Destination based group Gray hole attack detection in MANET through AODV

Avenash Kumar [1], Meenu Chawla [2]

[1]Research Scholar
Computer Science and Engineering Department
MANIT Bhopal INDIA

[2]Associate Prof.
Computer Science and Engineering Department
MANIT Bhopal INDIA

Abstract

MANET is easily vulnerable because of dynamic topology, infrastructure less nature and also due to lack of centralized administration. One of the most common attack on such networks is gray hole attack which drop some selective data. It is challenge to keep the network free form this attack. This paper presents a technique for detection of group gray hole attack through destination based scheme when more than one malicious nodes are in a Mobile ad hoc network.

Keywords: *Mobile ad hoc network, gray hole, drop packet*

1. Introduction

Mobile ad hoc network is a self-configuring network in which there is no dedicated router; it means each node acts as a router because of no centralized node. Each node has limited communication range in the network and each node act as a router to forward packets to another node. MANET routing protocols assume that all the nodes are trusted. If the packet information has been changed and the direction of the router has been modified, then the attacker/intruder would perform different types of attacks such as gray hole and black hole attack.

There are various denial of service attacks one of them is gray hole attack in which some selective data is dropped before it reaches the destination. In gray hole attack an adversary first works as a honest node during the route discovery process. Then it silently drops some of the data packets sent to it for further forwarding even when no congestion occurs. To detect these malicious nodes lot of research has been done in past one of the proposed algorithm to detect malicious node through previous node has been presented in[1].This paper presents the detection of group gray hole attack in mobile ad hoc network using AODV(Ad hoc on demand vector). One of the most critical problems in MANET is the security vulnerabilities of the routing protocols. That is, in mobile ad hoc network it is harder to detect malicious node: here routing protocol called AODV is a being use to perform the work of detection. AODV is a routing protocol in which route discovery is done by broadcasting route request RREQ from source to destination and return route reply RREP message is received from destination or from sa,e node which has a valid path to the destination.

The rest of paper organized as follow: Section 2 present related work for detection of gray hole. Section 3 provide about AODV and gray hole, Section 4 describes proposed work for group gray hole attack detection. Section 5 finally concludes the paper.

2. Related work

In the gray hole attack, the malicious node on receiving a route request from any other node in the network, replies immediately with the false shortest path to the destination [2]. This way the source considers the path through the attacker as the shortest path and uses the path through attacker node for all data flow between the source and destination. Then the attacker node selectively drops some of the traffic passing through it. A gray hole attack is a modified form of black hole attack in which a node initially behaves non-maliciously but later turns malicious after gaining initial trust of other nodes.

The Local Intrusion Detection security (LID) routing mechanism performs its tasks locally on the preceding node of the in-between node, whereas the Source Intrusion Detection mechanism performs detection

mechanism on the source node. The proposed Local Intrusion Detection [1] security routing mechanism takes into consideration that the preceding node is trusted and there is no group attack in the network; which means that if the in-between node is assumed, then it performs a single attack on the network.

SEN et. al. [3] the routing security issues in MANETs are described in general. Specifically the cooperative black hole attack has been discussed in detail. A security protocol has been proposed that can be used to detect multiple black hole nodes in a MANET and hence find a secure routing path from a source node to a destination node and avoiding the black hole nodes.

The malicious packet dropping attack is launched by an internal node, in which it promises to deliver the data packet, but refuses to carry out its responsibility during data delivery phase. Dropping of packet could degrade the performance of the network; they can disturb route discovery process. Use of aggregate signature is discussed in [4]. This mechanism leads to granted detection as evidence on forwards packets is used.

Another work for gray hole and black hole attack has been discussed [5] which determines a short and safe path in presence of the different other with insignificant difference in routing overhead.

3. AODV and Gray hole attack

This section describes the widely used ad hoc on demand vector routing protocol and describes about the vulnerable gray hole attack on AODV routing protocol.

3.1 AODV

Ad hoc on demand vector routing protocol is reactive routing protocol in which it does not maintain fixed routing table or path up to the destination. It is a reactive routing protocol [6]. When source node needs to deliver the packet then source node broadcast a message as route request (RREQ) to its one hop distance nodes called as neighbor nodes to find path to the destination. AODV is a method of routing message between mobile nodes and allow passing the message through its neighbor node. AODV also handle changes in routes and can create new route if there is an error. Because of limit on transmission range each node can only communicate with the neighbor node to it. When one node needs to send a message to another node that is not its neighbor it first broadcast a route request message. The route request message contains several keys such as source information, destination information and also a sequence number. And if intermediate node does not have destination information then it also broadcast the same route request message by updating route table.

When destination address is found at any intermediate node then the node sends (RREP) message back to source node. One special case is that when a link break occurs, a route error message is sent to source node. AODV always use hello message to maintain connection.

3.2 Gray hole attack

There are various denial-of-service attacks. One of them is gray hole attack. Gray hole attack is an attack in which some selective data packets are dropped by the malicious node. Gray hole attack is harder to find because of some data packets reached the destination and destination thinks that it is getting the full data.

Gray hole attack in routing protocol occur at the time of routing the data packet. In mobile ad hoc network this type of attack easily occurs due to dynamic nature of MANET. One of the major issue about the gray hole attacks is that it misguides the source by advertizing that there is a valid and shortest path to the destination. Thus the malicious node could do harm the network by degrading the network performance, disturbing route discover process etc.

4. Proposed work

In this section we propose the work which is performed to detect and prevent the group gray hole attack in MANET in ad hoc on demand protocol (AODV).

4.1 Methodology

The proposed work contains three steps:
1. Store the RREP packet on previous node.
2. Check 2 hop distance of a suspected node.
3. Rejection of RREP packet.

To identify the suspected node, the common neighbor of previous node and suspected node checks the two hop distance node for reach ability to the destination. To do so first it stores the RREP packet at previous node and attaches one hop distance of suspected node.

In AODV each node has its neighbor's information. In AODV routing protocol to discover a connection between source and destination, source node (N1) communicates with destination node (N10) shown in fig 1. Node (N1) broadcasts the *route request* (RREQ) message to its neighbor first. If neighbor is a destination then it send *route reply* (RREP) message reverse to source node otherwise it forward packet by updating their routing table.

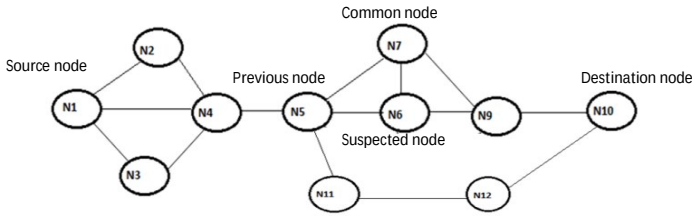

Fig: 1 Show mobile ad hoc network

This paper proposes that when RREP message replies to previous node it should also attach the one hop distance node of replying node (suspected node) otherwise previous node will reject the RREP message.

And in other case when there is no malicious node present in network, data packet successfully travels between source node to destination node but if there is malicious node present in MANET then it send *route reply* (RREP)message to source by falsely replying that there is valid route.

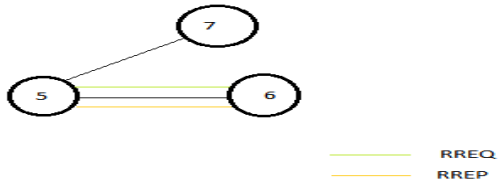

Fig 2 RREP by node 6

In fig 2, node 6 is a suspected malicious node, which sends a false route reply (RREP) message to previous node saying that there is a valid route and shortest path to destination.

4.2 Verify Suspected Node**:**

Here store the *route reply* (RREP) message and one hop distance of suspected node on previous node. Now we determine common neighbor of suspected node and previous node. Figure 3 shows suspected node 6 one-hop distance table.

NODE	Node	Node	Node	Node
	5	7	9	10

Fig 3 One hop distance of suspected node.

Then node 7, which is common neighbor of suspected node (assume at least one common neighbor in this paper), and previous node check whether destination node is in one hop distance or in two-hop distance. Here we consider node 7 is cooperative node [7] with the attacker, thus it supports suspected node and sends back *route reply* (RREP) to previous node that suspected node is valid. Therefore, source node follows that path and transfers the data packets, but some data lost at destination node due to co-operative gray hole effect.

Then finally, a fresh special *route request* (RREQ) message is sent through previous node, which does not follow any node that is one hop distance from suspected node as shown in figure 4. Now previous node checks routing table of destination node whether node 6 is in one hop distance of destination node, and if it is not in one hop distance then both node 6 and node 7 will be added in black listed node table.

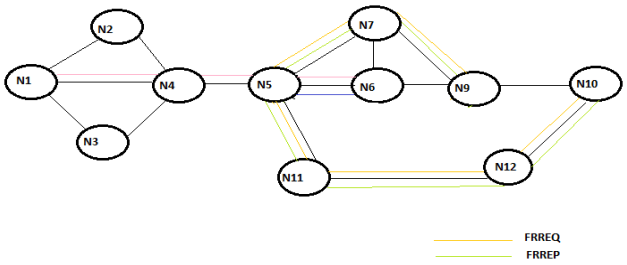

Fig 4 Fresh route request through previous node to destination node.

To do so detecting and preventing malicious node the proposed algorithm is as follows:-

Algorithm -

If RREP packet received from suspected intermediate node
{
Buffer the RREP packet
Send FRREQ packet to common neighbor node
If FRREP packet received extract FRREP packet information
If next node has a route to (destination and intermediate node)
Send FRREQ packet to destination through the route which don't have any nodes of one hop
Distance of suspected intermediate node
If destination node has route to intermediate node
Then
Discard FRREP packet
Unicast RREP to source node
Else
Discard both RREP and FRREP and generate alarm
Broadcast both RREP and FRREP
}

5. Conclusion

The gray hole attack [8] selectively drops data packet after falsely advertising itself as a valid route to reply packets. This behavior degrades network performance, especially if the gray hole is in the path from where majority of the data flows.

This paper proposed a method to detect cooperative malicious nodes by destination based routing method. It is expected to boost up network performance,

decrease end-to-end delay and routing overhead. The major factor is to increase the overall network throughput.

Reference-

[1] Maha abdelhaq, samiserhan " A local intrusion detection routing security over MANET network" 2011 International Conference on Electrical Engineering and Informatics.

[2] Sweta Jain, Meenu Chawla "A Review Paper on Cooperative Blackhole and Grayhole Attacks in Mobile Ad hoc Networks" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.3, September 2011DOI : 10.5121/ijasuc.2011.2305 71

[3] JaydipSen, M. Girish Chandra, Harihara S.G "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" ICICS 2007

[4] Chen Wei Long Xiang BaiYuebinGaoXiaopeng " A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks".

[5] Rutvij H. Jhaveri1, Sankita J. Patel2 and Devesh C. Jinwala" A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks"2012 Second International Conference on Advanced Computing & Communication Technologies.

[6] C. Perkins and E. M. Royer, "Ad hoc On-Demand distance Vector Routing," IETF MANET Internet Draft, July 2003.

[7] Zhao Min, Zhou Jiliu "Cooperative Black Hole Attack Prevention for Mobile ad hoc Network. 2009 International Symposium on Information Engineering and Electronic Commerce

[8] Vishnu k, Amos J Paul "Detection and Removal of Cooperative black/gray hole Attack in mobile ADHOC Network" 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22