

Disruption of Black Hole attacks in MANET

Dhanashree Toradmalle¹, Nivedeeta Banerjee²

¹Assistant Professor, Department of Information Technology, Mumbai University, India

²Master in Information Technology, Department of Information Technology, Mumbai University, India

Abstract—An Ad hoc network in a wireless system consist of an autonomous system, without centralization which results forming of mobile nodes. In MANET, each node works in a dual form that consists of a router as well as hosts. These nodes configure dynamically and communicate using hop to hop. Due to its simplicity it is used in mobile conferencing, military communication.

In MANET nodes can join and leave the network so MANET becomes vulnerable. Certain factors like dynamic network configures, distribution cooperation, open medium terrorized in routing which give rise to security issues. Once such protocol AODV has been a victim of security. In existing, MANET faces a severe problem known as the Black Hole problem. This Black hole problem is mostly found in reactive routing protocol called AODV. The black hole conducts its malicious node during route discovery process. Black hole node is a severe threat in AODV protocol that easily employed and becomes vulnerable in MANET. In this paper various techniques are discussed to overcome the Black hole attack.

Keywords—MANET, Ad-Hoc, Black Hole attack, RREQ, RREP.

I. INTRODUCTION

Wireless mobile ad hoc network is a collection of multiple nodes which incorporates wireless communication and networks processing capabilities. These devices communicate through radio range consisting of a transmitter and receiver at both the ends. In Wireless communication nodes share a similar frequency band and if the destination node is not in the transmission range, the source node will take help of intermediate nodes.

Ad-hoc network is dynamically built such that nodes can join or leave the network at any time. Since the nodes communicate they establish connection among themselves. These connections are in the form of routing protocols. The routing Protocol are mainly Dynamic Source Routing protocol(DSR), Ad hoc on demand distance vector protocol(ADOV), Destination Sequence Distance vector(DSDV). Since Wireless network carries no infrastructure, they are exposed to many attacks. One such

attack named is Black Hole attack. The Black hole attack fabricates the sequence number and pretends to have a fresh route to reach its destination. Malicious node does not process, in fact they respond with false information claiming the shortest route to forward the packets. So the network traffic routes to the destination from the sender through this the malicious node that disrupt the network service. The black hole node absorbs the network traffic.

This paper presents, Types of attack, Black hole attack on AODV and techniques overcoming Black hole attack. The motive of this paper is to focus on elimination of black hole attack in AODV protocol.

II. TYPES OF ATTACK

There are two types of Attack Passive attack and Active Attack

1. Passive attacks:

In Passive attacks, the attacks are not disrupting the network service. The most common example are eavesdropping attack and traffic analysis and monitoring

2. Active Attack:

In Active attacks, the attack degrade the performance of the network like altering or discarding data being exchanged in the network. This can be done in internally or externally in the network. Let us observe the different techniques of attacks in MANET that exploit the network services

2.1. Worm hole attack:

In Worm hole Attack, the Attacker causes vulnerabilities and disturbs the performance of network. It is very difficult to detect and prevent this type of attack. Worm hole attack is also known as tunneling type of attack. In this of attack a malicious node receives the packet at one location in the network and tunnels them from other location of network then later, it forwards the packet. An attacker with two different points connects the network

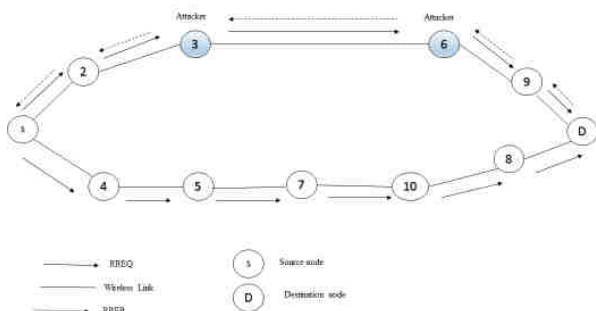


Fig.1: Worm Hole Attack[1].

2.2. Black hole attack

Black hole attack is the severe threat on Mobile Ad hoc networks. Before making an attack on AODV routing protocol, the malicious node tries to find shortest path in an optimal way.

Secondly when the malicious nodes enter into the network it either relays the packet or drops the packet. MANET always falls prey of Black hole attack.

In black hole attack, when malicious node enter into the network it fools the sender and fabricates the information such as possessing the shortest path and updating the routes to destination. In AODV protocol an attacker response by sending fake RREQ indicating that it has fresh path to send node. This means malicious node wants to make friend so it sends request and once request is accepted, attacker betrays the sender node.

Due to dynamic forming of topologies, a mechanism should introduce that helps in routing protocols to differentiate between fresh and stale information stored by the nodes. In AODV protocol, destination sequence number and hop count are a major criterion in selecting the route; it gives indication of how fresh is the route. Higher the sequence number fresher is the route. Hence the node having the highest destination sequence number is given the utmost importance and is selected in the route discovery process. The malicious node now uses AODV protocol that helps to sets its destination sequence number to a high value and sends a fake RREP to the source that hold highest sequence number. Now this increases the chance of route selection for routing data packets includes the attacker.[1]

2.3 Gray Hole Attack:

This type of attack is also known as routing misbehavior attack which leads to dropping of packets. It has two phase .In the first phase the node makes publicity of having fresh

route to destination .In the second phase node drops the packets with certain modification

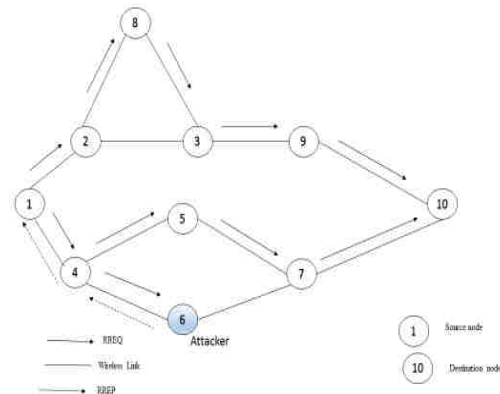


Fig.2: Black Hole Attack[1]

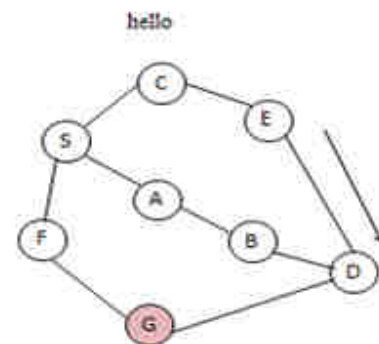
III. SOLUTION TO PREVENT BLACK HOLE ATTACK

When the destination node is attacked by Black hole node, possibility is to find multiple routes through which communication of source to destination is initiated .Then the source node sends ping packets to find route with sequence number and packet ID. Whoever route received first packet will not drop and carry this from source to destination.

Here the receiver and malicious node in addition to intermediate nodes whoever received the ping packets, will reply the ping packets. The source will check acknowledgements and process them in order to figure out which of them is malicious node or destination node.

First Solution: Detection of Malicious node

Pramod Kumar Singh, Govind Sharma [2] has proposed the use of promiscuous mode of the node. The promiscuous node is that if node A and node B are in same range then Node A overhears to and from Node B even if they don't communicate directly with each other



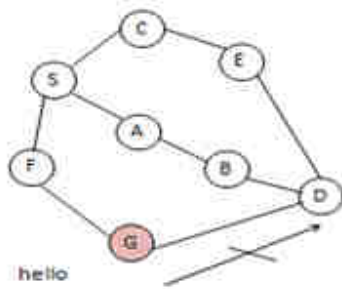


Fig.2: Flow of Hello packet towards destination (a) a good node forwards it (b) black node does not forward it.[2]

As shown in Fig 2 node S wants to initiate communication to node D but here in this case G is malicious node .Node S sends RREQ packets in the network and waits for RREP to receive. Now there options

Option1: When destination node or immediate node receives RREP packets, a node to its intermediate node enter into promiscuous mode and sends Hello message to node D using intermediate node.

If the intermediate node sends the hello message to destination, then considering the route is safe otherwise the route is not safe fearing of malicious node. The preceding node later floods with alarm messages to the network about the malicious node

Second Solution: Second shortest Path

AnandA Aware Kiran Bhandari [3] has proposed to prevent Black hole attack and to maintain data integrity using hash function.

As shown in above Fig 5 Consider Node A source node wishes to communicate and forward packets to node F, the destination node. So node A floods with RREQ packets to its neighbors node in search of destination node F .Now here node C is malicious node. When node C receives RREP message from Node A claiming it has the fresh path. So node A comes under influence of malicious node. The Source node A when receives the first RREP will not start sending the packets instead its waits for the second RREP packet from immediate node B which is said to be second shortest .So the Source node will discard the first route and take the routes from A-B-F to reach destination node F.

There could be the case that in a network there might be several malicious node. So to ensure the safe route between the nodes the hash function is applied on message. The hash value is computed on source and destination node. The hash function computed on source node is SHA-ONE .the hash function computed on destination node is SHA-TWO. If

hash values computed on both nodes are outputted the same result then the route is safe and message is transmitted without any error.

If the hash values are not equal then source node and destination node immediately release Data Packet Error (DPE) to inform other nodes about malicious node and the data packets are not safe in future.

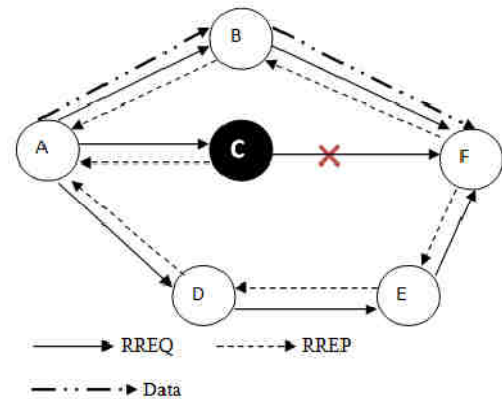


Fig.5: Black / Gray hole attack on AODV [3]

Third Solution: Multiple Route to route Data packets

Nidhi Sharma, Mr Alok Sharma[4] has proposed multiple routes to the destination .The source node pings the packet to destination node using more than one route. The route has sequence number and packet ids. So that it is easy to identify the data packets. Now there a two possibilities of attack elimination

A. Multiple route

In this type of Solution, the sender node authenticates the node that initiate the RREP packet by utilization the network redundancy. Since any packet can arrive from any routes, the solution is to wait for RREP packet to arrive from more than two nodes. As source node buffers the packet till it ensures the safe route is identified. When RREP arrives to the source it will extract full paths. Multiple node shared same hops. From these same hops to source and destination can declare the safe route.

If no shared node appear to be in multiple routes, the sender will wait for another RREP until a route is identified or routing timer is expired. This solution ensure the safety of the route that leads to destination node but the system has flaws of time delay.

B Sequence Number.

Every packet has sequence number .The sequence number is increasing order. The packet must have higher value than the current packet sequence number. The nodes maintain

last sequence number that it receives and verify whether this packet is originated under same source or not.

The sequence number is updated in routing table. In this type of solution for every transmission the last sequence number of the packet that it has received is updated. The node has two sized tables one to keep last packet sequence number for the last packet received from node.

Sender broadcasts the RREQ packets to its neighbours. The table is updated as the packet arrives and departs .Once these RREQ reaches to its destination, it initiates RREP to the source.

When an intermediate node has route to destination and receives RREP packet, the packet contains last packet sequence number from the source to its intermediate node

IV. CONCLUSION

An efficient and simple approach for defending AODV. Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by identifying the node with their sequence number; it is verified whether there is large difference between the sequence number of source node or intermediate node that carries packet to destination.

Since black hole attack is main security threat that degrades performance of the routing protocol in Mobile Ad hoc network. To detect and prevent is one of the important factors to ensure better quality of network performance. In this paper various techniques were discussed to detect and prevent the network from vulnerable attack.

REFERENCES

- [1] Pratibha Kaswan, Deepika Gupta “Impact Analysis of WORM Hole and black hole attack over Mobile AD hoc Networks” in International Journal on Recent and Innovation Trends in Computing and Communication, India, December
- [2] Pramod Kumar Singh, Govind Sharma “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET” 11TH International Conference on Trust, Security Privacy in Computing and Communication 2012 IEEE.
- [3] Anand A Aware Kiran Bhandari “Prevention of Black Hole Attack in AODV in MANET Using Hash Function” 2014 IEEE
- [4] Nidhi Sharma Mr Alok Sharama “The Black hole node attack in MANET 2012, IEEE