REVIEW ON TO DETECT AND ISOLATE BLACK HOLE ATTACK IN MANETs USING AODV

Neha[1], Jasvir Singh[2]
[1]*M.Tech (CE) Student ,Deptt. of computer Engg ,Punjabi University, Patiala, Punjab, India*
[2]*Assistant Professor (CE), Deptt. of computer Engg , Punjabi University, Patiala, Punjab, India*

***Abstract*- A mobile ad hoc network can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. The security in MANET is a highly preferred research area these days in one of the reactive routing protocol AODV because it is susceptible to various attacks like black hole attack which has been discussed in the paper. In AODV, route is establish to destination only on demand. Due to the black hole attack network performance degraded.**

***Index Terms*- MANET, Black hole attack, AODV, NS2**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that are communicating with each other using multi-hop wireless links without a centralized network infrastructure. Because the nodes in a MANET are mobile, the physical network topology changes frequently and unpredictably. In MANETs, there is no stationary infrastructure such as access points (APs), therefore each node has to act as router for forwarding packets to other nodes [1],[3].

In a MANET network, nodes do not have advance knowledge about the topology that is used in the network. In MANET there is a theory when a new node arrives in the network, it should announce its presence in the network and then listen to its neighbours. In this way, the node will gain information about other nodes, which are close to it and learn ways how to contact them and what are the routes. Therefore, by this way all other nodes know where the other neighbours are and the routes to send traffic to them and find out at least one route to other nodes. Proper network routing and security are challenges of today's network.

II. MANET ROUTING PROTOCOLS

There are several protocols proposed for wireless mobile ad-hoc network. In this paper, we have used the AODV Routing Protocol.

1. *Ad-hoc On-Demand Distance Vector Routing (AODV)*

It is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks it is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In AODV route request, route reply and route error are the control messages. When source node wants to establish route to the destination nodes, source node first route request control

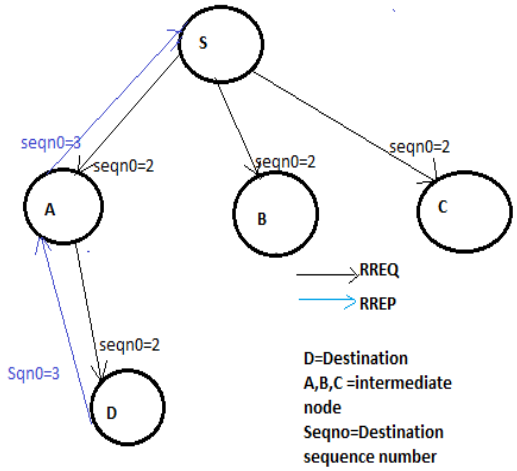

Figure 1: AODV protocol

packets to their adjacent nodes [2] .When adjacent node receives route request packets if node has the route to the destination node it will reply back to source node with route reply message. Source node select best route on the basis of hop counts and on the basis of sequence number.

AODV defines three types of control messages for route maintainence:

RREQ – A route request message is transmitted by a source node requiring a route to a destination node. As an optimization AODV uses an expanding technique when flooded these messages.Every RREQ carries a time to live(TTL) value that states for how many hops this message should be forwarded. This value is set to a pre-defined value at the first transmission and increased at retransmissions[4]. Retransmission occur if no reply are received. Data packets waiting to be transmitted (i.e the packets that intiated the RREQ) should be buffered locally and transmitted by a FIFO principal when a route is set.

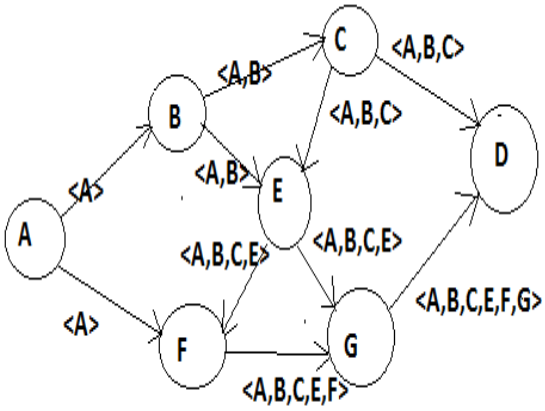

Figure 2 : Route Request Flooding

In the figure 2, the source node A floods the network with route request packets [5]. Every node adds its ID in the packet header until it reaches to the destination.

RREP – A route reply message is unicasted back to the originator of a RREQ. If the receiver is either the node using the requested address, or it has a valid route to the requested address.Then it will unicast the reply back, is that every other route forwarding a RREQ caches a route back to the originator.

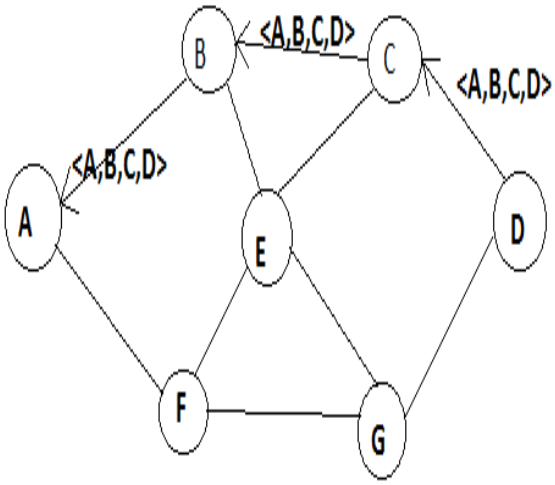

Figure 3: Route Selected between Source and destination

In figure 3, the route is established between the source and destination. The route has been selected on the basis of hop count and sequence number. The route with the minimum hop count and higher sequence number is selected as the best route. Once the optimal route has been selected, the confirmation packet is unicast via this route only.

RRER – Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RRER message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each of its neighbours that are likely to use it as next hop towards each destination.

III. SECURITY ATTACKS IN MANET

Mobile ad hoc networks are vulnerable to security attacks. Attack is the mechanism which disrupts the normal behavior of the network. The security attacks are triggered from the internal as well as external node [7]. There are many types of attacks in MANET like Routing attack,Wormhole Attack, Jamming Attack ,Eavesdropping, Denial of Service Attack, Black hole Attack.

1. *BLACK HOLE ATTACK* -Black hole attack, comes under the category of active attacks, that can be performed by the malicious nodes which are inside the network. Reactive routing protocol has been used

for selecting the route between the source and destination. Malicious node exits in the route which is between source and destination [6]. Malicious node is responsible for dropping the data. Consequently, destination node will not be able to receive sent by the source. So, Denial of service attack has been triggered.

1.1 BLACK HOLE Problem in AODV Protocol

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When node requires a route to a destination, it initiates a route discovery process [9] within the network. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired [8]. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred.

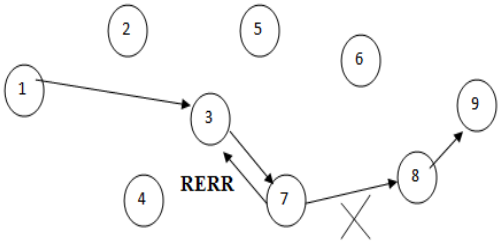

Figure 4 . Routing Discovery Process in AODV protocol

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets , it does not forward packets to its neighbors. Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node [10], does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it and discard the route reply comes from nodes 'B' and 'D'. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'.

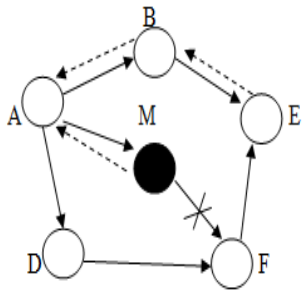

Figure 5 AODV problem in MANET

IV CONCLUSION

As MANET being infrastructure less it can be deployed with fewer efforts as compared with the traditional network infrastructure environment. It has a lot of potential but still there are some issues to overcome. One of the popular research areas nowadays is security in MANET and in this paper we are addressing security issues in one of the reactive routing protocol (AODV) in MANET. In this paper we will propose new technique to isolate and detect black hole attack to improve network performance.

REFERENCES

[1] S.Basagni, M. Conti, et.al , "*Mobile Ad Hoc Networking"*,Inc., Publication, August 2004.

[2] Ashish Bagwari, Raman Jee," Performance of AODV Routing Protocol with increasing the MANET Nodes and it's effects on QoS of Mobile Ad hoc Networks", International Conference on Communication Systems and Network Technologies,2012.

[3] Ivascu G. L., Pierre S., Quintero A., "Qos Support based on a Mobile Routing Backbone for Ad Hoc Wireless Networks", IWCMC, Canada, July 2006.

[4] Wells Paris, "Ad Hoc Wireless Network Comparision–A Comparision between DSR and AODV Routing Protocols"– Wireless Data Communications System, School of Engineering and Design, Brunel University.

[5] Shaily Mittal , Prabhjot Kaur, "PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S", International Conference on Advances in Computing, Control and Telecommunication Technologies,2012.

[6] A. Bhandare and S. Patil, "Study of Protocols (AODV, DSR) of MANET and Black Hole Attack in AODV", ISOR Journal of Electronics and Communcation Engineering, pp. 50-53, 2011.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks" ,*Springer,2006.*

[8] J. Sen, S. Koilakinda and A. Ukil, "A mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Network", *International conference on Inteligent Systems, Modelling and Simulation,* pp. 338-343, 2011.

[9] P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", *IEEE International conference on Trust, Security and Privacy in Computing and Communcation* ,pp. 902-906, 2012.

[10] Sheenu Sharma, Roopam Gupta "SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS", Journal of Engineering Science and Technology ,Vol. 4, No. 2 (2009) 243 – 250.

.