Cope with black hole attacks in AODV protocol in MANET by end to end route discovery

Prof.D.S.Patil[1], Prof.A.M.Ghorpade[2]
[1]*(E&C Department, MMEC/ VTU, India)*
[2]*(E&C Department, MMEC/ VTU, India)*

ABSTRACT : *Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and capability. The black hole attack which is one of the major possible attacks in AODV routing protocol, in which intermediate node absorbs all the packets instead of sending those to desired destinations and behaves as a black hole and degrades the performance .*

In this paper AODV is modified in such a way that ,the provision of checking and sending route reply by intermediate node is cancelled. But the destination node after inspecting the RREQ can only reply with RREP to the source node. Thus only one reply message is received to source and that is only from the desired destination. Thus misbehaving of intermediate node i.e. black hole behavior can be reduced and network can be made more reliable and secured.

Keywords - *AODV, black hole , intermediate node ,MANET, black hole, RREP,RREQ.*

I.Introduction

An ad hoc network is a collection of wireless nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since nodes are not controlled by any other controlling entity, they have unrestricted connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network. In this multi hop architecture, each node works as a host and as well as a router that forwards packets for other nodes that may not be within a direct communication range. Each node participates in an ad hoc route discovery protocol which finds out multi hop routes through the network between any two nodes. These infrastructure-less nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Thus ad- hoc networks provide an extremely flexible communication method for any place where geographical or terrestrial constraints are present and any fixed architecture, such as battlefields, and some disaster management situations[1].The AODV(Ad-hoc on demand distance vector routing) protocol is vulnerable to the well-known black hole attack. A black hole is a node that always responds positively with a RREP (Request Reply)message to every RREQ(Request), even though it does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These black hole nodes may work as a group. That means more than one black hole nodes work cooperatively to mislead other nodes[2]. This type of attack is called cooperative black hole attacks which damage the networks performance seriously.

II.AODV Routing Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions[3][4]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A Route Request (RREQ) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back a Route Reply(RREP) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the „Destination Sequence number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the

RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a „fresh route□ and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node can carry out many attacks against AODV.

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. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of data packets, the Black hole node simply drops them, instead of forwarding to the destination[3][5].

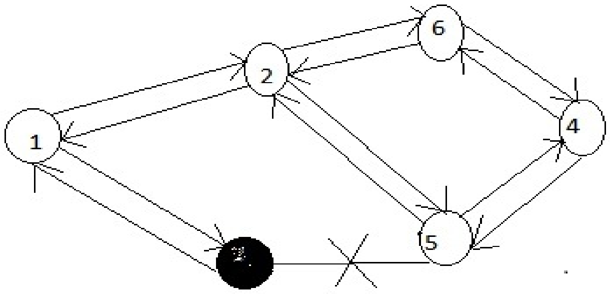


Figure 1:black hole node in the network.

IV.Modified AODV Routing Protocol

In modified AODV protocol, source node broadcasts the RREQ packet for route discovery . Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it does not check with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. Thus RREQ packet is routed till it reaches to the destination. After receiving RREP packet to the destination node, it replies with RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. Thus , only one RREP receives to source and that is from destination only. Since in this protocol, the intermediate nodes are not facilitated with replying the RREP packets , the probability of sending false RREP by intermediate nodes is reduced and black hole behavior of intermediate nodes can be restricted.

V.Performance Metrics

The following metrics are evaluated for existing AODV with black hole and modified AODV with black hole[5].

- *Packet Delivery Ratio*: which is the ratio of the data packets delivered to the destinations over the data packets generated by the traffic sources.
- *Average End to End Delay*: The sum of all possible delays caused by buffering during route discovery process, queuing at the interface queue, retransmissions at the MAC, and propagation and transfer through channel.
- *Control Overhead*: It is ratio of control packets to data packets.

VI.Simulation Environments and Results

In this section, we describe our simulation environment and report the simulation results. Computer simulation is done using the network simulator NS-2.28 to build our simulation environment. The CBR traffic is generated with a rate of 4 packets per second. A flat network is constructed for simulation purpose and monitored for a number of parameters. The simulation models 7 mobile nodes, moving over a rectangular flat space. Simulation time is 150 seconds. The random waypoint model is selected as a mobility model in a rectangular field (1000 × 1000 m2) with nodes speeds varying uniformly between 0 and a maximum value of 25m/s . Each node in the network is assumed to have a buffer with a capacity of 50 packets and use a FIFO interface queue.

In the first trial 7 node are created. They are moving in specific directions with different speeds. In this scenario none of the node is defined as malicious node. The node 0 is defined as source node and node 1 is defined as destination node. The TCP agent is attached to node 0 and TCP sink agent is attached to node 4.Existing AODV protocol is selected for routing the packets. The source node 0 can send the packets to node 4 via two paths,viz.node0-node2-node3-node 5-node4-node1 or node0-node6-node1. But node0 chose the path as shown in Fig. 2

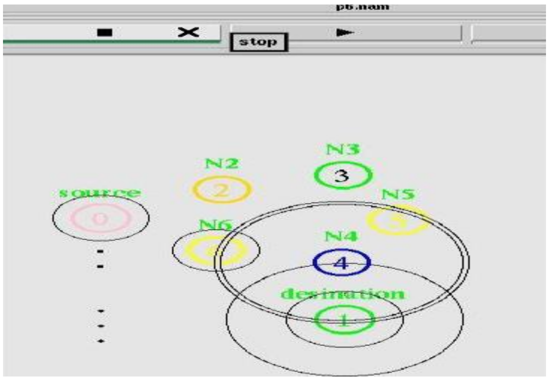
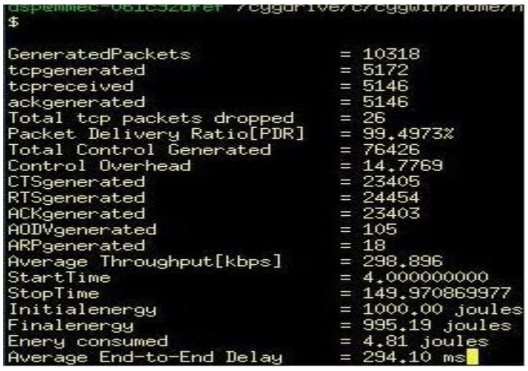


Figure 2:Mobile ad-hoc network without any black hole

The network parameters are as shown in Fig 3.



```
dsp@mmec-v61c32dref /cygdrive/c/cygwin/home/n
$

GeneratedPackets                 = 10318
tcpgenerated                     = 5172
tcpreceived                      = 5146
ackgenerated                     = 5146
Total tcp packets dropped        = 26
Packet Delivery Ratio[PDR]       = 99.4973%
Total Control Generated          = 76426
Control Overhead                 = 14.7769
CTSgenerated                     = 23405
RTSgenerated                     = 24454
ACKgenerated                     = 23403
AODVgenerated                    = 105
ARPgenerated                     = 18
Average Throughput[kbps]         = 298.896
StartTime                        = 4.000000000
StopTime                         = 149.970869977
Initialenergy                    = 1000.00 joules
Finalenergy                      = 995.19 joules
Enery consumed                   = 4.81 joules
Average End-to-End Delay         = 294.10 ms
```

Figure 3:Network parameters without any black hole

In the second trial 7 nodes are created. They are moving in specific directions with different speeds. In this scenario node 6 is defined as malicious node. The node 0 is defined as source node and node 4 is defined as destination node. The TCP agent is attached to node 0 and TCP sink agent is attached to node 4.Existing AODV protocol is selected for routing the packets. The source node 0 can send the packets to destination node1 via two paths,viz.node0-node2-node3-node5-node4-node1 or node0-node6-node1.But node6 being the black hole absorbs all the packets instead of forwarding towards the destination as shown in Fig.4

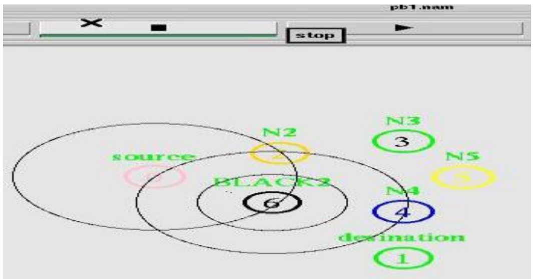
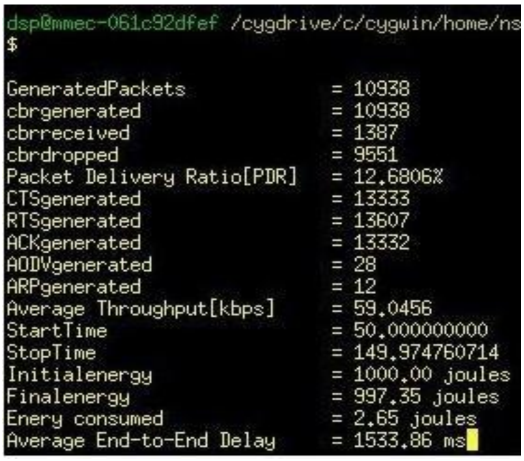


Figure 4:Mobile ad-hoc network with one black hole

The network parameters are as shown in fig 5.The PDR is severely affected by existence of black hole.



```
dsp@mmec-061c92dfef /cygdrive/c/cygwin/home/ns
$

GeneratedPackets             = 10938
cbrgenerated                 = 10938
cbrreceived                  = 1387
cbrdropped                   = 9551
Packet Delivery Ratio[PDR]   = 12.6806%
CTSgenerated                 = 13333
RTSgenerated                 = 13607
ACKgenerated                 = 13332
AODVgenerated                = 28
ARPgenerated                 = 12
Average Throughput[kbps]     = 59.0456
StartTime                    = 50.000000000
StopTime                     = 149.974760714
Initialenergy                = 1000.00 joules
Finalenergy                  = 997.35 joules
Enery consumed               = 2.65 joules
Average End-to-End Delay     = 1533.86 ms
```

Figure 5:Network parameters with one black hole .

In the third trial 7 node are created. They are moving in specific directions with different speeds. In this scenario node 6 and node 5 are defined as black holes. The node 0 is defined as source node and node 4 is defined as destination node. The TCP agent is attached to node 0 and TCP sink agent is attached to node 4.Existing AODV protocol is selected for routing the packets. The source node 0 can send the packets to node 1 via two paths,viz.node0-node2-node3-node5 node4-node1or node0-node6-node1. But node6 being the black hole absorbs all the packets instead of forwarding towards the destination as shown in fig.6.When node 6 goes out of range , the packets are routed via node 2-node 3-node 5-node 4-node 1 ,but node 5 being black hole does not forward the packets to its neighbor it absorbs all as shown in Fig 7.

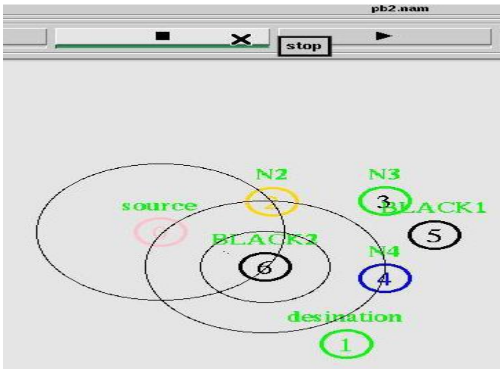
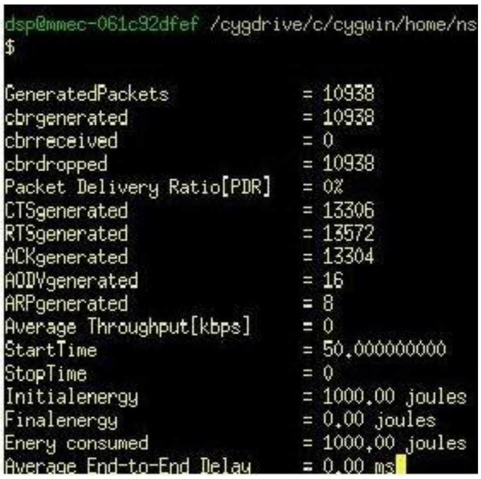


Figure 7:Mobile ad-hoc network with two black holes

In presence of two black network parameters PDR is severely affected and it nearly reaches to 0 as shown in Fig.7.



```
dsp@mmec-061c92dfef /cygdrive/c/cygwin/home/ns
$

GeneratedPackets             = 10938
cbrgenerated                 = 10938
cbrreceived                  = 0
cbrdropped                   = 10938
Packet Delivery Ratio[PDR]   = 0%
CTSgenerated                 = 13306
RTSgenerated                 = 13572
ACKgenerated                 = 13304
AODVgenerated                = 16
ARPgenerated                 = 8
Average Throughput[kbps]     = 0
StartTime                    = 50.000000000
StopTime                     = 0
Initialenergy                = 1000.00 joules
Finalenergy                  = 0.00 joules
Enery consumed               = 1000.00 joules
Average End-to-End Delay     = 0.00 ms
```

Figure 8:Network parameters with two black holes

In the fourth trial ,the topology of the network is kept identical but only one change is made that is the modified AODV protocol is selected for routing the packets. In the scenario node 6 is only defined as black hole .The source node 0 can send the packets to node 1 via two paths,viz.node0-node2-node3-node5-nodee4-node1 or node0-node6-node1. But in this scenario the node 0 is not sending the packets through node 6 as it is in the earlier scenario but it sending the packets by route as shown in Fig 9.Thus the black hole who sends false RREP can be avoided in the modified protocol .

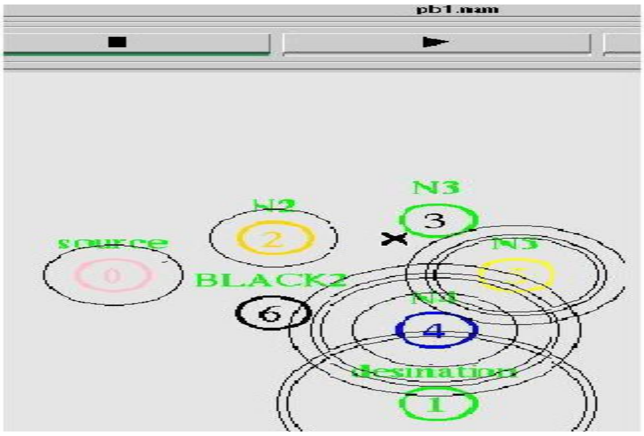
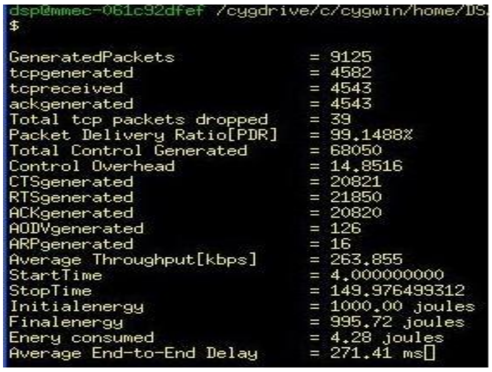


Figure 9:Packet transmission in network with one black hole

Due to the modified AODV protocol the network parameters especially PDR in presence of one black can be improved which is as shown in Fig.10.



```
dsp@mmec-061c92dfef /cygdrive/c/cygwin/home/DS
$

GeneratedPackets                  = 9125
tcpgenerated                      = 4582
tcpreceived                       = 4543
ackgenerated                      = 4543
Total tcp packets dropped         = 39
Packet Delivery Ratio[PDR]        = 99.1488%
Total Control Generated           = 68050
Control Overhead                  = 14.8516
CTSgenerated                      = 20821
RTSgenerated                      = 21850
ACKgenerated                      = 20820
AODVgenerated                     = 126
ARPgenerated                      = 16
Average Throughput[kbps]          = 263.855
StartTime                         = 4.000000000
StopTime                          = 149.976499312
Initialenergy                     = 1000.00 joules
Finalenergy                       = 995.72 joules
Enery consumed                    = 4.28 joules
Average End-to-End Delay          = 271.41 ms▯
```

Figure 10:Network parameters with one black hole

In the fifth trial , the topology of the network is kept identical but only one change is made that is the modified AODV protocol is selected for routing the packets. In the scenario node 6 and node 5 are defined as black holes .The source node 0 can send the packets to node 1 via two paths,viz.node0-node2-node3-node5-nodee4-node1 or node0-node6-node1. But in this scenario the node 0 is sending the packets through node2-node3-node4-node1by avoiding both(node 5,node6) the black holes in the routes as shown in Fig.11

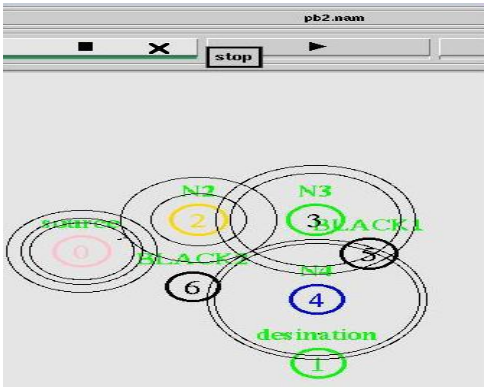
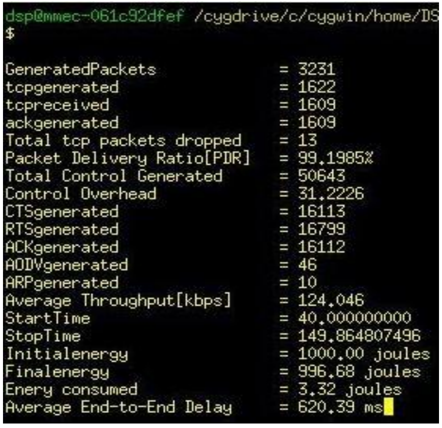


Figure 11:Packet transmission in the network with two black holes.

Due to the modified AODV protocol the network parameters especially PDR in presence of two black holes can be improved which is as shown in Fig.12.



```
dsp@mmec-061c92dfef /cygdrive/c/cygwin/home/DS
$

GeneratedPackets            = 3231
tcpgenerated                = 1622
tcpreceived                 = 1609
ackgenerated                = 1609
Total tcp packets dropped   = 13
Packet Delivery Ratio[PDR]  = 99.1985%
Total Control Generated     = 50643
Control Overhead            = 31.2226
CTSgenerated                = 16113
RTSgenerated                = 16799
ACKgenerated                = 16112
AODVgenerated               = 46
ARPgenerated                = 10
Average Throughput[kbps]    = 124.046
StartTime                   = 40.000000000
StopTime                    = 149.864807496
Initialenergy               = 1000.00 joules
Finalenergy                 = 996.68 joules
Enery consumed              = 3.32 joules
Average End-to-End Delay    = 620.39 ms
```

Figure 12:Network parameters with two holes

In the Fig. 13 PDR parameter of existing AODV and modified AODV is compared in identical environments.

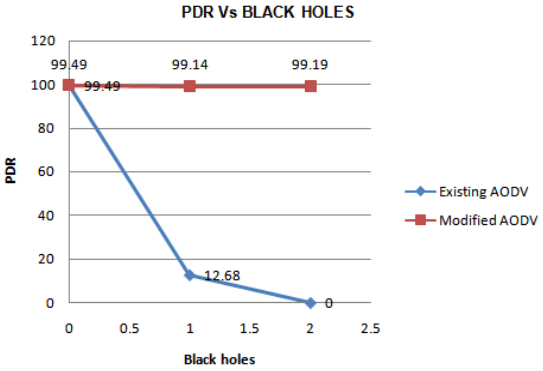


Figure 13:Comparison of PDR .

VII. Conclusion

By observing the results of simulation of network on NS2,,it is concluded that the existing AODV protocol is not able to cope with attacks like black hole . But in modified AODV false RREP is not received to source. The only node that can reply with RREP is the destination . Thus after establishing end-to- end (source to destination) connection, source node transmits the data packets. In the simulation of modified AODV it is seen that the networks performance(PDR) is enhanced to considerable extent in such type of attacks. Thus ,the modified ADOV has better capability to cope with black hole attack than existing AODV.

References

Journal Papers:

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

[2]Zhao Min and Zhou Jiliu , Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks , *International Symposium on Information Engineering and Electronic Commerce,2009*

Books:

[3]C.Siva Ram Murty and B.S.Manoj, Ad-hoc Wireless Networks,Architectures and Protocols (Fourth Edition,Pearson Education,2009)

Proceedings Paper:

[4]Mehdi Medadian, Ahmad Mebadiand and Elham Shahri, Combat with Black Hole Attack in AODV Routing Protocol , *Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009 Kuala Lumpur Malasiya.*

[5]C.E.Perkins and E.M.Royer, AD-HOC On-Demand Distance Vector Routing, , *In proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and,Applications,p,p . 90-100, New 04- U. Feb. 1999.*