A SURVEY ON DETECTION AND PREVENTION TECHNIQUES FOR GRAY-HOLE ATTACK IN MANET

GEETHA PRIYA.S [1], JOY JEBA MERLIN.S [2], JEEVITHA.P [3], DHANALAKSHMI.M [4], KEERTHANA.D [5]

[1] GEETHA PRIYA.S, ASSISTANT PROFESSOR, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA
[2] JOY JEBA MERLIN.S, ASSISTANT PROFESSOR, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA
[3] JEEVITHA.P, STUDENT, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA
[4] DHANALAKSHMI.M , STUDENT, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA
[5] KEERTHANA.D.S, STUDENT, SRI KRISHNA COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA

ABSTRACT

A mobile ad-hoc network (MANET) is a infrastructure of very less dynamic network consists of wireless mobile node collection that communicates without the use of centralized network. Security in MANET is the important for the basic functionality of network. The malicious node does not advertises the shortest path to the destination node during the process of route discovery by forging the sequence number and hop count of routing message . In this paper we will discuss about the gray hole attack with various network parameters used to check the performance, it's detection and prevention techniques.

Keywords: - *AODV Protocol, Gray Hole attack, Routing protocols*

1. INTRODUCTION

In a MANET, a collection of mobile hosts form a temporary network with wireless network interfaces without the aid of any fixed infrastructure or centralized. Due to absence of fixed infrastructure with any kind and open wireless implementation of medium security is difficult. Manet each node functions as a host and also as router, forwarding packets for another node in the network. MANET is vulnerable to different kinds of attacks. These include active route interfering, imprecation and also denial of service one of many possible attacks in MANET is Black hole attack. In this attack, a malicious node sends a forged Route REPLY (RREP) packet to a source node that initiates the route discovery in order to pretend to be a end node. The malicious node with least hop route count and highest destination sequence number to the node which proceeds with the route discovery. MANETs are applicable to different types of attacks including passive eavesdropping, active interfering and denial of service. In this paper we will discuss about the gray hole attack and also black hole attack which disrupt various network parameters used to check the performance, it's detection and prevention techniques.

1.1 ROUTING PROTOCOLS

1. Proactive Routing Protocol- In routing table, here the mobile nodes periodically exchange routing information and also maintain the network topology information. It is called as table driven routing protocol
2. Reactive Routing Protocol- Here there is no exchange of Routing information sequentially. Instead a necessary path is obtained when it needed. It is called on demand routing protocol.
3. Hybrid Routing Protocol- It combines both proactive and reactive routing protocols features. A table driven approach is used within the routing zone of each node while an on demand approach is used for the nodes that are in the outside routing zone

2. AODV PROTOCOL

The Ad-hoc on demand distance vector routing is a protocol in which one of the widely used routing protocols in MANET. The route is established only when it is desired by the source node for packets of data. Whenever node needs a route to the destination, a route discovery process is initiated. The source node was flooded to the Route Request packet to its neighbors. The source identifier, destination reside in Route Request Packet. AODV make a route by a route request or route reply query cycle. It does not already have a route, a source node needs a route to a destination for which it broadcasts a route request (RREQ) packet across the network. The route tables update their information for the source node these nodes admit to their packets and set up backwards pointers to the source node.

3. CLASSIFICATION OF SECURITY ATTACKS

3.1 Passive attacks :

A passive attack does not changes the data transmitted within the network. But it includes the unauthorized “listening” to the accumulates data or network traffic in it. Passive attacker discover the important information from routed traffic but does not disrupt the operation of a routing protocol

3.2 Active attacks :

Active attacks are very severe attacks on the network that prevent message flow between the two nodes. However active attacks can be internal or external attacks. Active external attacks that do not belong to the network can be carried out by outside sources. Malicious nodes are part the network of Internal attacks where, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network to make changes such as modification of packets, DOS, congestion etc to help the attacker.

4. Attacks at Physical Layer

Some of the attacks identified at physical layer like eavesdropping, interference, and jamming etc.

4.1 Eavesdropping:

Eavesdropping is considered as the real time interception of a communication through phone, messaging and video conferencing to obtain the confidential information that should be kept secret during the communication.

4.2 Jamming:

Jamming is a special class of DOS attacks after determining the frequency of communication, which are initiated by malicious node. Jamming attacks prevents the reception of legitimate packets.

4.3 Active Interference*:*

An active interference is a denial of service attack which blocks the distorting communications or wireless communication channel.

5. Gray Hole attack

Gray Hole attack is behaves as a trusted node during the route discovery process and then may change its node to malicious. The malicious node may drop some or many of the data packets. The gray hole attack is very hard to detect because of its traffic issues, packet load and the ability to change its node. Instead it behaves as an honest node and when data packets arrive through this path, it drops all the packets of data. A condition is added to drop all data packets if it is the destination otherwise it will not receive all the data packets. Gray hole node acts as a trustworthy t node during route discovery process but actually it is an intruder.

• Dropping all UDP packets while forwarding TCP packets.

• Dropping a half of the packets or based on its probabilistic distribution. They seek to distract the network without being detected by the security measures.

Pradeep Kumar Sharma et al, proposed a centralized system with MANET to prevent the attacks. All nodes s gets connected to a server as a mediator for all sending and receiving informations. The server stores information about the users and all the communications between the nodes as a centralized server-structure. The packet drop ratio is more in black Hole attacks than Gray Hole attacks. The routing load increases in the presence of Black Hole attacks compared to Gray Hole attacks.

H. Deng et al proposed a technique to detect gray hole attack the entire traffic data is divided into a set of small packets. Initially a backbone network of strong nodes is built by this technique over the Manet. These strong nodes are efficient in terms of computing power and radio frequency. Each strong node is a trustworthy.

Nodes are considered as a strong node otherwise ordinary node. The disadvantage is the assumption that some strong nodes which are powerful in terms of power and antenna range are available in the network.

The efficiency of the main network is not represented in terms of least capacity and coverage. The assumption that strong nodes are trusted node will fail if the intruder attacks strong nodes.

An algorithm is used for detecting gray hole on the basis of agent based approach. It makes the next hop information to be available to a node. With DSR routing, uses route cache information to obtain the next hop data.

In this algorithm phone mediator (PM) has been enhanced with a timer. This timer is currently a function of PM code size with the PM mediator size. The timeout period is based on the observation 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 phone mediator is unable to return to its home context before timeout.

Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh proposes that a black hole / gray hole attack which are most serious threats in mobile ad hoc network. In group black hole attack more than one node combine with each other hence this attack is more difficult to detect.

Jitendra Parmar, Jitendra Parmar proposed a Different Approach of Intrusion Detection and Response System for Relational Databases .Detection of intrusion is possible in the databases and various authentication techniques are implemented to made this databases secure.

Database security and authentication focuses on major factors such as authentication, intrusion response system, timestamp and triggers provides more security to the database. The proposed methodology implemented here provides security, authentication, and database policies**.**

5. Conclusion and Future Scope

Various methods have been studied in this literature review used for detection and prevention of black hole and Gray hole. There may be many methods for prevent malicious node and increase packet delivery ratio, end to end delivery, reduce the dropping of packet and increase throughput of the system. In future we will enhance the performance and increase the packet delivery ratio more the present scenario.

6. 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 Black hole 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] Jagdish J. Rathod , Amit Lathigara," Novel Approach of Preventing and Detecting Gray Hole Attack on AODV based MANET", Volume 3, Issue 1, January 2015

[9] Hoang Lan Nguyen , Uyen Trang Nguyen "A Study of different types of attacks in mobile adhoc networks ", Department of Computer Science and Engineering, pp. 2-7, 2012.

[10] 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.

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

[12] A. Desai, Prof. P. 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.