ISSN:0975-9646

A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET

Mahesh Kumar Kumawat, Jitendra Singh Yadav

Department of Computer Science Engineering
JECRC University, Jaipur, Rajasthan, India

***Abstract*— Mobile Ad Hoc Network (MANET) is a kind of wireless ad hoc network. It is a self-managed network of mobile routers connected by wireless links with no access point. Every mobile device or node in a network is independently controlled in autonomous mode. The mobile devices are free to move randomly and organize themselves arbitrarily. The wireless ad-hoc network is particularly vulnerable due to it's open medium nature, dynamic changes in network topology, co-operative algorithms, lack of centralized monitoring point and lack of a clear line of defense. In this paper we will discuss about the gray hole attack which disrupt the various network parameters used to check the performance, it's detection and prevention techniques.**

***Keywords*— MANET, Gray hole, Gray hole attack detection and prevention techniques, Mobile Adhoc Network, Security attacks, Routing protocols.**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes that cooperate and forward packets for each other. Such networks extend the fixed wireless transmission range of each node by multi-hop packet forwarding, and therefore they are ideally suitable for scenarios in which pre-deployed infrastructure support is not available. MANETs have some special characteristics such as unreliable wireless links used for communication between hosts, limited bandwidth, constantly changing network topologies, computation power and low battery power etc. Confidentiality and integrity of the data in network services can be achieved by assuring that security issues have been met. MANET often suffers from security attacks due to its basic features like open medium, cooperative algorithms, dynamic changes in network topologies, lack of a clear line of defense, lack of centralized monitoring and management point. While these characteristics are important for the pliability of MANETs, they introduce specific security concerns that are either absent or less intense in wired networks. MANETs are permeable to various types of attacks including passive eavesdropping, impersonation, active interfering and denial-of-service [1]. In this paper we will discuss about the gray hole attack which disrupt various network parameters used to check the performance, it's detection and prevention techniques.

II. GRAY HOLE ATTACK

Gray Hole attack is an active type of attack in which attacking node first agrees to forward packets and then fails to do so, which leads to dropping of messages. Gray Hole attack is one of the attacks in network layer which comes under the category of active attacks in MANET**.** In Gray Hole attack we can't predict the probability of losing data. In Gray Hole Attack a malicious node refuses to forward certain packets and merely drops them. The packets originating from a single IP address or a range of IP addresses selectively drops by attacker and forwards the remaining packets. Gray Hole nodes in MANETs are very dominant. Every node maintains a routing table that stores the next hop node information. When a source node wants to route a packet to the target node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes start 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 [2].

III. ROUTING PROTOCOLS

Routing protocols plays a important role in determining performance parameters such as packet delivery fraction, packet loss, end to end delay etc. of any ad hoc communication network. MANET routing protocols can be categorized into several parts as: table-driven/proactive, on demand driven/reactive & hybrid [Fig.1]. Depending on the routing topology table-driven are typically proactive protocols. Examples of this type include (DSDV) Destination Sequence Distance Vector. Source-initiated on-demand or Reactive protocols do not periodically modify the routing information. It is transmitted to the nodes mere when essential. For Example, (DSR) Dynamic Source Routing and (AODV) Ad Hoc On Demand Distance Vector. Hybrid protocols make use of both proactive and reactive techniques. Example of this type of technique is Zone Routing Protocol (ZRP). Some important Mobile Ad hoc Network routing protocols [3] are described below:

A. Adhoc On Demand Distance Vector (AODV) Routing Protocol

The Ad hoc On-demand Distance Vector (AODV) is a widely used simple, efficient and effective routing protocol. It typically minimizes the number of required broadcasts by creating routes on a demand basis, when a source node wishes to route a packet to a destination node, it uses the specified route if afresh enough route to the destination

node is available in its routing table. If not, it starts with a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated while it reaches an intermediate node with afresh enough route to the destination node specified in the RREQ ,or the destination node itself. AODV make a route using a route request / route reply query cycle. When a source node requires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes admit this packet update their information for the source node and set up backwards pointers to the source node in the route tables.

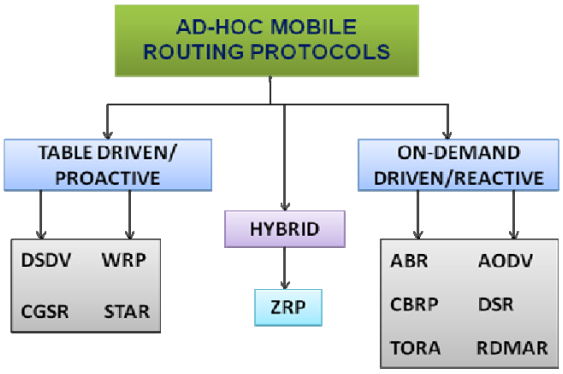

Fig 1: Routing Protocols for Mobile Ad hoc Networks

B. Dynamic Source Routing (DSR) Protocol

Dynamic Source Routing (DSR) is a type of reactive protocol. The main characteristic of DSR is source routing in which the source ever knows the complete route or path from source to destination. Route maintenance is applied to monitor correctness of established routes and to initialize route discovery if a route fails. The Dynamic Source Routing is an effortless and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. In DSR, intermedial nodes do not need to maintain the routing information.

C. Zone Routing Protocol (ZRP)

Zone Routing Protocol reduces the proactive scope to a zone entered on every node. In an incomprehensive zone, the maintenance of routing information is easier. Also, the amount of routing information that is never used is minimized. It can be categorized as a flat protocol because the zones overlap. Hence, best routes can be determined and network congestion can be reduced. ZRP comes under the hybrid protocol category. It uses the characteristics of reactive & proactive routing protocol.

D. Destination Sequenced Distance Vector (DSDV) Routing Protocol

In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. The destination node is assigned a sequentially numbered for each entry. These sequence numbers are enabled the mobile nodes to distinguish stale routes from new ones, thus avoiding the creation of routing loops. The table consistency is maintained periodically by routing table modifications in the network. Each node maintains a route to every other node in the network by Destination Sequence Distance Vector and there by routing table is formed. Each entry in the routing table stores sequence numbers which are even if a link exists; else, an odd number is used. The number is generated by the destination and the emitter requires sending out the next update with this number.

IV. TECHNIQUES FOR DETECTION AND PREVENTION OF GRAY HOLE

Several techniques have been proposed for detection and prevention of gray hole attack in MANET. H. Fu et al [4] proposed an algorithm in which an additional Data Routing Information (DRI) table is maintained by each node. In the DRI table, 'true' is represented by 1 and 'false' is represented 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). When any node received data packet from one of its neighbours or any node that sent data packets through one of its neighbours, the DRI entry is updated automatically. It is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attack. This is the main drawback of this algorithm. It takes O (n2) time whenever a node decides to send packets to another node. Nodes in ad hoc networks move randomly, a true node which has recently moved in the vicinity of a node may be treated as black hole as it might not have done any data transfer through or from the other neighbouring nodes. Hence the updating of DRI entry must also take into account the mobility of nodes.

A. M. Kanthe et al [5] proposed an algorithm to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates and checks the peak value whether reply packet sequence number is less than or not. The parameters used to calculate the peak value are: 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.

G. Xiaopeng and C. Wei [6] proposed a novel gray hole attack detection scheme. This scheme comprises three related algorithms which are: 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, it will invoke this algorithm to detect the malicious node. 3) The diagnosis algorithm. The evidences returned by the checkup algorithm, the source node could trace the malicious node.

H. Deng et al [7] proposed a technique for detecting a chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc networks. In order to detect gray hole attack the total traffic volume is divided into a set of small data blocks. Initially a backbone network of strong nodes is

built by this technique 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 are considered as a strong node otherwise ordinary node. The major drawback of this approach is the assumption that some strong nodes which are powerful in terms of power and antenna range are available in the network. The optimality of backbone network is not proved in terms of minimality and coverage. The assumption that strong nodes are always trusted node will fail if the intruder attacks strong nodes.

In trace Gray algorithm for detecting gray hole, is based on agent based approach. Trace Gray wants that the next hop information to 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 handy for a destination in the route cache, mere the first hop node is used to avoid false positives. In this algorithm mobile agent (MA) has been enhanced with a timer. This timer is currently a function of MA code size + MA agent size. The basic promise in assigning the timeout period is based on the observation that during change of context of a mobile agent, the size of the mobile code and data required for remote execution determines how large the timeout interval should be. The presence of a gray hole is indicated if a mobile agent is unable to return to its home context before timeout [8, 9].

D. G. Kariya et al [10] proposed an algorithm which is based on a course based scheme. In this scheme, a node observes only the next hop in current route path but does not observe every node in the neighbour. In this scheme FwdPacketBuffer is maintained by every node, it is also known as a packet digest buffer. The algorithm is divided into three steps: A) when a packet is forwarded out, its digest is stored 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) The detecting node should calculate the overhear rate of its next hop node and compare it with a threshold in a fixed period of time. The overhear rate of the Nth period of time is defined as OR (N), the percentage of the data packets which are actually received by the destination.

V. CONCLUSIONS AND FUTURE WORK

In this paper we have discussed different techniques for detection and prevention of gray hole attack in MANET. A lot of efforts have been done for the detection and prevention of gray hole attack which are still computational intensive. There is also need to explore new types of coordinated attacks that can be launched on mobile ad hoc networks, design and implement an efficient algorithm to detect and prevent them, because these attacks can greatly reduce the system performance in a small amount of time and result in a larger damage. In our future work we are going to propose a new algorithm based on trace gray and course based algorithm which can improve the gray hole detection rate and reduce network load as well.

REFERENCES

[1] A. Desai “Review Paper on Detection and Prevention Techniques of Gray-Hole Attack in Manet” International Journal of Computer Science and Mobile Computing Vol. 2, pp. 105-108, May 2013

[2] J. Sen, M. G. Chandra, Harihara S.G., H. Reddy, P. Balamuralidhar “A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks” ICICS 2007

[3] M. Gupta and K. K. Joshi “ A Review on Detection and Prevention of Gray-Hole Attack in MANETs” International Journal of Scientific & Engineering Research, Volume 4, Nov. 2013

[4] H. Fu, S. Ramaswamy, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of Cooperative Blackhole 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.

[5] A. M. Kanthe, D. Simunic, R. Prasad “A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks” International Journal of Computer Applications , Volume 53, Sep. 2012.

[6] G. Xiaopeng and C. Wei “A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks” IFIP International Conference on Network and Parallel Computing, 2007

[7] H. Deng, W. Li, and D. P. Agarwal, “Routing Security in Wireless Ad hoc Networks,” IEEE Communications Magazine, Vol. 40, pp. 70-75, Oct. 2002.

[8] A. Tagu and A. Tagu “Trace Gray : An Application-layer Scheme for Intrusion Detection in MANET using Mobile Agents”

[9] A. Desai, Prof. P. Ramanuj, “*Agent based mechanism for gray hole detection in MANET*”, International journal of innova-tive research & studies, May 2013, ISSN 2319-9725, vol 2, Issue 5.

[10] D. G. Kariya, A.. B. Kathole, S. R. Heda “Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method” IJTAE, Jan-2012.