Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.105 – 108

REVIEW ARTICLE

Review Paper on Detection and Prevention Techniques of Gray-Hole Attack in Manet

Ashok Desai[1]

[1]L.D. College of Engineering, Ahmedabad, India

[1] *Ashok.desai64@gmail.com*

Abstract— MANET is a kind of wireless ad hoc network. It is a self-configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. In other words, ad hoc network do not rely on any fixed infrastructure. 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, detection and prevention technique which disrupt the various network parameter as PDR, throughput and degrades the performance of the network.

Key Terms: - Manet; aodv; dsr; gray-hole; RREQ; RREP

I. INTRODUCTION

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism.

Active Attacks: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Both passive and active attacks can be made on any layer of the network protocol stack.

Passive Attacks: Passive attacks are the attack that does not disrupt proper operation of network. Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is Also able to interpret data gathered through snooping .Detection of this attack is difficult since the operation of network itself does not get affected.

II. GRAY HOLE ATTACK

Gray Hole attack is the attack on the adhoc network .Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data. In Gray Hole Attack 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 its routing table. Otherwise, nodes initiate a route discovery process by broadcasting *Route Request* (RREQ) message to its neighbours. 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. We now describe the gray hole attack on MANET'S.

III. DSR PROTOCOL

DSR is completely on-demand ad hoc network routing protocol collected of two parts: Route Discovery and Route Maintenance. Here, the basic form of Route Discovery and Route maintenance in DSR is described. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to discover a route; this node is known as the initiator of the Route Discovery, and the destination of the packet is known as the Discovery's target. The initiator transmits a Route Request (RREQ) packet as a local broadcast, specifying the target and a unique identifier from the initiator. Each node receiving the Route Request, if it has recently seen this request identifier from the initiator, rejects the Request. Otherwise, it appends its own node address to a list in the Request and rebroadcasts the Request. When the Route Request reaches its target node, the target sends a Route Replay (RREP) back to the initiator of the Request, including a copy of the gathered list of addresses from the Request. When the Replay reaches the initiator of the Request, it caches the new route in its Route Cache. Route Maintenance is the means by which a node sending a packet along a particular route to some destination detects if that route has wrecked, for example because two nodes in it have moved too apart. DSR is based on source routing: when sending a packet, the initiator lists in the header of the packet the complete sequence of nodes through which the packet is forwarded. Each node along the route forwards the packet to the next hop indicated in the packet's header, and attempts to confirm this by means of a link-layer acknowledgment or network layer acknowledgment. If, after a limited number of local retransmissions of the packet, a node in the route are unable to make this confirmation, it returns a Route Error to the original source of packet, identifying the link from itself to the next node was broken. The sender then removes this broken link from its Route Cache; for following packets to its destination, the sender may use any other route to its destination in its Cache, or it may attempt a new Route Discovery for that target if necessary.

IV. TECHNIQUES FOR PREVENTION AND DETECTION OF GRAY HOLE

In [1], S. Ramaswamy et al have presented an algorithm in which each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 'true' is represented by 1 and 'false' by 0. The first bit "From" denotes that the node has routed data packets *from* the node while the second bit "Through" denotes that the node has routed data packet *through* the node (in the Node field). The DRI entry is updated when any node received data packet from one of its neighbours or any node that sent data packets through one of its neighbours. The main drawback of this algorithm is that it is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. Also it is computational intensive as it takes O (n2) time whenever a node decides to send packets to another node. Moreover as the nodes in ad hoc networks move randomly, a non-malicious node which has recently moved in the vicinity of a node may be treated as black hole as it might not have done nay data transfer through or from the other neighbouring nodes. Hence the updating of DRI entry must also take into account the mobility of nodes.

In [7], Ashok M. Kanthe et al have presented an algorithm is to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates the peak value and checks whether reply packet sequence number is less than or not. This parameter is used to calculate the peak value a) Routing table sequence number. b) Reply packet sequence number. c) Elapsed time of ad hoc network which is analogous to current simulation time of simulator in simulation environment... d) Total number of reply packets received by the intermediate/neighbour /replying node. e) Reply Forward Ratio (RFR) of replying node.

In[9],Gao Xiaopeng have proposed novel A Novel Gray Hole attack detection scheme, in this scheme comprises three related algorithms. 1) The creating proof algorithm. Each node involved in a session should create a proof based on aggregate signature algorithm to demonstrate it has received a message. 2) The check up algorithm. When the source node suspects that the packet dropping attack has happened, for example, the destination reports that fewer packets have been received than that should be received under normal condition, it will invoke this algorithm to detect the malicious node. 3) The diagnosis algorithm. According to the evidences returned by the checkups algorithm, the source node could trace the malicious node.

In [8], P. Agrawal et al have proposed a technique for detecting a chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc networks. In order to gray hole attacks as well the total traffic volume is divided into a set of small data blocks. In this technique initially a backbone network of strong nodes is built over the ad hoc network. These strong nodes are assumed to be powerful in terms of computing power and radio ranges. Also each strong node is assumed to be a trustful one. Nodes other than strong nodes are considered as regular nodes. The major drawback of this approach is the assumption that some strong nodes which are powerful in terms of power, antenna range are available in the network. Such an assumption is not valid for all types of mobile ad hoc network. The optimality of backbone network in terms of minimality and coverage is not proved. Algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong nodes are always trusted node.

In [6], Ani Taggu et al have presented trace Gray algorithm for detecting gray hole, this algorithm based on agent based approach. Trace Gray requires that the next hop information be available to a node. With DSR routing, the proposed scheme uses route cache information to obtain the next hop information. Although the entire source route is available for a destination in the route cache, only the first hop node is used to avoid false positives. In this algorithm mobile agent has been enhanced with a timer. This timer is currently a function of MA code size + MA agent size. The basic premise in assigning the timeout period is based on the observation that during change of context of a MA, the size of the mobile code and data required for remote execution determines how large the timeout interval should be. As explained in the next section, if a mobile agent is unable to return to its home context *before* timeout, it indicates the presence of a gray hole.

In [10], Disha et al have proposed algorithm is based on a course based scheme. That is, a node does not observe every node in the neighbour, but only observes the next hop in current route path. In this scheme every node should maintain an FwdPacketBuffer, which is a packet digest buffer. The algorithm is divided into three steps: A) when a packet is forwarded out, its digest is added into the FwdPacketBuffer and the detecting node overhears. B) Once the action that the next hop forwards the packet is overheard, the digest will be freed from the FwdPacketBuffer. C) In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. The overhear rate in the Nth period of time is defined as OR (N), the percentage of the data packets which are actually received by the destination. We measure the overall throughput to analyze how gray hole attack impacts the performance of the whole network under different number of attackers and different gray magnitude.

V. CONCLUSION AND FUTURE WORK

In this paper we have discussed different techniques for detection of gray hole. A lot of work has been done in the detection and prevention of Gray hole attack which are still computational intensive. There is a further need to explore new types of coordinated attacks that can be launched on mobile ad hoc networks and design efficient techniques to detect and prevent them, as coordinated attacks can greatly reduce the system performance in a small amount of time and result in a larger damage

In our future work we proposed new algorithm based on trace gray and course based algorithm and Improve gray hole detection rate and reduce network load.

REFERENCES

[1] H. Fu, S. Ramaswamy,M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of CooperativeBlackhole Attack in Wireless Ad Hoc Networks,” In Proc. of 2003 Int. Conf. on Wireless Networks, ICWN’03, Las Vegas, Nevada, USA, 2003, pp. 570–575.

[2] Praveen Joshi “Security issues in routing protocols in MANETs at network layer” in sciencedirectG, 2010.

[3] G Sen, M. G Chandra, Harihara S.G., Harish Reddy, P. G, A Mechanism for Gray Hole Attack Detection in Mobile AdHoc Networks, ICICS 2007.

[4] J. Sen, M. Girish Chandra, P. G, S.G. G, and H. Reddy, “A distributed protocol for packet dropping attack detection in mobile ad hoc networks,” In G of IEEE International Conference on Telecommunications (ICT-07), May 2007, Penang, Malaysia.

[5] GCAI, Ping YI, Jialin CHEN, G WANG, G LIU, “An Adaptive Approch to Detecting Gray and Black Hole Attacks in Ad Hoc Networks”, Advanced Information Networking and Applications (AINA), 2010th IEEE International Conference.

[6] Ani Tagu and Amar Tagu “TraceGray : An Application-layer Scheme for Intrusion Detection in MANET using Mobile Agents

[7] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 53– No.16, September -2012.
[8] H. Deng, W. Li, and D. P. Agarwal, "Routing Security in Wireless Ad hoc Networks," IEEE Communications Magazine, Vol. 40, Number 10, Oct. 2002, pp. 70-75.
[9] Gao Xiaopeng, Chen Wei "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" 2007 IFIP International Conference on Network and Parallel Computing.
[10] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" IJTAE, JAN-2012.

