A Survey on Gray Hole Attack in MANET

V. SHANMUGANATHAN

Master of Computer Science and Engineering

K.S.R. College of Engineering

Tiruchengode, India.

Mr.T.ANAND M.E.,

Associate Professor, Department of CSE

K.S.R. College of Engineering

Tiruchengode, India.

***Abstract* – Mobile Adhoc Network (MANET) are used most commonly all around the world, because it has the ability to communicate each other without any fixed network. It has the tendency to take decisions on its own that is autonomous state. MANET is generally known for infrastructure less. The bridges in the network are generally known as a base station. A unified security solution is very much needed for networks to protect both route and data forwarding operations in the network layer. Security is an essential requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes eaves dropping and selective forwarding attack generally known as gray hole attack. In this paper we surveyed about the different types of attacks occurred in the network layer in MANET. Gray Hole attack is one of the attacks in network layer which comes under security active attacks in MANET.**

Keywords: MANET; Network layer; Gray hole attack.

I. INTRODUCTION

A Mobile Adhoc Network (MANET) can be defined as collection of mobile nodes. It does not rely on any fixed infrastructure. Since it is an infrastructure less network, the mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination and it is a self-configuring network. Gray hole attack is one of the attack in network layer which comes under security attacks. MANET can be used in different applications such as battlefield communication, emergency relief scenario etc. The nature of MANET is a dynamically changing process, due to its dynamically changing process its vulnerable for wide range of attack [11]. The Characteristics of MANET pose both challenges and opportunities in achieving security goals.

II. SECURITY GOALS OF MANET

The ultimate goal for MANET is to provide security solutions. To provide a solution for security reason there are some of the mechanism which is used to prevent, detect and respond. They are mainly Availability, Confidentiality, Integrity and Authentication. A brief explanation about these terms

A. Availability

The network should be available only for the authenticated users and this mechanism is used to protect against the kind of attacks like Gray hole, black hole, Information disclosure and Message altering.

B. Confidentiality

In MANET it is very hard to attain the confidentiality due to intermediate nodes routing, which can easily retrieve the information from the routing nodes.

C. Integrity

The transmission of information should be protected against any alteration and message modification.

D. Authentication

The network should be accessed only by the authenticated nodes such as Digital signature, Reply and Non repudiation.

III. NETWORK SECURITY ATTACKS

Since MANET is multihop in nature, it sturdily depends upon the cooperation among the nodes in the network [3]. The guarantee of cooperation among nodes is required. In recent times we have seen a variety of attacks have been identified and detected in the network. To provide a secure communication in the network we need to face the security challenges [6]. There are two major categories where we have to consider always in the security attacks, they are

A. Passive attacks:

A passive attack won't interrupt the normal operation of MANET, while data have been exchanged from the network [4]. The solely nature of passive attack is to identify the data exchanged in the network [12]. The attacker snoops the data exchanged in the network without altering it. Here the requirements of confidentially gets violated. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead [6]. There are two different kinds of attacks in the Passive attacks they are Eaves Dropping and Traffic analysis Monitoring. These are the two attacks which occur frequently in the passive attack. But when we use a powerful encryption method we can diminish the problem. Generally in the passive attack the task of the network is to monitor and analyze which type of communication is going on [2]. Here the Traffic analysis adversaries monitor packet transmission to infer important information such as a Source, destination and Source- destination pair [7]. Eaves dropping are another kind of attack that usually happens in the mobile adhoc networks. It aims to obtain some confidential information that should be kept secret during the Communication. The information may include the location, public key or even passwords of the nodes [13]. Because such data is very much useful and important to the security state of the nodes, they should be kept away from the unauthorized nodes.

B. Active attacks:

An Active attack always tries to modify the normal operation of MANET, which means the interruption have been made in the network, such as doing data interruption, modification, deletion and fabrication. Active attacks can be internal or external. The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of route request though it is not authenticated node so the other node rejecting its request due to these route requests the bandwidth is consumed and network is jammed [1]. Some of the security threats in the networks are Interruption, Interception and Modification. Some of the important active attacks are follows, they are Gray hole attack, Black hole attack, Worm Hole attack, Information disclosure and Routing attacks. These attacks can be happened at any point of time in the network. So it very much necessity to avoid such attacks in the network. Since it is very hard to find and detect these kinds of attacks, we need to rectify the problem by some of the powerful encryption techniques.

Other type of classification of attacks in the network is External attacks & internal attacks.

C. External attacks

Here the attacker aims to cause congestion in the network which can be done by propagating fake routing information or to disturb the nodes from providing services [5]. The attacker always disrupts the nodes to avail the services.

D. Internal attacks

In internal attack, the attacker needs to gain the access to participate in the network activities. Here the attacker comes with some malicious impersonation to get access from network as a new node.

IV. NETWORK LAYER ATTACKS

In Adhoc networks routing mechanism has three layers namely Network, Physical and MAC layers play a vital role [1]. As we all know MANETs are more vulnerable to various attacks, all these three layers suffer from different attacks and it cause routing disorders. The different kind of attacks in the network layer varied such as selective forwarding attack and modifying some parameters of routing messages

A. BLACK HOLE ATTACK

Most frequent attack happened here is stop forwarding the data packets. If we consider a malicious node which keeps waiting for its neighbor node to initiate RREQ packet [8]. As a node receives the RREQ packet, it will send a false RREP packet instantly with a modified high sequence number. So that the source node will assume that there is a new route is available towards the destination. The source node ignores the RREP packet from the other nodes including the correct nodes where it automatically denies the other nodes and it will start sending the packets towards the malicious nodes [14]. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets anywhere. This type of attack will happen frequently which is severe to find out and we use a detection techniques to solve these attacks. This attack is called a black hole where it swallows all the data.

B.GRAY HOLE ATTACK

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

- Dropping all UDP packets while forwarding TCP packets.

- Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node [9]. 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 [10]. 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.
The gray hole attack has two phases:

Phase 1:

A malicious node exploits the AODV 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 [8]. 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. The other name for Gray hole attack is node misbehaving attack.

V. ROUTING ATTACKS

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below:

- Routing Table Overflow: In this attack, the attacker tempts to create routes to nonexistent nodes.
- Routing Table Poisoning: The Compromised nodes in the network send fictitious routing updates packets sent to other uncompromised nodes.
- Packet Replication: In this attack, an adversary node replicates stale packets.
- Route Cache Poisoning: Each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past.
- Rushing Attack: On demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

VI. CONCLUSION

The Misbehavior of nodes have been caused severe damage and the whole network has been attacked in the network layer which is a Gray hole attack in MANET. Security is the most important feature for deployment in MANET. In this paper we have seen the number of attacks happened in network layer and especially for gray hole attack. Due to its dynamic nature, MANET prone to different limitations and weakness. To overcome this problem we have to use a new technique which should be designed. Our aim is to detect and mitigate the false node which is acting as a normal node, which is very hard to find out. But if we design a new approach of detecting the attacker node we can ensure that there is a safety in the network [9]. Once security is lost in the network then the entire network will get failed. Gray hole attack ultimately decrease the concert of the network. The main goal of the gay hole attack should be the improvement of security and as well as the performance of the network. During the survey we addressed how the attack has been happened in the network layer.

REFERENCES

[1] V. Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" IJCSE, Vol.3, No.2, Feb 2011.
[2] M. Wazid, Rajesh Kumar Singh, R.H.Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some available Detection Techniques" IJCA , Vol.3, No,2 Feb 2011.
[3] D. Manikantan shila, Yu Cheng , Tricha Anjali "Mitigating selective forwarding attacks with a Channel aware detection Approach in WMNS" IEEE Transactions on Wireless communications Vol.9, No.5, May 2010.
[4] A.Saini, R. Sharma, "A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.
[5] G.S Mamatha, Dr.S.C. Sharma "Network layer attacks and defense mechanism in MANETS- A Survey" IJCA Nov 2010.
[6] 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.
[7] 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.

[8] 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.

[9] 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.

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

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

[12] Stephen Carter and Alec Yasinac "Secure Position Adhoc Routing"

[13] 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..

[14] Q. Guan, F. Richard Yu, Shennimg Jing and Victor C.M Leung "Joint Topology on Vehicular technology" Vol.61, No.6, Jul 2012.