on the other node is. When a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is assumed to be more accurate information and whichever node sends the highest sequence number, its information is considered most up to date and route is established over this node by the other nodes.

III. BLACK HOLE ATTACK

A Black Hole attack is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination.

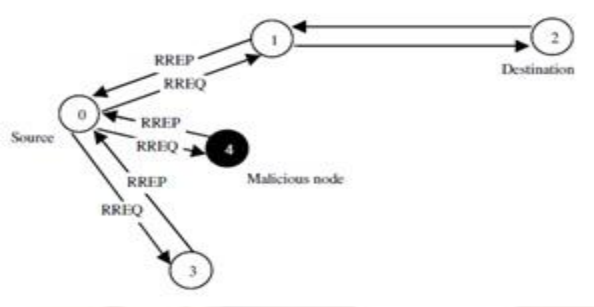


Fig1.RREQ Broadcast

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in Fig. 1 above, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on.

VI. EXISTING TECHNIQUE

Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks. H. Weerasinghe and H. Fu [2], introduces the use of DRI (Data Routing Information) to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes. The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication. The second drawback is over consumption of limited bandwidth. Cross-checking of the validity of routes contained in RREP message from an intermediate node is implemented by sending a FREQ (Further Request) message to the next-hop of the particular intermediate node. Sending additional FREQ messages consumes a significant amount of bandwidth from an already limited and precious resource.

H. Deng, W. Li and D. Agrawal [3], research is similar to Weerasinghe's technique except an additional weakness of inability to prevent attack from multiple black hole nodes. P. Raj and P. Swadas [4], proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast.

V.PROPOSED METHODOLOGY

5.1 Implementing BLACKHOLEAODV Protocol

To analyse the black hole behavior we modify the AODV protocol. All the routing protocols in NS are installed in directory of "ns-2.34".We start the work by duplicating AODV protocol and changing the name to "BLACKHOLEAODV". All the files that are labeled as "aodv" are changed to "blackholeaodv" such as blackholeaodv.cc, blackholeaodv.h, blackholeaodv.tcl, blackholeaodv_rqueue.cc, blackholeaodv_rqueue.h etc. in this new directory except for "aodv-packet.h". Because both AODV and Black Hole AODV protocol will send each other the same AODV packets. We have changed all classes, functions, structs, variables and constant names in all the files in the directory except struct names that belongs to AODV packet.h code.

The First file modified is "\tcl\lib\ns-lib.tcl" where protocol agent are coded as procedure. When the nodes use blackholeaodv protocol, this agen t is scheduled at the beginning of simulation and is assigned to the nodes that will use blackholeaodv protocol. The agent procedure for blackholeaodv is shown in figure 2.

Second file modified is “\makefile” in the root directory of “ns-2.34”. After all implementations are ready , we have to complile NS-2 again to create object files. We have added the lines show in figure 3 to the “\makefile”.

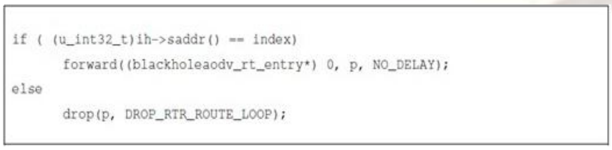
```
blackholeAODV {
set ragent [$self create-blackholeaodv-agent $node]
       }
Simulator instproc create-blackholeaodv-agent { node } {
       set ragent [new Agent/blackholeAODV [$node node-addr]]
       $self at 0.0 "$ragent start"             # start BEACON/HELLO Messages
       $node set ragent_ $ragent
       return $ragent
}
```

Fig 2. “blackholeaodv” protocol agent is added in “\tcl\lib\ns-lib.tcl”

```
blackholeaodv/blackholeaodv_logs.o blackholeaodv/blackholeaodv.o \
blackholeaodv/blackholeaodv_rtable.o blackholeaodv/blackholeaodv_rqueue.o \
```

Fig 3. Addition to “\makefile”

So far, we have implemented a new routing protocol which is labeled as blackholeaodv. But Black Hole behaviors have not yet been implemented in this new routing protocol.To add Black Hole behavior into the new AODV protocol we made some changes in blackholeaodv/blackholeaodv.cc C++ file.We will describe these changes we made in blackholeaodv/blackholeaodv.cc file explaining working mechanism of the AODV and Black Hole AODV protocols below. When a packet is received by the “recv" function of the “aodv/aodv.cc", it processes the packets based on its type.If packet type is any of the many AODV route management packets, it sends the packet to the “recvAODV" function .If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a Black Hole it drops all data packets .In the code below, the first “if" condition provides the node to receive data packets if it is the destination.The “else" condition drops all remaining packets.



```
if ( (u_int32_t)ih->saddr() == index)
       forward((blackholeaodv_rt_entry*) 0, p, NO_DELAY);
else
       drop(p, DROP_RTR_ROUTE_LOOP);
```

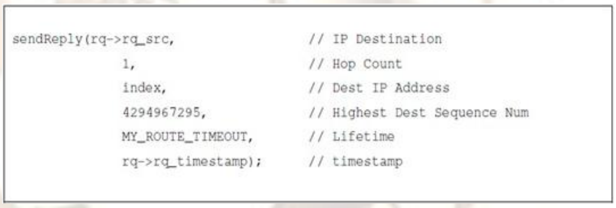
Fig 4. “If” statement for dropping or accepting packets.

```
case AODVTYPE_RREQ:
   recvRequest(p);
   break;
case AODVTYPE_RREP:
   recvReply(p);
   break;
case AODVTYPE_RERR:
   recvError(p);
   break;
case AODVTYPE_HELLO:
   recvHello(p);
   break;

default:
   fprintf(stderr, "Invalid blackholeAODV type (%x)\n", ah>ah_type);
   exit(1);
```

Fig 5. Case statement for choosing AODV control message types

If the packet is an AODV management packet, “recv" function sends it to “recvblackholeAODV" function. “recvblackholeAODV" function checks the type of the AODV management packet and based on the packet type it sends them to appropriate function with a “case" statement.For instance; RREQ packets are sent to the “recvRequest" function, RREP packets to “recvReply" function etc. case statements of “recvblackholeAODV" function is shown in fig 5.

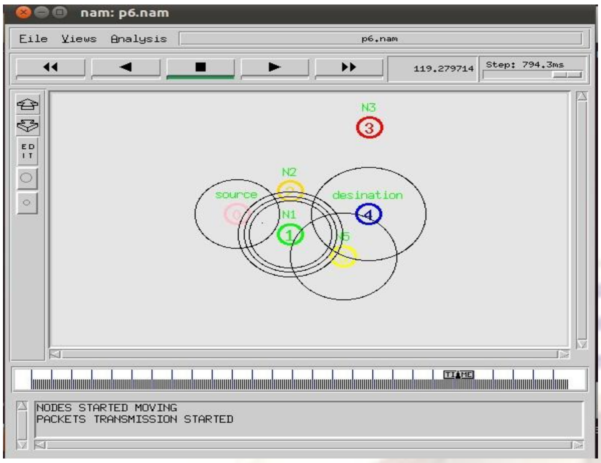


```
sendReply(rq->rq_src,                // IP Destination
          1,                         // Hop Count
          index,                     // Dest IP Address
          4294967295,                // Highest Dest Sequence Num
          MY_ROUTE_TIMEOUT,          // Lifetime
          rq->rq_timestamp);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

Fig 6. False RREP message of Black Hole Attack

In our case we will consider the RREQ function because Black Hole behavior is carried out as the malicious node receives an RREQ packet. When malicious node receives an RREQ packet it immediately sends RREP packet as if it has fresh enough path to the destination. Malicious node tries to deceive nodes sending such an RREP packet. Highest sequence number of AODV protocol is 4294967295, 32 bit unsigned integer value . Values of RREP packet that malicious node will send are described below. The sequence number is set to 4294967295 and hop count is set to 1. The false RREP message of the Black Hole Attack is shown in fig 6. After all changes are finished we have recompiled all NS-2 files to create object files.

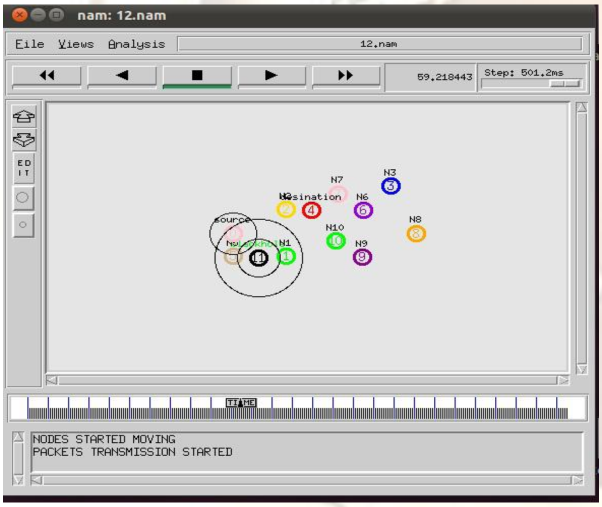
5.1.1) Simple Wireless Scenario



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

The first scenario is simple wireless scenario where there is no any Black Hole Node, connection between Node 0 and Node 4 is correctly flawed when we look at the animation of the simulation, using NAM .The packets are transmitted by source node to destination node via node 1 and node 5.

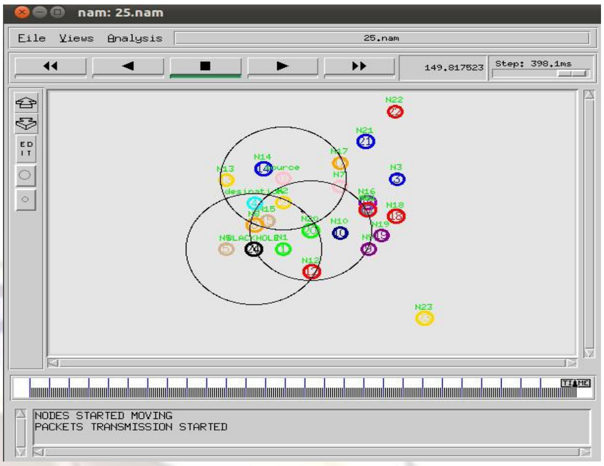
5.1.2) 12 Nodes with One Black Hole



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

In this scenario Black Hole nodes absorb all incoming packets from source. When source wish to send data on network it sends RREQ message on network .All the nodes on network receives that message, but Black Hole node immediately responds with RREP message to source. The source then starts sending packets to Black hole node assuming that it will transfer it to destination .But Black Hole nodes absorb all the packets without forwarding it to destination.

5.1.3) 25 Nodes with One Black Hole



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

In this scenario 24 Node is the Black Hole node which absorb all incoming packets from source without forwarding to destination.

5.2 Implementing IDSAODV Protocol

To minimize the effect of blackhole node and improve the packet delivery ratio we modify the AODV protocol as IDSAODV. Therefore, we cloned the “aodv” protocol, changing it to “idsaodv” as we did “blackholeaodv” before. As the black hole send an RREP message without checking the tables, it is more likely for the first RREP to arrive from the Black Hole. The IDSAODV Protocol will check the RREP packet from Black Hole node for minimum path to destination and maximum destination sequence number. The IDSAODV Protocol will discard the first RREP packet from Black Hole node and choose second RREP packet that comes from destination. The IDSAODV Protocol will find another path to destination ,other than Black Hole path. To analyse the black hole we changed the receive RREQ 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 check the RREP from Black Hole. To see the effect of IDSAODV we configure the nodes as IDSAODV Protocol and observed the performance parameters. We used same scenarios as we used for normal AODV and BLACKHOLEAODV to do the comparison.

```
void
idsAODV::rrep_insert(nsaddr_t id) {
  idsBroadcastRREP *r = new idsBroadcastRREP(id);
  assert(r);
  r->expire = CURRENT_TIME + BCAST_ID_SAVE;
  r->count ++;
  LIST_INSERT_HEAD(&rrephead, r, link);
}

idsBroadcastRREP *
idsAODV::rrep_lookup(nsaddr_t id) {
  idsBroadcastRREP *r = rrephead.lh_first;
  for( ; r; r = r->link.le_next) {
if (r->dst == id)
return r;
}
  return NULL;
}

void
idsAODV::rrep_remove(nsaddr_t id) {
  idsBroadcastRREP *r = rrephead.lh_first;
  for( ; r; r = r->link.le_next) {
  if (r->dst == id)
LIST_REMOVE(r,link);
delete r;
break;
}
}

void
idsAODV::rrep_purge() {
  idsBroadcastRREP *r = rrephead.lh_first;
  idsBroadcastRREP *rn;
  double now = CURRENT_TIME;
  for(; r; r = rn) {
rn = r->link.le_next;
if(r->expire <= now) {
LIST_REMOVE(r,link);
delete r;
}
}
}
```

Fig 7. RREP Caching Mechanism

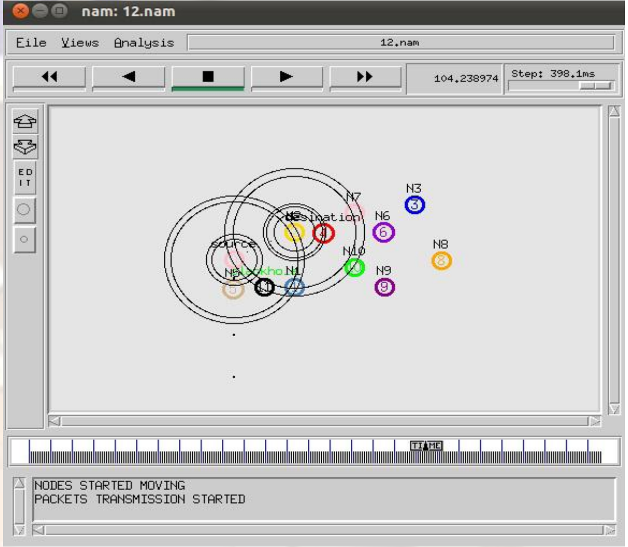
The RREP chaching mechanism is shown in fig. 7. “rrepinsert" function is for adding RREP messages, “rrep lookup"function is for looking any RREP message up if it is exist,“rrep remove" function is for removing any record for RREP message that arrived from defined node and purge" function is to delete periodically from the list if it has expired. We chose this expire time “BCAST ID SAVE" as 6.

```
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;
       }
       UPDATE ROUTE TABLE
   } else {
       Forward(p);
   }
}
```

Fig 8. Receive RREP function of IDSAODV

In the “recvReply" function, we first control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived .If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is cached before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbor. Figure 8 shows how the receive RREP message function of the idsaodv is carried out.

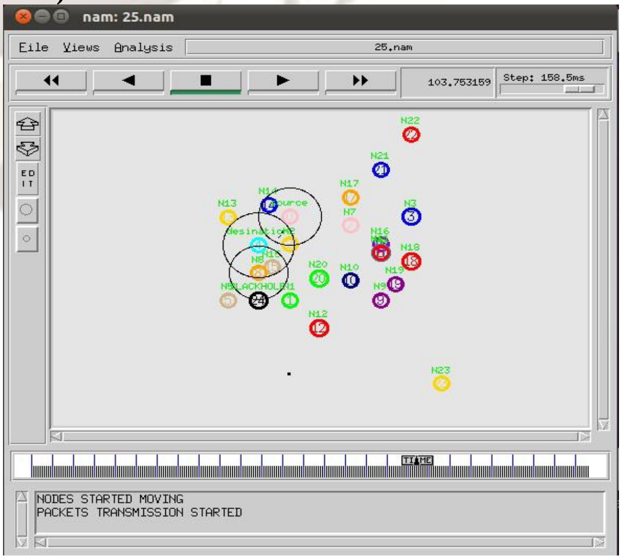
5.2.1) 12 Nodes with IDSAODV



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

This is the scenario with IDSAODV. We use same scenario as we used for BLACKHOLEAODV ,here we configure nodes as IDSAODV instead of AODV . In IDSAODV the source node will check RREP from Black Hole node for maximum sequence number and minimum route to destination ,it discard the message and find other route to destination. The Packet Delivery Ratio is improved by 73 % for 12 node scenario.

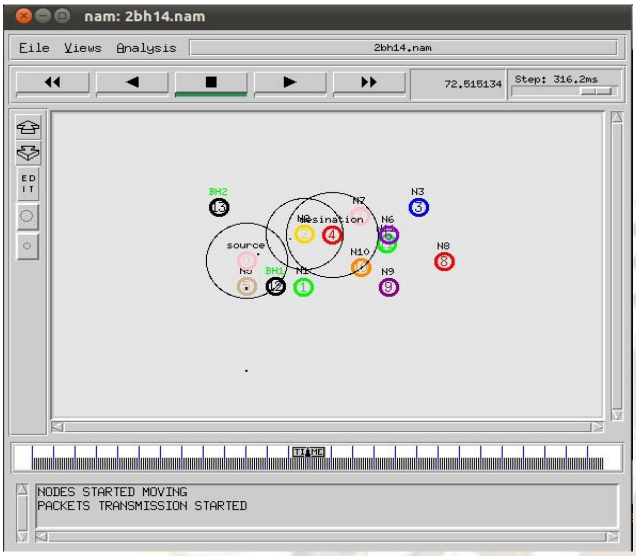
5.2.2) 25 Nodes with IDSAODV



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

This is the scenario of 25 nodes with one Black Hole.The Packet Delivery Ratio for this scenario is 90%.

5.2.3) IDSAODV with Two Black Hole



```
NODES STARTED MOVING
PACKETS TRANSMISSION STARTED
```

VI. SIMULATION RESULT

6.1 Performance Parameters without Black Hole

Parameters	**12 nodes**	**16 nodes**	**21 nodes**	**25 nodes**
Generated Packets	13844	13935	13241	21411
Received Packets	13766	13867	13158	21357
Packet Delivery Ratio (%)	99.43	99.51	99.37	99.74
Data Packets	24203	24225	23891	23531
Control Packets	24151	24177	23784	23495
Total Dropped Packets	78	68	83	54
Control Overhead (%)	99.78	99.80	99.55	99.84
Average Throughput	387.19	390.07	370.18	600.18
Average Delay(ms)	209.03	208.85	211.57	133.30

6.2 Performance Parameters with Black Hole

6.2.1 With One Black Hole

Parameters	**12 nodes**	**16 nodes**	**21 nodes**	**25 nodes**
Generated Packets	10938	13125	6721	5601
Received Packets	0	0	0	4
Packet Delivery Ratio (%)	0	0	0	0.07
Data Packets	10810	13132	6727	5497
Control Packets	10810	13131	6726	5497
Total Dropped Packets	10938	13125	6721	5597
Control Overhead (%)	100	99.99	99.98	100
Average Throughput	0	0	0	1.420
Average Delay(ms)	0	0	0	147.1

6.2.2 With Two Black Hole

Parameter	**9 nodes**	**14 nodes**	**25 nodes**
Generated Packets	27345	10749	10938
Received Packets	0	0	11
Packet Delivery Ratio (%)	0	0	0.10
Data Packets	22419	10626	15777
Control Packets	22298	10626	15775
Total Dropped Packets	27345	10749	10921
Control Overhead (%)	99.46	100	99.98
Average Throughput(kbps)	0	0	3.89
Average Delay(ms)	0	0	65.20

6.3 Performance Parameters with IDSAODV

6.3.1 With One Black Hole

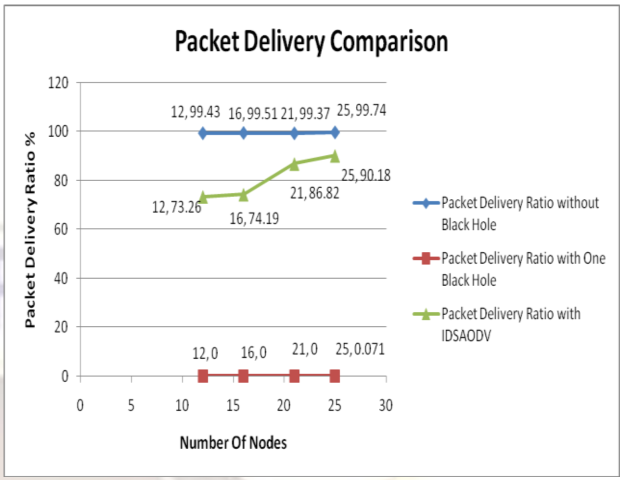
Parameters	12 nodes	16 nodes	21 nodes	25 nodes
Generated Packets	10938	13125	6721	5601
Received Packets	8014	9737	5835	5051
Packet Delivery Ratio (%)	73.26	74.186	86.82	90.18
Data Packets	16400	19950	12205	10140
Control Packets	16096	19636	11993	10140
Total Dropped Packets	2924	3388	886	550
Control Overhead (%)	98.15	98.43	98.26	100
Average Throughput	328.26	332.37	199.19	206.97
Average Delay(ms)	614.60	580.78	910.86	1266

6.3.2 With Two Black Hole

Parameter	14 nodes	25 nodes
Generated Packets	10749	10938
Received Packets	7912	8372
Packet Delivery Ratio	73.60%	76.5405%
Data Packets	16206	16800
Control Packets	15910	16766
Total Dropped Packets	2837	2566
Control Overhead	98.17%	99.79%
Average Throughput(kbps)	324.135	342.92
Average Delay(ms)	622.07	771.137

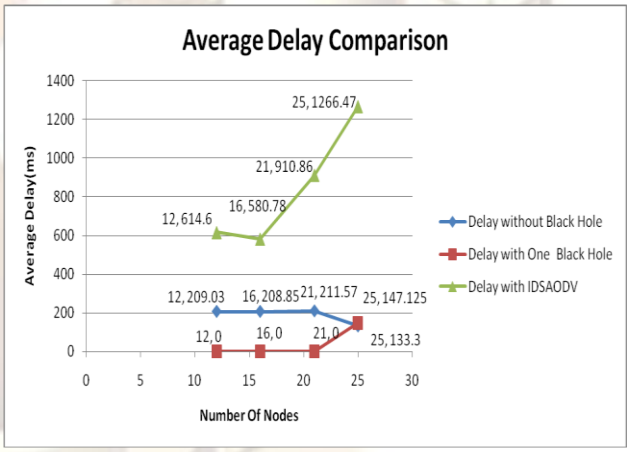
VII. SIMULATION GRAPH

7.1 Packet Delivery Ratio Comparison



For without Black Hole Scenario (Normal AODV) the Packet Delivery Ratio is between 98 to 99%.For with Black Hole Scenario (Standard Parameters) the Packet Delivery Ratio is almost 0%.For IDSAODV Scenario the Packet Delivery Ratio is improved between 73 to 90%.

7.2 Average Delay Comparison



For without Black Hole Scenario the Average Delay decreases as Generated Packets increases .For with Black Hole Scenario the Average Delay is 0 with Packet Delivery Ratio 0.For IDSAODV Scenario the Average Delay increases as Packet Delivery Ratio improves.

VIII. CONCLUSION

In this paper, we analyzed the effect of Black Hole in AODV network. For this we implemented an AODV protocol that behaves as Black Hole in NS2. Having simulated the black hole attack , we saw that the packet loss is increased in ad-hoc network. The Black Hole Attack affects the overall network connectivity and causes data loss in network.

Therefore to minimize the black hole effect, we implemented IDSAODV protocol .The IDSAODV protocol will improve the packet delivery ratio and minimize the data loss. The advantage of this approach is the implemented protocol does not make any modification in packet format hence can work together with AODV protocol. Another advantage is that the proposed IDSAODV does not require any additional overhead and require minimum modification in AODV protocol.

IX. FUTURE WORK

The proposed strategy is tested for standard parameters of black hole node such as maximum destination sequence number and minimum hop count. But the malicious node changes their strategy could be considered as future work.

X. REFERENCES

[1] C. E. Perkins, E. Beliding-Royer, and S. Das, "*Ad hoc on-demand distance vector (AODV) routing*," IETF Internet Draft, MANET working group, Jan. 2004.

[2] Hesiri Weerasinghe and Huirong Fu, *Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks*:Simulation Implementation and Evaluation International Journal of Software Engineering and Its Applications Vol. 2, No.3(2008)pp.39-5.

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

[4] P. Raj and P. Swadas, *A dynamic learning system against black hole attack in AODV based MANET*,IJCSI International Journal of Computer Science, Vol.2, (2009).

[5] Semih Dokurer, Y.M. Erten, and Can Erkin Acar- *Performance Analysis of Ad-hoc Networks under Black Hole Attacks* , Proc. of the IEEE SoutheastCon, pp. 148-153, 2007.

[6] Latha Tamilselvan and Dr. V Sankaranarayanan, *Prevention of Blackhole Attack in MANET*, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (Aus Wireless 2007).

[7] Yibeltal Fantahun Alem and Zhao Cheng Xuan , *Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection*,2010 2nd International Conference on Future Computer and Communication.

[8] Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao , *Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks*,2010 IEEE International Symposium on Parallel and Distributed Processing with Application.