Comparison of Different Methods for Gray Hole Attacks on AODV based MANET

[1]Mehul Vasava, [2]Mr. Hardik Patel
[1]PG Student,,[2]Assistant Professor
[1]Information and Technology Department, Shantilal Shah Engineering Collage, Bhavnagar, Gujarat.
[2]Sir Bhavsingh Polytechnic Institute, Bhavnagar, Gujarat.
[1]mehulv8@gmail.com,[2]hardikpatel.growmore@gmail.com

***Abstract* - Now a day, MANET security has become a big issue and one of the central attentions to the researchers. MANET is a network of wirelessly connected self configuring nodes which functions under the particular routing protocols. There isn't any central administration or a fixed infrastructure in the MANET. Any node within the MANET can move to any other network at anytime or other nodes can also connect to the MANET. This makes MANET highly vulnerable for different attacks.This paper focuses on a GrayHole attack among the different types of attacks possible in a MANET. GrayHole attack is one type of active attack which tends to drop the packets during the routing from source to destination. This paper also includes thecomparison of different techniques to deal with the GrayHole attack.**

***Key terms:*MANET, AODV protocol, GrayHole attack**

1. INTRODUCTION

Gone are the days when people had to work with the stable infrastructure networks. Today MANET, a mobile ad-hoc network has taken place to ease instant network requirements. This type of network promises many advantages in terms of cost, flexibility compared to the infrastructure based networks. MANET is an autonomous network with no central administration. Also, there isn't fixed topology in MANET. Nodes are wirelessly connected with all other nodes within the MANET. Being mobile, these nodes can move from one network to any other network anytime. Also other nodes from outside the network can enter in a particular network. As the nodes keep on moving from network to network, topology of MANET keep changes. These nodes can not only act as a host but also act as a router and allow other users to communicate through their mobile devices.In MANET all network activities like discovering the routing path, message delivery etc. are performed by nodes only. For these activities MANET use different routing protocols such as DSDV, DSR and AODV etc.

The open medium access, dynamically changing network topology and absence of any central administration makes MANETmore vulnerable to various types of attacks than a typical wireless network. One of such attacks is packet dropping attack. GrayHole attack may occur due to malicious/misbehaving node. In GrayHole attack, a malicious node sometimes acts as a normal node and passes the packets without any damage or dropping. But sometimes same node acts as a malicious node and start dropping the packets. Due to this nature of the malicious node it becomes very hard to detect the GrayHole attack. There must be some techniques to deal withsuch type of attacks. In past a lot of work have been done on detection and prevention of GrayHole attack. But still today there is no assurance for trustworthy countermeasure against the GrayHole attack. In this paper, I have studied different methods for the detection and prevention of GrayHole attack and compared them on the basis of different parameters.

2. ROUTING PROTOCOLS

In ad-hoc network nodes can move freely from one location to another. So the path established by a source may not exist after a short interval of time if any intermediate node moves from one network to another. Routing determines the path from source to destination so that the nodes can communicate. There are three types of routing Protocols for ad-hoc networks,

A. *Reactive protocols*

Theyare known as demand driven protocol meaning that they find routing path only when it's needed. To discover new route these protocols makes use of route request androute reply messages. After receiving route reply messages the route is established by the nodes. Route discovery makes a big delay and it is the major drawback of these protocols.

B. *Proactive protocols*

Theyare Table Driven Protocols. These protocols constantly maintain the network topology. In a network every node contains the information of the neighbors. This information is stored in different tables and these tables are updated according to the changes in the network topology.

C. *Hybrid protocols*

The combination of proactive and reactive protocols is a Hybrid protocols. These protocols make use of distance-vector for more precise metrics to establish the best paths to destination networks. In this network each node has its own routing zones and the size of the zone is defined by a zone radius i.e. number of hops in one zone. Each node keeps a record of

routing information for its own zone. In hybrid protocols, routers only maintain information about the adjacent routers. Source initiates the establishment of routes to a given destination on demand during reactive operation.

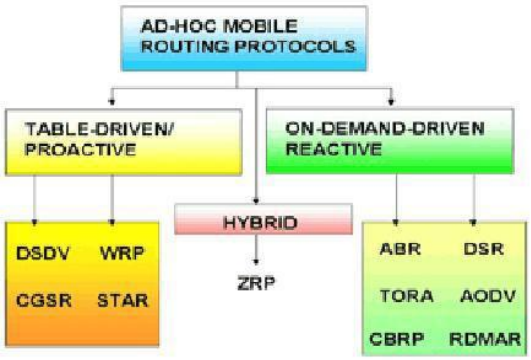

Fig 1 Classification of MANET routing Protocol

3. AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL

Ad-hoc on demand distance vector protocol [1] is one the main routing protocols broadly used in MANET. It is a reactive or on demand routing protocol. It aims to minimizethe requirement of system-wide broadcasts to its extreme. Itdoes not maintain routes from every node to every other nodein the network rather they are discovered as and when needed& are maintained only as long as they are required.

When a node wants to send a data packet to a destinationnode, the entries in route table are checked to ensure whetherthere is a current route to that destination node or not. If it isthere, the data packet is forwarded to the appropriate next hoptoward the destination. If there is no route to the destination, the route discoveryprocess is initiated. To discover a new route AODV initiates a route discovery processusing Route Request (RREQ) and Route Reply (RREP). Thesource node will create a RREQ packet containing its IPaddress, its current sequence number, the destination's IPaddress, the destination's last sequence number andbroadcast ID. The broadcast ID is incremented each time thesource node initiates RREQ. The source node broadcasts theRREQ packet to its neighbors and then sets a timer to waitfor a reply. When the destination node or an intermediate node with aroute to the destination receives the RREQ, it creates theRREP and unicast the same towards the source node usingthe node from which it received the RREQ as the next hop.When RREP is routed back along the reverse path andreceived by an intermediate node, it sets up a forward pathentry to the destination in its routing table. When the RREPreaches the source node, it means a route from source to thedestination has been established and the source node canbegin the data transmission. Since there is movement of nodes in mobile ad hoc networkand if the source node moves during an active session, it canreinitiate route discovery mechanism to establish a new routeto destination.Conversely, if the destination node or some intermediatenode moves, the node initiates RouteError (RERR) message to the affected active nodes on its route backward to the source node. When RERR is received bythe source node, it can either stop sending the data orreinitiate the route discovery mechanism by sending a newRREQ message if the route is still required.

4. NETWORK SECURITY ATTACKS ON MANET

There are mainly two types of attacks that can happen over a MANET.

1. Active attack
2. Passive attack

Passive attacks are of those types which cause no interruption to the functionality of the network. The main target of such attack is to get information about the data being exchanged over the network without interrupting the data transmission process. Data confidentiality may be at danger when such type of attack takes place over the network. As this type of attacks cause no damage or interruption to the network functionality, it becomes impossible to be alerted about passive attacks.

Unlike passive attacks, Active attacks don't just keep watch on the network data being transmitted over the network but it can damage or alter the data being transmitted. These types of attacks can be classified in to two types, internal attack and External attack. Internal attacks can be initiated by the malicious nodes which are already a part of the network. External attacks are performed by the attacker node from outside the network.

Passive attacks	Snooping, Eavesdropping, Traffic analysis,Monitoring
Active attacks	Wormhole, Black hole, Gray hole, Information disclosure, Resourceconsumption, Routing attacks

In this paper, an active attack which is GrayHole attack is studied. Brief information about GrayHole attack and various techniques to deal with the GrayHole attack are described in preceding sections.

5. GRAY HOLE ATTACK

A Gray Hole attack is an active attack which takes place at the network layer in the MANET. This type of attack cause damage or interrupt the network functionality by dropping the data packets which are being transmitted.GrayHole is a node that selectively drops the packet and after sometime it will start forwarding the packets normally like any other nodes in the network.

Gray Hole attack takes place in two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a shortest route to the destination, with the intention of intercepting the packets. But in actual there is no such short route to the destination exists. In the second phase, after trapping the source node maliciously, GrayHole will receive the packets from the source node and eventually start dropping the packets. As per its default nature, GrayHole attack will drop the data packets selectively without any certainty. Due to such nature, it becomes hard to detect the GrayHole as it can act both as a normal node as well as a malicious node. A GrayHole may exhibit its malicious activities in different ways. It may drop the packet coming from a particular source only and passes the other packets from other node normally. It may drop all the packets for some particular time period and after that time limit it may act normally and pass the packets toward its destination.

Impact of GrayHole Attack on Ad-hoc Network [2]

When a Gray Holeattack takes place in the ad-hoc network, performance of ad-hoc network decreases. GrayHole attack decreases certain performance metrics of the network such as packet delivery ratio, end to end delay & packet loss ratio.

- **Packet delivery ratio (PDR):**It is ratio of packets sent from the source to packets received at the destination.

PDR =Ps/Pr

- **End to end delay (e2e):** it refers to the time taken for a packet to be transmitted across a network from source to destination.

End to end delay D =Td-Ts

- **Packet loss ratio:**It defines the packet dropped ratio when the network traffic fails to reach at the destination in a timely manner.

Packet loss, Pd= Ps-Pa

As stated above a GrayHole attack can interrupt the network functionality at a higher level and can cause a great inconvenience to the users and it is also very difficult to detect such attack. So here in section, various detection and prevention methods for GrayHole attack have been studied and compared with each other to find out an efficient and more secure method.

6. DIFFERENT WAYS FOR DETECTION AND PREVENTION OF GRAY HOLE ATTACK

6.1 Detection and removal by source node/ destination node/ neighborhood node

Detection and removing of GrayHole attacks processes are [4, 5]:

6.1.1 Detection process for GrayHole attack by source node

- Divide data packets into k equal parts.
- Send a message to destination containing number of messages.
- Broadcast messages to all neighbors of route.
- After ensuring that destination node knows count of messages, source begins sending of data.
- Set up a timer until getting number of data packets that destination receives.
- If number of announced data packets from destination is less than a limit, initiate removing process of GrayHole attack.
- Also if no message is received from destination after timer is terminated, start Gray Hole removing process.

6.1.2 Detection process for GrayHole attack by destination node

After knowing the number of data packets sent from the source node, timer is set to zero and start counting data packets being received from the source node. After timer gets out, received data packet numbers is sent back to source node. If there is any difference in numbers, it defines the presence of gray hole attack.

6.1.3 Detection process for GrayHole attack by neighborhood nodes

On getting monitoring message from source node, each node starts a counter to count number of data packets of its neighbors.

6.1.4 Remove process for GrayHole attack by source node

- Source node gets vote of one node's neighbors about the maliciousness.
- According to the votes of neighbors, starts counter for malicious node in FindMalicious table.
- If votes of neighbors about maliciousness exceeds from a limit, source enters that node in Gray table and finds a new route to destination. Also announces to the network that node is a malicious one.

6.1.5 Remove process for GrayHole attack by neighbor nodes

When they get monitoring message, they start counting number of packets that malicious node sends. If number of passed messages is less than a limit, inform about it to source node.

6.1.6 Advantages

- Due to limit for identifying malicious nodes, number of mistakes in identifying GrayHole attack is decreased. This limit is threshold which is the probability of packet tobe dropped by a node. Packet dropping may occur due to overhead, lack of CPU cycles, buffer space or bandwidth, congestion or collusion to forward packets.
- This method can detect both black and GrayHole attacks and also can detect selfish node.

6.1.7 Disadvantages

- All nodes have to always monitor each other which cause high overhead for network and energy consumption per node is also increased.
- Detection process for malicious nodes is veryslow and a lot of data loss is possible until malicious node is detected.

6.2Using watchdog

In [6] malicious node can be detected using a watchdog timer. Each node monitors its next node in the route. If any packet forwarding misbehavior or any packet dropping in a predefined period of time for its next node is found, the next node is announced as a malicious node to the source.

6.2.1Advantages

- It is very simple method. One node need just listen to its next node in the route.

6.2.2Disadvantages

- Each node must monitor its next neighbor node.
- Source node has to trust the other node's information about one node's misbehavior.
- As there isn't any threshold value is used, it increases numbers of mistakes to find GrayHole attacks.

6.3 Using SCAN approach

SCAN [7] makes use of two ideas to protect AODV in MANET as mentioned below:

a. **Local collaboration**:Basic idea behind this approach is that each nodemonitors each other and also sustains routing tables for each other. Every node has a token that provides authentication for the network. If one node is suspected to be malicious, other nodes revoke its token and alert token revocation to all nodes in network. Malicious node is inserted in token revocation list. So, the malicious node cannot have any access to the network.

b. **Informationcross-validation** Incoming routing packets checked by the each node. As each node have all the information about its neighbors' routing table, it can cross-check the overheard transmissions of them. Fig. 1 shows this action, node M uses routing tables of X and Y, if X or Y announces a new fault routing update, M compares routing tables of two neighbors and if any misbehavior found, it announces that node as malicious to the network and revokes its token.

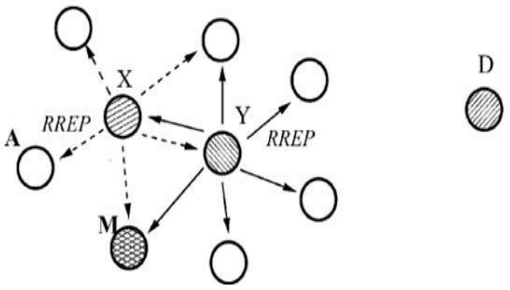

Fig 2 Cross-checking routing updates of neighbors [10].

6.3.3Advantages

- A token is used which authenticates the node to the whole network. Without a valid token, a node cannot participate in the network and using token enhances the security of network to some extends.

6.3.4Disadvantages

- Mobility of nodes makes changes in routing tables which causes probable mistakes in finding malicious nodes. Also it is mandatory to update the table entry of neighbors in certain time periods.

6.4Using Strong Nodes

In [7], a method is defines which uses some additional nodes, Strong nodes, which help source and destination to find GrayHole attacks. These nodes are assumed to be trustful and also capable of tuning its antenna to large ranges as well as short ranges. Each normal node is within the range of one of these strong nodes. Strong nodes help the source and the destination nodes to perform an end-to-end check and get to know whether the data packets are reached to the destination or not. If any difference is found in number of messages sent from source and received in destination, strong nodes ask the nodes in their area about the monitoring results of one node's behavior. If the checking results show misbehavior according to the votes, then the backbone network runs a protocol which can detect black or GrayHole attack. At the end announces malicious node to the network by broadcasting messages.

6.4.1Advantages

- Due to strong nodes ratio of monitoring of neighbors is decreased. Only nodes in particular area of malicious node have to monitor.

6.4.2Disadvantages

- Strong nodes are assumed to be trustable and there isn't any solution considered for attacks.
- There is no threshold value for detection of maliciousness of one node which increases mistakes to distinguish between normal and strong nodes.

6.5Using Signature attack

In [8], Gray Hole attack is implemented. Both the scenarios i.e. with and without the presence of malicious nodes is implemented and packed delivery ratio is calculated for both scenarios. In malicious scenario packet delivery ratio is comparatively less. Using an algorithm such malicious nodes can be identified.

Simulations results are in two format i.e. NAM and trace file. After simulation of both scenarios, we get two trace results from normal scenario andmalicious scenario accordingly. Using these trace results a new detection algorithm is proposed which uses these two trace files to detect malicious node.

The algorithm analyzes the data collected from both trace files. First trace file is for normal scenario which defines legal behavior. In malicious scenario, some nodes are set as malicious. Now trace file behavior of these malicious nodes is compared with legal behavior which defines a specific behavior pattern of Gray Hole attack for malicious node. This behavior pattern is called signature of attack which is used to detect malicious node.

When user defines any scenario then its trace file is compared with previously created signature of attack. If the signature is matched with trace results of some nodes from user defined scenario then it declares those specific nodes as malicious.

In this method, a main criterion for identification of a malicious node is the creation of signature of attack from malicious scenario and it is compared with a normal scenario. Nodes which drops packet according to signature are misbehaving nodes, while remaining nodes are normal behaving ones.

6.5.1Advantages

- As we are already having a signature of attack, finding out misbehavior becomes very easy by comparing the signature of attack and trace file of user defined scenario.

6.5.2Disadvantages

- We must have to implement both normal and malicious scenario to apply this approach.

6.6 Detection using four reliable steps

The method introduced in [9] detects malicious nodes in four steps:

6.6.1 Data collection of neighbors: Each node collects information about all neighbors and stores it in its DRI table. If any neighbor node is found with from and through table fields with 0values then that node is assumed as a malicious node.

6.6.2 Local anomaly detection: Now source node selects a Cooperative Node (CN). This node contains both DRI fields filled with 1 value and is a trusted node as source previously sent to and received data from it. Source node broadcasts RREQ to CN as destination, then source asks to CN if it has received RREQ from malicious node, if it receives then source node removes that node from malicious nodes list as it does not drop RREQ packets. But if CN does not receive RREQ packet from malicious node, source node increases its maliciousness.

6.6.3 Cooperative anomaly detection: To avoid mistakes in malicious node detection, source node sends a cooperative detection request to all neighbors of malicious node. On receiving this request all neighbors send RREQ message through that node to source node as destination. That node returns RREP to neighbors. These neighbor nodes also sends a probe packet from malicious node to source and also another packet from another path to announce source about that packet, if source does not get probe packet. Until three times of sending probe packets by neighbors does not mark that node as Gray Hole attack and after three times marks that node as an attacker.

6.6.4 Global alarm sending: Finally, source node announces a nodeas a Gray Hole attacker.

6.6.5 Advantages

- Nodes do not need to monitor each other, so does not consume a lot of energy.
- Three times of checks for a node increases surety and decreases mistakes.

6.6.6Disadvantages

- Increases the speed of distinguishing a Gray Hole attack increases and overhead for each malicious node detection is high.

7. COMPARISON OF METHODS

Method	Detection of gray hole attack	Detection of black hole attack	Mistakes in detection of attacks	Detection of misbehavior in source node	Overhead
1. Detection and removal by source node/ destination node/ neghbourhood node	Yes	Yes	Few - because of using thresold value for packets.	According to votes of neighbours	Find malicious and Gray/Black hole table and overhead of voting from neighbors
2. Detection using watchdog	Yes	Yes	Many - because it does not use any thresold value for packets	No	No
3. Based on Destination Sequence Number	Yes	Yes	Few - because first RREP with higher DSN will alsways from a malicious node	No	Find malicious and Gray/Black hole by comparing DSN with thresold value
4. Using SCAN approach	Yes	Yes	Many - because it does not use any thresold value for packets	No	Uses a token for each node
5. Using Strong Nodes	Yes	Yes	Many - because it does not use any thresold value for packets	Yes	Strong nodes with stronger signal ratio
6. Using Signature of attack	Yes	Yes	Few - because comparison with signature of attack	By comparing user defined scenario trace file with signature of attack	Uses a normal and malicious scenario results
7. Detection using four reliable steps	Yes	Yes	Few - using three times channels	Yes	DRI tables, probe packets

8. CONCLUSION

Gray Hole attacks are very big security problems in MANET. Gray Hole attackdrops packets in transmitting step. Detection of gray hole is more difficult because the attacker works as normal node then starts dropping of data. In this paper, I have introduced

some methods to detect Gray Hole attacks, pointed out their advantages and disadvantages and at the end, these methods are compared on the basis of common parameters. Most of these methods suffer from overload and low speed which is a research area of future work against these attacks. Future work is based on developing an efficient method for Gray Hole detection and prevention.

REFERENCES

[1] A Survey of Routing Protocols in Mobile Ad Hoc Networks by Sunil Taneja and Ashwani Kush, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010, ISSN: 2010-0248

[2] SIMULATION OF SECURE AODV IN GRAY HOLE ATTACK FOR MOBILE AD-HOC NETWORK by Onkar V. Chandure, Aditya P. Bakshi, Saudamini P. Tidke, Priyanka M. Lokhande, International Journal of Advances in Engineering & Technology, Nov. 2012.IJAET, ISSN: 2231-1963

[3] A Modified Grayhole Attack Detection Technique in Mobile Ad-hoc Networks by Mangesh M. Ghonge and Pradeep M. Jawandhiya, International Journal of Advanced Research in Computer Science, Sept –Oct, 2010, ISSN No. 0976-5697

[4] Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks by Sukla Banerjee, Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA. ISBN: 978-988-98671-0-2

[5] Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad-hoc Networks by Shalini Jain, Mohit Jain, HimanshuKandwal, 2010 International Journal of Computer Applications (0975 – 8887)Volume 1 – No. 7

[6] Mitigating Routing Misbehavior in Mobile Ad-hoc Networks by Sergio Marti, T.J.Giuli, Kevin Lai, Mary Baker, Department of Computer Science, Stanford University, Stanford, CA 94305 U.S.A.

[7] Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET byMarjanKuchaki Rafsanjani, Zahra ZahedAnvari and ShahlaGhasemi, IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[8] Intrusion Detection System for AODV Protocol in MANET by Ms. S.R. Shirke, Prof. (Dr.) V. R. Ghorpade, International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, May - 2013 ISSN: 2278-0181

[9] A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks byJaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, 1-4244-0983-7/07/$25.00 ©2007 IEEE ICICS 2007.