ISSN 2229-5518

A Review on Detection and Prevention of Gray-Hole Attack in MANETs

Madhuri Gupta, Krishna Kumar Joshi

Abstract— MANETs are wireless network without having any fixed infrastructure. It is a self-organizing network of mobile routers connected by wireless links with no access point. In MANET nodes have limited sources like bandwidth, battery power and storage capacity. The mobile adhoc networks are vulnerable to Denial of Service (DOS) attacks. Grayhole attack is an event that degrades the overall network's performance by intentional malicious activity. Grayhole attack may drop packet coming from or destined to certain specific nodes in the network while forwarding all the packets for other nodes. In this paper we will discuss about the gray hole attack detection and prevention technique which disrupt the various network parameter used to check the performance.

Index Terms— Active attacks, AODV, Gray hole attack, DSR, DSDV, Mobile Adhoc Networks, Passive attacks, Reactive Routing Protocol, Security Threats.

1 Introduction

Mobile adhoc networks are multihop temporary wireless network without having any fixed infrastructure. It has different characteristics such as lack of centralized administric, distributed cooperation, changing topology without any existing infrastructure. Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of Network.

Dynamic topology, distributed cooperation and resource constraints are some of the unique features that exist in the adhoc network which inevitably increase the vulnerability of such network. Many features might be used to classify attacks in the adhoc networks. Example would consists look at the behavior of the attacks (passive vs active), the source of the attacks (external vs internal, the processing capacity of the attackers (mobile vs wired) and the number of attackers (single vs multiple).

Black hole attack is kind of DoS attack where black hole node can attract all packets by pretending shortest route to the destination. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source. Grayhole attack is a specialization variation of blackhole attack, where nodes switch their states from black hole to honest intermittently and vice versa. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to congestion. .Detection is difficult because the node's nature is not fixed, it can't predict that when node will be virulent and when it will become to normal node.

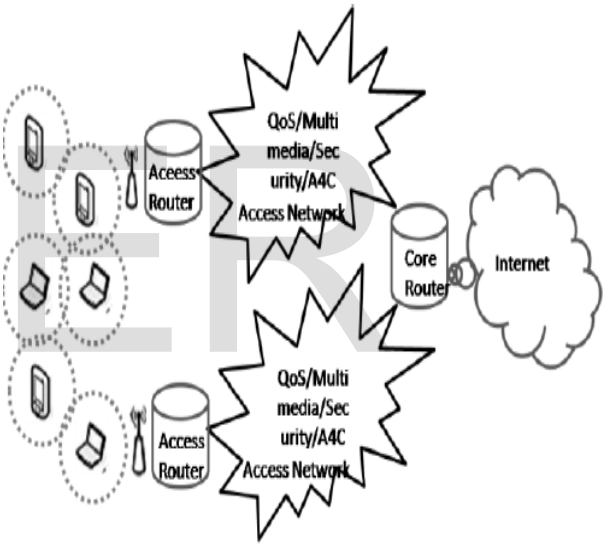

Fig 1: Mobile Ad hoc Networks

2 Routing Protocols

MANET routing protocols can be categorized into different classes as: table-driven/proactive, on demand driven/reactive &hybrid. Routing protocols play crucial role in determining performance parameters such as packet delivery fraction, end to end (end 2 end) delay, packet loss etc. of any ad hoc communication network .Depending on the routing topology .Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source -initiated on-depending on the routing topology. Reactive or source-initiated on-demand protocols do not periodically modify the routing information. It is transmitted to the nodes only when necessary. For Example, Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive techniques. Example of this type includes Zone Routing Protocol (ZRP).

Fig 2: Routing Protocols for Mobile Ad hoc Networks

Some important Mobile Adhoc Network routing protocols are described below:

2.1 Adhoc On demand Distance Vector (AODV) Routing Protocol

AODV is a very simple, effective and efficient Routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. It is typically minimizes the number of required broadcasts by creating routes on a demand basis.The Ad hoc On-demand Distance Vector (AODV) is the widely used protocol. 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 begins a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated until it reaches an intermediate node with afresh enough route to the destination node specified in the RREQ ,or the destination node itself. AODV builds routes using a route request / route reply query cycle. When a source node wants 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 accepting this packet update their information for the source node and set up backwards pointers to the source node in the route tables.

2.2 Dynamic Source Routing (DSR) Protocol

Dynamic Source Routing (DSR) is a reactive kind of protocol. The main feature of DSR is source routing in which the source always knows the complete route from source to destination. Route maintenance is used to monitor correctness of established route s & to initialize route discovery if a route fails. The Dynamic Source Routing is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. In DSR, intermediate nodes do not need to preserve the routing information.

2.3 Zone Routing Protocol (ZRP)

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

2.4 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. Each entry is sequentially numbered assigned by the destination node. The mobile nodes are enabled by these sequenced numbers to distinguish stale routes from new ones, thus avoiding the formation of routing loops. Routing table modifications are periodically transmitted throughout the network for maintaining table consistency. In Destination Sequence Distance Vector each node maintains a route to every other node in the network and there by routing table is formed. Each entry in the routing table consists of 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.

3 Security Threats In MANETs

Due to their highly adaptive nature MANETs are threatened by a lot of attack. Mainly the attacks can be classified as:

3.1 Passive vs. Active Attacks

Passive attacks are launched to lose value information in the targeted networks. Passive attacks are the attacks that do not disrupt proper operation of network Attackers snoop data exchanged in network altering it. An active attack attempts to change or delete the data being exchanged in the network , thereby disturbing the normal functioning of the network.

3.2 External vs 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.

Internal attacks are initiated by the authorized nodes in the networks and might come from both compromised and misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are using them to launch attacks against adhoc networks.

3.3 Mobile vs wired attack

Mobile attackers are the attackers that have the same capabilities as the other nodes in the adhoc networks. Since, they have the same resource limitations; their capabilities to harm the new operations are also limited.

Wired attackers are the attackers that are capable of gaining access to the external resources such as the electricity. Since

they have more resources, they could launch more severe attacks in the network such as jamming the whole network or breaking expensive cryptography algorithms.

3.4 Single vs Multiple attack

Single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities .If several attackers are colliding to launch attacks, defending the adhoc networks against them will be much harder. Colliding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operational including the security mechanisms.

Some dangerous attacks are described below:

Blackhole attack

Instead of relaying routing messages as the protocol requires, an attacker can drop them, in order to reduce the quantity of routing information available to the other nodes. This is known as blackhole attack by Hu, and is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a determined destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of creating the destination node unreachable or downgrade communications in the network.

Message tampering

An attacker can also modify the messages originating from other nodes before relaying them, if a mechanism for message integrity (i.e. a digest of the payload) is not utilized.

Replay attack

As topology changes, old control messages, though valid in the past, explains a topology configuration that no more exists. An attacker can perform a replay attack by recording old valid control messages and re-sending them, to make other nodes to update their routing tables with stale routes. This replay attack is successful even if control messages bear a digest or a digital signature that does not include a timestamp.

Wormhole attack

The wormhole attack is quite terrible, and consists in recording traffic from one region of the network and replaying it in a different area. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where nodes A and B are not themselves within transmission range of each other. Intruder node X hardly tunnels control traffic between A and B (and vice versa), without the changes presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that X is virtually not visible.

Rushing attack

An offensive that can be carried out against on-demand routing protocols is the rushing attack. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to minimize cluttering. The attack consists, for the opponent, in quickly forwarding its Route Request messages when a route discovery is initialized.

The Grayhole Attack

Gray Hole Attack a malicious node refuses to forward certain packets and drops them. The attacker specifically drops the packets originating from a single IP address or arrange of IP addresses and forwards rest of the packets. In MANET, gray hole nodes are very effective. Each node maintain a routing table which 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. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its 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.

The main criteria for identifying a malicious node is the estimated percentage of packets dropped, which is compared with a pre-established misbehavior threshold. Any other node that drops packets in excess of the pre-established misbehavior threshold is said to be mischievous, while for nodes whose percentage of dropping packets is below the threshold are said to be correctly behaving. A deviation of this attack is the gray hole attack, in which nodes either drop packets in a statistical manner (e.g. dropping 50% of the packets or drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or dropping them with a probilistic distribution.

Node S wants to send data packets to node D and initiates the route discovery process. It is considered that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately transmits the response to Source node. If the response from node 2 reaches first to node S then node S consider that the route discovery is complete, ignores all other reply messages and starts to send data packets to node 2. As a result, all packets through the node 2 are lost or consumed. In Gray Hole Attack a malicious node denies forwarding certain packets and drops them. The attacker selectively drops the packets coming from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective.

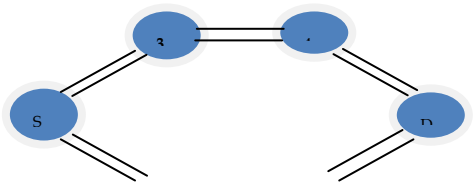

Fig. 3 Grayhole attack in MANET
In above figure
S- Source
D- Destination
1- Node, 3- Node, 4-Node
2-Malicious Node

4 Literature Survey

Mr. C.S. Dhamande et al [1] has proposed a technique which is summarised as: 1. to study the effects of Gray Hole attack in the light of packet delivery ratio (PDR), network load and End to End delay in MANET. 2. Simulating Grayhole attack using Ad- hoc On Demand Vector (AODV) Routing protocol. 3. Comparing the results of AODV protocol with and without Gray Hole attack. 4. Proposed new efficient security technique in AODV protocol as a counter measure of gray hole attack & also minimize the impact of gray hole attack

Onkar V. Chandure et al [2] presented a method which is used to detects and prevents the gray hole attack and also detects the behaviour of malicious node. This algorithm increases the packet delivery ratio and end to end delay. The performance of the network also increases by using SAODV in the algorithm.

Ashok Desai et al [3] proposed a mechanism wich is based on the mobile agent. In this method, each mobile agent has two parameters, one is expiry time and other is RTT time. In a fixed time interval mobile agent is generated from source node and move to the network. In a fixed time period, it should calculate the overhear rateof its next hop and compare it with the threshold value. In this algorithm, mobile agent does not visit each neighbour node but only observes the next node in current route. This algorithm detects the gray hole and minimizes the packet drop and congestion.

Avnesh Kumar et al [4] proposed a methodology which detect and prevent the group gray hole attack in the network. In this method, to detect the malicious node, the previous neighbour node and suspected node checks the two hop distance node for each possible path which goes towards the destination. So, firstly it stores the RREP packet at previous node and adds one hop distance of suspected node. This algorithm is based on destination based routing method. The major factor of this algorithm is to maximize the overall network throughput.

Sarita Chaudhary et al [5] proposed a technique for detection and removal of black holes and gray holes from the network. In this methodology, the concept of core maintenance of the allocation table is used in which when a new node adds in the network, it broadcasts a message as a request for IP address. Then backbone node randomly selects a IP addresss which are free in the network.The new IP address is allotted to the new node and sends an acknowledgement to the backbone node.

Onkar V. Chandure et al [6] proposed an algorithm that is based on security based technique which is used to recognise and eradicate the problem of gray hole attack. It works in two phases, firstly it develops a method which is used to handle the malicious node in the network and then routing protocol is used to recognise the gray hole attack.

A.M Kanthe et al [7] proposed approach uses effective way of providing security in AODV against grayhole attack. Proposed mechanism is to detect grayhole attack and eliminate the normal nodes with higher sequence number to enter in the black list .Effective decision making regarding black listing of nodes by keeping track on switching activity Adequate use of peak value and implementation of fresh approach of current elapsed time of adhoc network to make the proposed mechanism more efficient.

Shivani Sharma et al [8] Sequenced Queue based Routing Algorithm (SQRA) is proposed for Detection and Correction of Grey Hole attack by Implementing Intrusion Detection System. In this, the Detection of grey hole attack & Implements of corrective measures against it. Recovering system operation for grayhole attack. Implementing Sequenced Queue based Routing Algorithm for new routing table. Direct link established after recovering the attacks. The working of our algorithm is based on detection of broadcast IDs stored in the routing table of various intermediate nodes. The working of various nodes whoever depends upon how fast IDS responded to partially query and thus there is always a problem of overhead that may be encountered but our IDS we have limited this problem to much extend by using the application of distance vector routing algorithm.

C.S. Dhamande et al[9] proposed work is to compare effect of normal AODV and grayhole attack in the term of packet delivery ratio, network load and end to end delay, packet loss ratio in MANET and find the performance of the adhoc network. In this method using AODV as a counter measure of grayhole attack and minimise the effect of grayhole effect and improves the reliability and effectiveness of the adhoc network.

Shivani Sharma et al [10] proposed sequenced queue based routing algorithm for detection and correction of grayhole attack by implementing intrusion detection system.

Explaination of above review in tabular form-

S No	Year of Publication	Author	Techniques used	Simulator
1	Feb 2012	C.S. Dhamande H.R.Deshmukh	Implementation of AODV routing protocol, Procedure for finding the suspected node.	NS-2
2	Mar 2012	C.S. Dhamande H.R.Deshmukh	Compared the effects of AODV and gray hole attack in the pdr & etoe delay.	NS-2
3	Jul 2012	Avenash Kumar Meenu Chawla	Used destination based approach when there are more than one malicious nodes	NS-2
4	Aug 2012	Sarita Chaudhary, kriti Sachdeva	Core Maintenance of the allocation table is used.	OPNET
5	Sep 2012	A.M.Kanthe, Dina Simunic Ramjee Prasad	Detection of malicious node during route discovery process. This mechanism detects gray hole attack and eliminates the normal nodes.	NS-2
6	2013	Shivani Sharma Tanupreet singh	Sequence queue based routing algorithm for new routing table and intrusion detection system. Direct link established after recovering the attack.	NS-2
7	May 2013	Ashok Desai Purvi Ramanuj	Mobile agent based approach is used.	NS-2

Table 1. Summarization of previous approaches

5 Conclusions And Future Scope

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 Grayhole 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, because this attack 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 grayhole detection rate and reduce network load.

References

[1] Mr.Chetan S. Dhamande, Prof. H.R. Deshmukh ," *A efficient way to minimize the impact of gray hole attack in adhoc network*", International journal of emerging technology and advanced engineering, (ISSN 2250-2459, volume 2, issue 2,feb 2012).

[2] Onkar V. Chandure, Aditya P. Bakshi, Saudamini P. Tidke, Priyanka M. Lokhande, " *Simulation of secure AODV in gray hole attack for mobile adhoc network*" , International journal of advances in Engineering & Technology, Nov. 2012, ISSN: 2231-1963,vol. 5, Issue 1, pp. 67-76.

[3] Ashok Desai, Prof. Purvi Ramanuj, "*Agent based mechanism for gray hole detection in MANET*", International journal of innovative research & studies, May 2013, ISSN 2319-9725, vol 2, Issue 5.

[4] Avenash Kumar, Meena Chawla, "*Destination based group gray hole attack detection in MANET through AODV*", International journal of compuert science issues, vol. 9, issue 4, jul 2012.

[5] Sarita Chaudhary, Kriti Sachdeva, "*Discovering a secure path in MANET by avoiding black/ gray holes*", International journal of recent technology and engineering, ISSN: 2277-3878, volume-1, Issue 3, Aug 2012.

[6] Onkar V. Chandure, Prof. V. T. Gaikwad, "*A mechanism for recognition & eradication of gray hole attack using AODV routing protocol in MANET*", international journal of computer science and information technologies, vol. 2(6), 2011, 2607-2613, ISSN: 0975-9646.

[7] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad,"*A mechanism for grayhole attack detection in Mobile adhoc networks*", International journal of computer applications (0975-8887) volume 53- No. 16, September 2012.

[8] Shivani Sharma, Tanupreet Singh, "*An effective intrusion detection system for detection and correction of gray hole attack in MANETs*", International journal of computer applications (0975-8887, volume 68- No. 12, April 2013).

[9] Dhamande C.S., Deshmukh H.R., "*A competent way to diminish the brunt of gray hole attack in MANET* ", International Journal of Wireless Communication (ISSN: 2231-3559 & E-ISSN: 2231-3567, VOLUME 2, ISSUE 1, 2012)

[10] Shivani Sharma, Tanupreet Singh, "*Sequenced queue based routing algorithm (SQRA) for detection and correction of gray hole attack by implementing IDS*", Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013.