Detection and Prevention Techniques for Gray Hole Attack in MANET: Review

Amit A. Bhusari
Faculty,MCA Dept.
Dr. B.N.C.P.E.Yavatmal

Pradeep M. Jawandhiya, Ph.D.
Profeesor, Head comp. Engg. Dept
J.C.O.E.T. Yavatmal

ABSTRACT

(Mobile Adhoc network) is a infrastructure less network used for wireless communication. MANET can be built with the mobile nodes which can move anywhere at any time. This results into the dynamic topology of MANET. Each node is responsible for routing the message from one node to the other like a router, causes network more vulnerable to the different attacks. In this paper we will discuss about the gray hole attack type of DOS [2] attack, detection and prevention technique which disrupt the various network parameter as throughput, PDR and degrades the performance of the network.

INDEX: Gray hole attack, DOS attack

INTRODUCTION: MANET is a collection of mobile nodes that communicates with adjacent nodes without fixed infrastructure. It is decentralized network where the nodes act as a router to exchange the messages to other. A node can joins and leaves the network rapidly and it makes the topology dynamic. The dynamic topology [1] causes the security issues for MANET. Gray hole is a packet drop attack in which malicious node misbehaves the source node to forward the packets to destination and drops the packets coming from the source node or any intermediate nodes. Gray hole is widely used on AODV (Adhoc on demand distance vector) routing protocol.

Gray hole Attack: Gray Hole attack is the attack on the adhoc network. In Gray Hole Attack [1] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it’s routing table. Otherwise, nodes initiates a route discovery process by broadcasting *Route Request* (RREQ) message to it’s neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A *Route Reply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

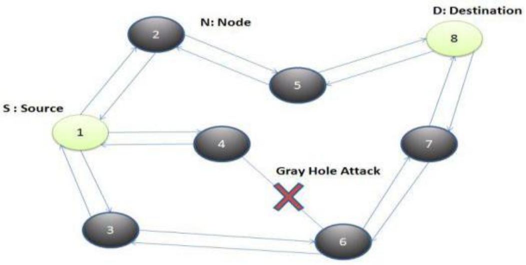

Fig.1 Gray hole attack

The gray hole attack has two phases:

Phase 1:
A malicious node exploits the AODV (Adhoc on demand distance vector) routing protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.
Phase 2:
In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray hole attack is a difficult process. Normally in the gray hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack.

RELATED WORK:

Dhamande C.S. & Deshmukh H.R. [4] proposed a mechanism to prevent the Gay hole attack on AODV protocol by setting the waiting time for the source node SSN (Source sequence number) to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node ID i.e. NI n RR-Table until the computed time exceeds.
Vishnu K. and Amos Paul [7] proposed a mechanism to detect and remove the attack on Source node & intermediate node. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address.
Marjhan Kuchaki Rafsanjani, Zahra Zahed Anvari & Shahla Ghasemi [3] proposed different methods for detection & prevention Black hole & Gray hole. In first technique if

number of packets announced by destination are less than the packet transmitted from source to destination then the packets are discarded. In second technique they proposed a methodology for detecting a malicious node based on packet forwarding misbehavior or packet dropping behavior within predefined period of time. They suggested the use of Watchdog timer for counting a time for transmission of packets from source to destination. In third method they proposed the local collaboration and cross validation method in which the nodes checks out the routing tables of the other node to locate the misbehavior. In fourth method they proposed the use of strong nodes to detect the misbehavior by source and destination nodes by assuming the trustful nodes which are in the range of these strong nodes. In Tenth method they proposed to use of Data Routing Information table (DRI table) which sores all entries of routing maintained by each node. If the DRI table fields from and through are zero then corresponding nodes are considered as malicious. Field from indicates which node has sent the message and the field through indicates that which intermediate node has propagated the message up to the destination.

Megha Arya and Yogendra kumar Jain [8] proposed the IDS based method IDSAODV for detecting and preventing Gray hole attack in network.

Omkar Chandore and Prof. V.T. Gaikwad [6] assume three kinds of nodes for detecting and preventing gray hole. IN (Initiator node) send the RREQ and for this it receives the RREP from various nodes along SN (suspected node). By using DRI table IN probes the CN (cooperative node) and if finds the malicious then discard the route.

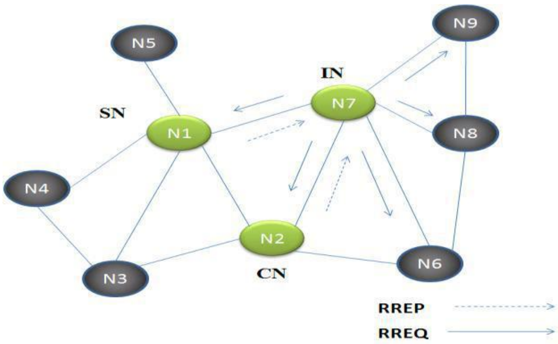

Fig. 2
Process of finding malicious node

The Gray Hole attack causes the instant RREP for the RREQ send by the source node. The destination node sends the RREP by increasing the sequence number.

Higher the sequence number , more fresh route is consider to route the message. And hence when the source node receives the RREP with more high sequence number it start sending the packets through that path considering the route as genuine. And this causes the gray hole attack as malicious node can send the quick response to RREQ.

We compare the different methods with following metrics.

CONCLUSION:

Network security is the biggest challenge that networks are facing today. Gray hole is kind of DOS attack which cause the damage to an entire network. Our aim is to discuss a method to detect and prevent the attack with fewer networks overhead. In this survey paper we have tried to review the different methods to detect and prevent the Gray Hole attack.

Method	Mistakes in Detection Attack	Overhead
1.A Competent way to diminish the burnt of Gray hole attack in MANET	Few	Managing Routing entries in RR
2.Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks	Few	Maintenance of Allocation table
3.Detecting/Removal of cooperative Gray hole attack in MANET	Few	Finding malicious nodes and overhead of voting from neighbors
4. Mitigating routing behavior in MANET	Many as not consider any limit for packet	No overhead
5. Network Layer Security in MANET self organized	Many as not consider any limit for packet	Uses token for each node
6. Cooperative Black hole and Gray Hole attack in MANET	Many as not consider any limit for packet	Strong nodes with stronger signal ratio
7. A mechanism for detection of Gray hole attack in MANET	Few	DRI table, Probe table
8. Gray hole attack and its prevention in MANET	Few	IDS
9. Detection and Prevention of Gray Hole attack in MANET by using AODV routing Protocol	Few	Maintaining Three kinds of nodes IN,CN and SN

REFERENCE:

[1] V. Shanmugnathan, Mr. T. Anand M.E. “A survey on Gray Hole attack in MANET” IJCNWC ISSN 2250-3501 December 2012

[2] Mangesh m.ghonge, Pradip M. Jawandhiya, Manoj Tambakhe,Amol Bhosle “ Gray Hole attack Detection technique in MANET” ICCA 2010.

[3] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Sha hla Ghasemi “Methods of Detecting and Preventing Black Hole/Gray Hole attacks on AODV based MANET” IJCA Nov 2010.

[4] Dhamande C.S and Deshmukh H.R “A Competent to diminish the brunt of gay hole attack in MANET” Vol.2, Issue 2 Mar 2012.

[5] Pradip M. Jawandhiya, Mangesh m.ghonge, DR. M.S Ali and Prof. J.S Deshpande “ A Survey of Mobile adhoc network attacks” Vol.2, No.9, Sep 2010.

[6] Onkar V.Chandure, Prof V.T.Gaikwad “ A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET” IJCSIT , Vol.2, No.6, Jul 2011.

[7] Vishnu K and Amos J Paul "Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" IJCA Vol.1, No.22 Jan 2010.

[8] Megha Arya and Yogendra Kumar Jain "Gary hole attack and prevention in Mobile Adhoc Network" IJCA Vol.27, No.10. Aug 2011.

[9] G.S Mamatha , Dr.S.C. Sharma "A Highly Secured approach against attacks in MANETS" IJCTE Vol.2, No.5, Oct 2010.

[10] Z. Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu "Risk Aware mitigation for MANET Routing attacks" IEEE Transactions on Dependable and Secure Computing Vol.9, No.2 Mar/Apr 2010.

[11] A.Saini, R. Sharma, "A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.