A study on intrusion detection system against DDOS attack in MANET

N.Sharmila Kumari, Santhosh Kumari, Apoorva.D, Mrs.Neelufar*

Department Of Information Science & Engg,Dr.TTIT,India
*HOD ISE,Dr.TTIT, India

Abstract**-** Mobile ad-hoc network (MANET) is one of the most important fields for development of wireless network. A mobile ad hoc network is an autonomous collection of mobile devices like laptops, mobiles, sensors, etc. MANET is an emerging technology and have great strength to be applied in critical situations in military battlefields and commercial applications such as building traffic system, MANET is infrastructure less, with no any centralized controller exist. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. There are many security attacks in MANET and DDOS (Distributed denial of service) is one important attack in MANET.

Index Terms- Security, Mobile ad-hoc network, Intrusion detection system, DDOS

I. Introduction

MANET is an autonomous system in which nodes are connected by wireless links and send data to each other. Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications.there is no any centralized system so routing is done by node itself.

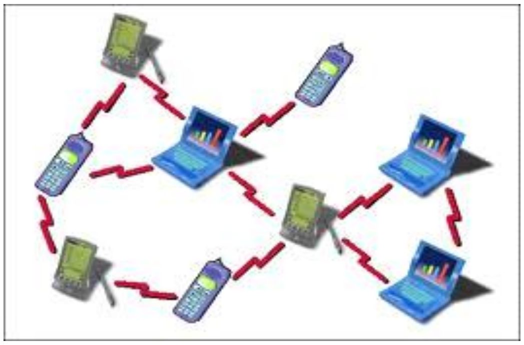

Figure1.2. MANET Architecture

The main task of the intrusion detection system (IDS) is to discover the intrusion from the network packet data or system audit data. One of the major problems that the IDS might face is that the packet data or system audit data could be overwhelming. Some of the features of audit data may be redundant or contribute little to the detection process. So the reduction in the size of data set is needed. To perform the reduction, two methods of feature selection, namely, markov blanket discovery and genetic algorithm are proposed. The Intrusion Detection System is distributed in nature so each node of a mobile ad hoc network equipped with an IDS.

II. PROBLEM STATEMENT

Lot of security vulnerabilities in a wireless environment, such as MANET, has been identified and a set of countermeasures were also proposed. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge. ONE OF the serious attacks to be considered in adhoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

Due to its mobility and self routing capability nature, there are many weaknesses in its security. THE presence of a DDOS increases the packet loss in the network considerably AND LEADS TO SECIRITY ISSUES IN THE NETWORK.DDoS attack is a natural development from the SYN Flood. The idea behind this attack is focusing Internet connection bandwidth of many machines upon one or a few machines. This way it is possible to use a large array of smaller (or “weaker”), widely distributed computers to create the big flood effect.

Usually, the assailant installs his remote attack program on weakly protected computers using Trojan horses and intrusion methods, and then orchestrates the attack from all the different computers at once. This creates a brute force flood of malicious "nonsense" Internet traffic to swamp and consume the target server's or its network connection bandwidth. This malicious packet flood competes with, and overwhelms, the network's valid traffic so that "good packets" have a low likelihood of surviving the flood. The network's servers become cut off from the rest of the Internet, and their service is denied.

III. LITERATURE SURVEY

A .Types of attack in MANET

Attacks in MANETs can be divided into two main categories, namely passive attacks and active attacks.

Passive Attacks: Passive attacks are those where the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. This in turn can lead to the disclosure of critical information about the network or nodes such as the network topology, the location of nodes or the identity of important nodes.

Active Attacks: In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Some of these attacks are caused by a single activity of an intruder and others can be caused by a sequence of activities by colluding intruders. Active attacks (as compared to passive attacks) disturb the operations of the network and can be so severe that they can bring down the entire network or degrade the network performance significantly, as in the case of denial of service attacks. Therefore, in this paper we have focused on active network layer attacks.

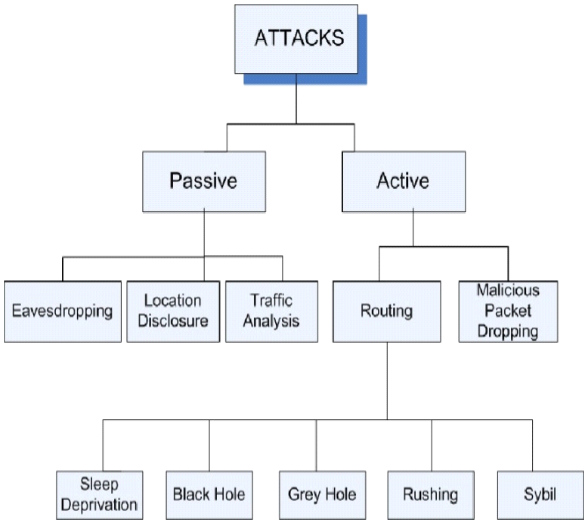

Figure3.1 Classification of attacks in MANETs

3.1 Wormhole

The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network.. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

3.2 Blackmail

This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated .

3.3 Routing Table Poisoning

Routing protocols maintain tables that hold information regarding routes of the network. In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [6]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network.

3.4 Replay

A replay attack is performed when attacker listening the conversation or transaction between two nodes and put important massage like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender.

3.5 Location Disclosure

Location disclosure is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

3.6 Black Hole

In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

3.7 Denial of Service

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

3.8 Distributed Denial of Service

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

3.9 Rushing Attack

Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols . For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

3.10 Masquerade

It is an intruder who gain the privilege of any one system as an authenticate user by stolen user password, through finding security gaps in programs, or through bypassing the authentication mechanism.

3.11 Passive Listening and traffic analysis

The intruder could passively gather exposed routing information. Such an attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol.

IV. INTRUSION DETECTION SYSTEM

To solve the security issues we need an Intrusion detection system, which can be categorized into two models:

1. Signature-based intrusion detection [1]
2. anomaly-based intrusion detection.

In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory.

Disadvantage

System is that if there is an attack and its signature is not in IDS database then IDS cannot detect that attack.

To solve this problem anomaly based IDS is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. Anomaly based IDS are based on tracking unknown unique behavior pattern of detrimental activity

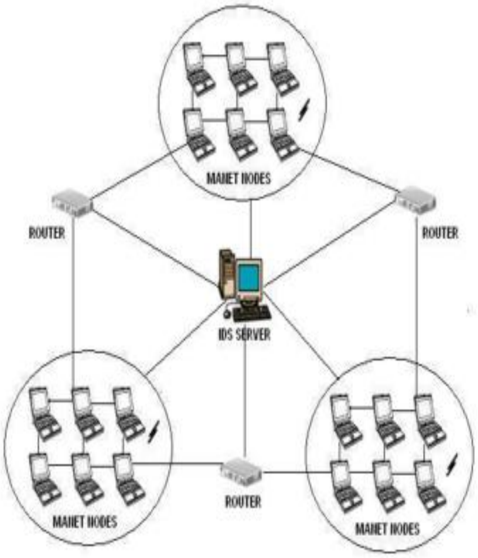

Figure 4.1 Intrusion detection system

Advantages

1. Doesn’t require prior information of the node
2. Helps to reduce the “limitations problem”.
3. Conducts a thorough screening of what comes through.

V. CONCLUSION

In this paper, an introduction to mobile ad hoc networks is provided along with its various vulnerabilities. We firstly survey various attacks and problems Different types of attacks called Active and Passive are discussed. After that a survey is conducted regarding intrusion detection techniques which can find out misbehaving links in reliable manner like Security is a very important in MANET. A variety of attacks have been discussed in this paper . An Intrusion Detection System uses various techniques for detecting attacks like DDoS attack on the wireless mobile adhoc network. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion detection on attack is easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. Intrusion detection systems can effectively identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an unavoidable and important component to provide defense-in-depth security mechanisms for MANETs.

REFERENCES

[1] U. Sharmila Begam, Dr. G. Murugaboopathi “A Recent Secure Intrusion Detection System For Manets” International Journal of Emerging Technology and Advanced Engineering Vol 3, Special Issue 1, January 2013.

[2] Mugdha Kirkire, Poonam Gupta"Intrusion Detection in Mobile Ad-hoc Network "International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, pp. 869-876 ,February- 2014

[3] R.Heady, G.Luger, A.Maccabe, and M.Servilla."The architecture of a network level intrusion detection system" In Technical report, Computer Science Department, University of New Mexico, August 1990

[4] Prajeet Sharma, Niresh Sharma and Rajdeep Singh "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" Vol. 41-No.21,pp.16- 21, March 2012.

[5] Tiranuch Anantvalee, Jie Wu "A survey on Intrusion Detection in Mobile Ad Hoc Networks"Y. Xiao, X.Shen, and D.-Z. Du (Eds.) pp. 170 – 196, 2006.

AUTHORS

First author – N.Sharmila kumari, B.E, M.TECH, Dr.TTIT,Karnataka,India, sharmila.nesan@gmail.com.
Second Author – Santhosh kumari, B.E, M.TECH, Dr.TTIT,Karnataka,India, santhoshkumariy@gmail.com.
Third Author – Apoorva.D, B.E, M.TECH, Dr.TTIT,Karnataka,India, apoorva.bhavikatte@gmail.com.
Forth Author - Mrs.Neelufar, HOD ISE,Dr.TTIT