MODIFIED AODV TO ELIMINATE THE EFFECTS OF BLACK HOLE NODE IN MANET

[1]V.Tamizhazhagan,

Assistant Professor,
Dept. of Computer Science & Engineering , FEAT,
Annamalai University, India.
Email- rvtamizh@gmail.com

[2]P.Manjamadevy

Dept. of CSE, FEAT, Annamalai University, India.

[3]R.Tamil Nilavu

Dept .of CSE ,FEAT, Annamalai University, India.

ABSTRACT

Mobile Adhoc Network (MANET) consists of a collection of wireless mobile hosts without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security. In this paper, therefore, we attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANET viz. the Adhoc On Demand Distance Vector (AODV) routing protocol. Our focus specifically, is on ensuring the security against the Black hole Attack. A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. The proposed solution is capable of eliminating the effect of presence of black hole nodes in the MANET. The simulation study is performed using Network Simulator NS-2.34.

KEYWORDS: ***Mobile Ad-hoc Network, Black Hole Attack, Simulation, Security, Network simulator.***

1. INTRODUCTION:

MANET[1][2] is a multi-hop temporary communication network of mobile nodes equipped with wireless transmitters and receivers without the aid of any current network infrastructure. Nodes within the radio range of each other can communicate directly over the wireless link, while those that are far apart use other nodes **as** relays. There are a number of challenges associated with providing security in MANET. The main reason for such concerns is the absence of a fixed central infrastructure that makes the scheme of central authorization and key management extremely difficult. However, MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability.

Routing plays an important role in the security of the entire network. The currently available routing protocols for MANETs are mainly categorized into proactive routing protocols and reactive routing protocols. In a proactive routing protocol, every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date and correct, such as DSDV (Destination Sequence Distance Vector)[4] and OLSR (Optimized Link State Routing Protocol)[5]. In a reactive routing protocol, a route is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as AODV (Ad hoc On-Demand Distance Vector)[6] or DSR (Dynamic Source Routing)[7]. A source node generally broadcasts a

route request message to the entire network by means of flooding, in order to search for and establish a route to the destination node. The AODV[6] is the most popular routing protocol and has been extensively discussed.

A black hole attack can be achieved by a single node or by several nodes in collusion. A single-node black hole attack forges the sequence number and hop count of a routing message in order to forcibly acquire the route, and then eavesdrop or drop all data packets that pass.

2. Adhoc On Demand Distance Vector Protocol

The Ad hoc On Demand Distance Vector (AODV) routing protocol is a pure on demand data acquisition system[6][8]. It is a reactive protocol and route maintenance is only between nodes that have to communicate. Whenever a source node wants to send packets to a destination node there is no fixed route as in a table driven system and the source has to initiate a route discovery process. This is done by broadcasting a RREQ (route request packet) to its neighbours. The neighbouring active node updates their Routing Tables (RTs) with an entry for the source node, and checks if it is the destination node or has a fresh enough routing to the destination node. If not the neighbours forward these requests to their neighbours until a complete route to the destination is established. The intermediate nodes that join the network can also initiate a route reply (RREP) if they have a valid path to the destination. The RREP packet is propagated along the reverse path to the source node. The validity and freshness of the route are ensured by the destination sequence number (DSN). Each node maintains its own sequence number to the intended destination and an intermediate node can reply only if its destination sequence number is greater than or equal to that contained in the RREQ. The source chooses that path from which it has received the first RREP for the transmission of data packets to the destination. The RREP's that are further received are discarded. Whenever a source node moves it has to reinitiate the process of route discovery to the destination. Whenever there are broken links or unreachable destinations, then RERR (Route error) messages are broadcasted to the nodes to indicate the same and the path discovery process is again reinitiated.

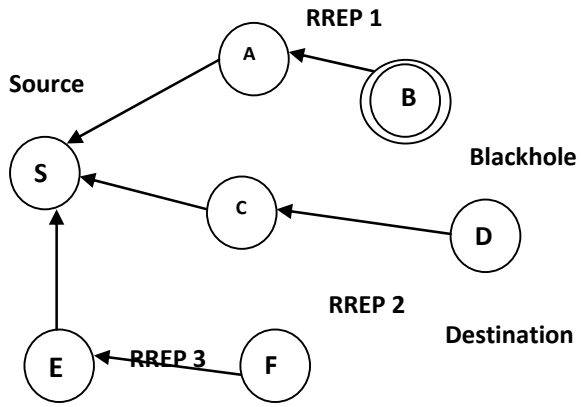
The major drawback of the AODV protocol is the lack of security mechanisms to ensure that the packets have reached the destination. There is no acknowledgement procedure that is present and hence no delivery validation.

3. SEQUENCE NUMBERS

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number[3]. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message. When a particular node forwards the RREP message coming from its neighboring node, it compares its own previously stored sequence number with that of the information that has been received recently. If it notices that the sequence number is newer than its own, then it changes its route table entry as necessary.

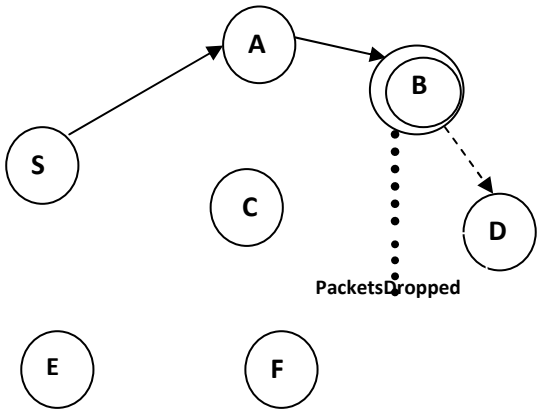
4. THE SINGLE BLACK HOLE PROBLEM

According to the functioning of the AODV protocol, whenever a source wants to relay data to an intended destination it broadcasts a RREQ to all its neighbours. These neighbours further check if they have a fresh enough route to the destination and then send in a RREP to the source. It has to be kept in mind that the source accepts that route from which it has received the RREP first. All other RREPs that come in later are discarded. A malicious node that is a black hole takes advantage of this feature of AODV and broadcasts to the source through an RREP with an extremely large sequence number and hop count of 1 to source node without actually checking if it has a fresh enough route to the destination, thereby it is always the first to reply. When receiving RREQs from normal nodes, the destination node would also select a route with a minimal hop count, and then, return a Route Reply (RREP) packet. Further due to the lack of an acknowledgement scheme in the AODV protocol the malicious node could deceptively retain/consume the intercepted packets leading to loss of the relayed critical information[9][10]. According to the AODV design, a source node would select the latest and shortest route to send data packets upon receipt of several RREPs packets. Thus, a route via a black hole node would be selected by the source node. The black hole node will then eavesdrop, or directly drop the received data packets.



RREP 1: Request Reply from Black hole B → S
RREP2: Request Reply from Destination D→ S
RREP 3: Request Reply from Intermediate F→S

Fig.4.1 RREP PROPAGATION IN NETWORK



Packets sent from S→D via Black hole B
B drops packets without forwarding to D

Fig.4.2 PACKETS DROPPED BY BLACKHOLE NODE

5. MODIFIED AODV

Generally the adhoc routing protocol selects the route based on the sequence number and hop count. This kind of route selection strategy mostly leads to congestion in the network. And also AODV does not have the feature to detect and eliminate the black hole node in the network. In this paper, I have modified the standard AODV routing protocol to address the issues discussed above. The Route Reply method and Route Solution process in the AODV protocol is modified. The proposed solution does not detect the Black hole node rather it eliminates the effects of Black hole node's presence in the network.

5.1 Route Reply Process

In AODV, any node that possesses information about the destination can send Route Reply packet to the destination. A black hole node takes this as an advantage and always sends reply packets to the source node and with highest sequence number. The source node selects this route and the Black hole node drops all the packets sent to the destination through it. In my proposed approach I have added a new rule that an intermediate node cannot send route reply packets rather they can only forward the Route Request to the destination. The destination node alone can send route reply packets to the source node. All the intermediate nodes will discard the duplicate route request packets arriving to them. But the destination node accepts all the route request packets reaching the destination after travelling in disjoint route paths. The destination node will send reply packets to all the RREQ in the same direction in which the corresponding route request arrived to it. All the intermediate nodes lying in between the destination and source will forward the route reply packets from

the destination to the source node. This almost eliminates the effect of black hole node. Even if there are black hole nodes lying in any of the routes between source and destination they can forward the route from the source to destination and the reply from the destination to the source node.

5.2 Route Selection Process

In this proposed approach all the nodes while forwarding the route reply packet from the destination to the source sum up their queue length and remaining node energy to the route reply packet. The route reply when reaches the source node contains the aggregate queue length and total remaining energy in the path. In AODV generally the route selection process is based on the hop count. But we have added two more parameters to the route solution strategy. The route solution is based on the following equation.

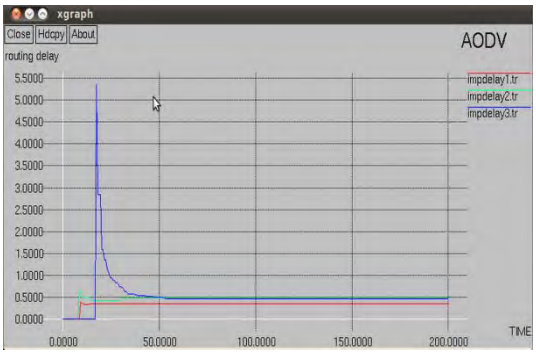
$$W = W_1 * \text{Hop count} + W_2 * \text{Aggregate queue length} + W_3 * \text{Remaining Energy}$$

$$\text{where, } W_1 + W_2 + W_3 = 1$$

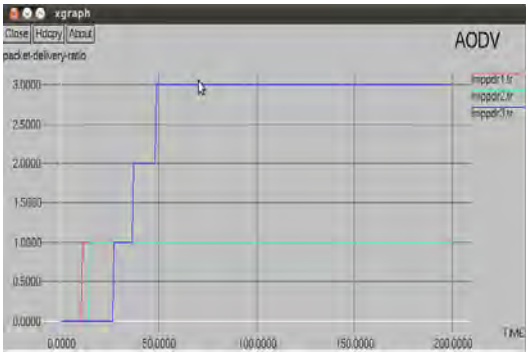
Weight of each route reply is calculated and route having the highest weight will be selected for data transmission [11]. By considering all these three parameters in selecting the route, the load can be evenly distributed in the network. This greatly reduces the congestion in the network since the load is evenly distributed to different paths of the network.

6. SIMULATION & RESULTS

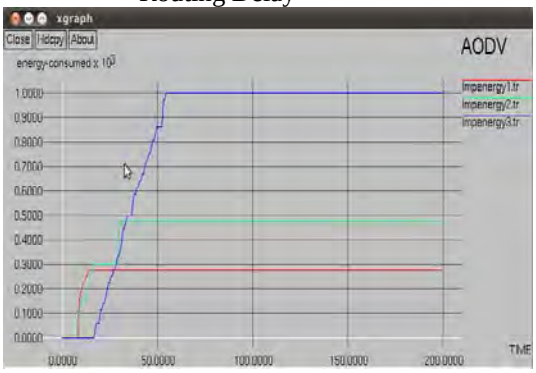
To analyze the performance of BlackHole nodes in AODV and modified AODV routing protocol NS-2.34 is used. In all the simulation scenarios the total number of mobile nodes is kept constant as 50. The routing protocol used in all the simulations for general node is AODV. In each scenario the number of BlackHole Node is increased to evaluate corresponding increase in Packet Loss percentage. UDP connections are established between even numbered nodes (0 (zero) included) and odd numbered nodes and we used 50 nodes in the scenarios .In the scenarios, even numbered nodes (Node 0 - Node 48) are the sending nodes and odd numbered nodes (Node 1 -Node 49) are the receiving nodes and the even numbered nodes send the packets to the next odd numbered nodes, for example Node 0 to Node 1, Node 2 to Node 3, Node 4 to Node 5 etc. Thus, we could count the sent and received packets between any 2 nodes. In the scenarios, UDP agents are attached to the even numbered nodes and NULL agents are attached to odd numbered nodes. In all the scenarios, we have a total of 24 connections between 48 nodes and all of these connections are always between the same nodes. But, in each scenario, every single node is placed in different coordinates and exhibits different movements. This helps us get different results with the same nodes and for scenario we increased the mobility speed of the nodes. We attach the CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. The total simulation time in all the scenarios is 200 Seconds In our scenarios CBR parameters are; Packet Size : 512 bytes Data Rates : 10 Kbits and we did not use random packets in the simulation. We first try to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. We noticed that the percentage of data loss in the presence of the Black Hole AODV is increased more than the normal AODV network simulations in all scenarios. After implementing proposed modifications in the AODV successfully then, we performed the same simulations on the scenarios we used for the BlackHole nodes to compare the performance of modified AODV.



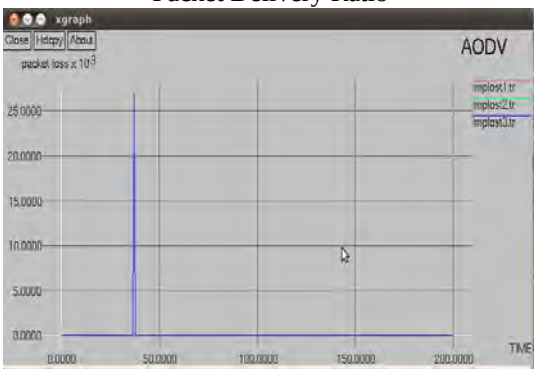
Routing Delay



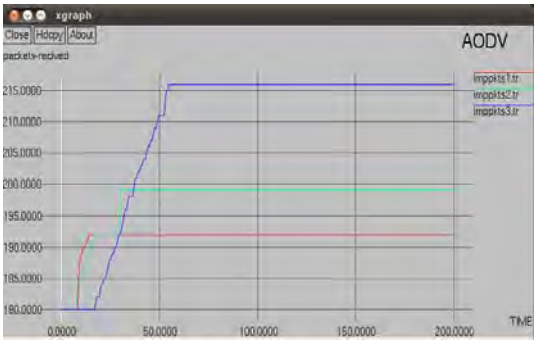
Packet Delivery Ratio



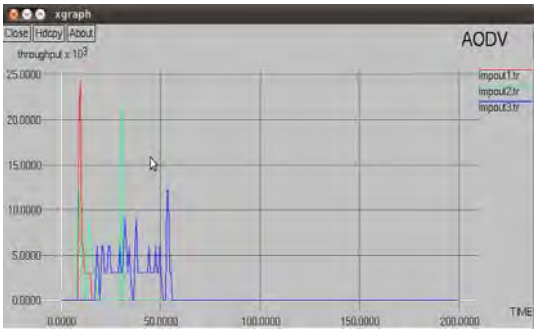
Energy Consumed



Packet Loss



Packets Received



Throughput

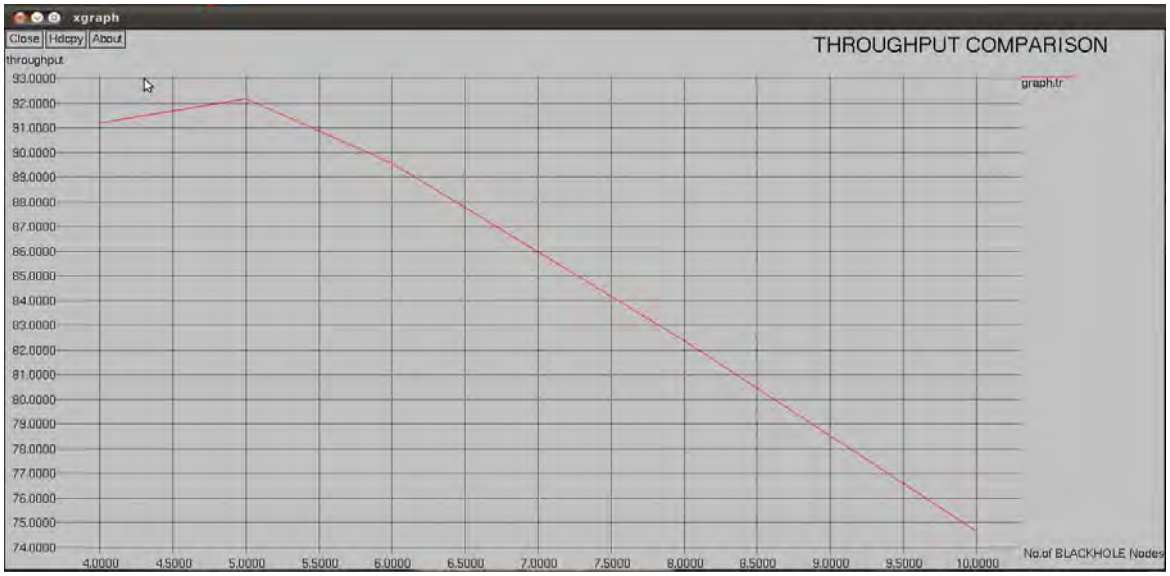


Fig 6.1 PERFORMANCE ANALYSIS OF MODIFIED AODV

7. CONCLUSION

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated five scenarios where each one has 50 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to eliminate the Black Hole effects in NS-2 and simulated the solution using the same scenarios. Our simulation results are analyzed below: Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. The graph 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. On an average AODV network has normally 8.21 % data loss and if a Black Hole Node is introducing in this network data loss is increased to 82.59 %(this depends on the proportion of the black hole to the total no. of nodes). As 8.21 % data loss already exists in this data traffic, blackhole Node increases this data loss by 74.38 %. When we used modified AODV protocol in the same network, the data loss decreased to 38 % on an average. These two results show that our solution reduces the Black Hole effects by 36.8 % as packet loss in a network using modified AODV. The performance analysis obtained is depicted in the following graphs.

8. REFERENCES

[1] Deng, Hongmei, Li, Wei and Agrawal, Dharma P, Routing security in wireless ad hoc networks, IEEE Communications Magazine, Oct.2002, pp.70-75 29.
[2] Junhai luo; Mingyu Fan, Research on trust model based on gaem theory in mobile ad-hoc networks, Journal of Computer Research and Deevelopment, Vol 45, No.10 2008, pp1704-1710
[3] C. E. Perkins and E. M. Royer, “The Ad hoc On-Demand Distance Vector Protocol,” in Ad hoc Networking, C. E. Perkins, Ed.Addison- Wesley, 2000, pp. 173–219.
[4] Charles E. Perkins and Pravin Bhagwat, “Highly Dynamic Destination- Sequenced Distance-vector Routing (DSDV) for Mobile Computers,” *SIGCOMM*, 1994.
[5] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR),” IETF RFC 3626, October 2003.
[6] 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.
[7] D. B. Johnson, D.A. Maltz, and Y.-C. Hu, “The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR),” IETF Internet Draft, July 2004.
[8] C K. Toh, Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall, January 2002.
[9] H. Deng, W. Li, and D.P. Agarwal. Routing Security in Wireless AdHoc Networks. IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40 No. 10, October 2002.
[10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Proceedings of the International Conference on Wireless Networks, June 2003.
[11] Rani, A. , Weighted load balanced routing protocol for MANET, Networks, 2008. ICON 2008. 16th IEEE International Conference.