IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Survey on Intrusion Detection System for DDoS Attack in MANET

Nshunguye Justin [1], Nitin. R. Gavai [2]

Department of Information Technology, Sinhgad College of Engineering, Pune, India[1, 2]

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 has 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.

Keywords: security, mobile ad-hoc network, intrusion detection system, DDOS, Attack.

I. INTRODUCTION

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, to methods of feature selection, namely, markov layer 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. 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.

A) MANET Architecture

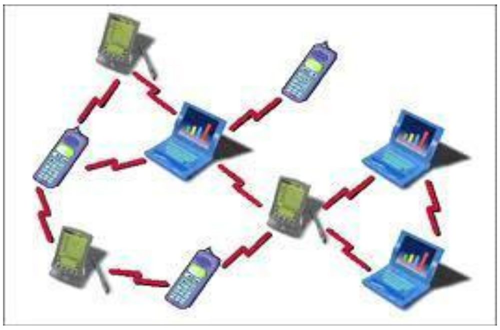

Figure1.2. MANET Architecture

B) Challenges

The design of ad hoc network faces quite a few Challenges [6].

1) The nodes in an ad hoc network, i.e. the source nodes, the subsequent destinations and the routing nodes, forwarding traffic between them may be moving [11].

2) As the wireless communication range has limits, the link between a pair of adjacent nodes breaks soon as they move out of range. Classification of routing protocols in mobile ad hoc network namely Proactive, Reactive and Hybrid. [6].

II. IDENTIFYING ISSUES

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 ad hoc 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 security 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

DOI 10.17148/IJARCCE.2016.54284

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 [6].

III. OBSERVATION

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.

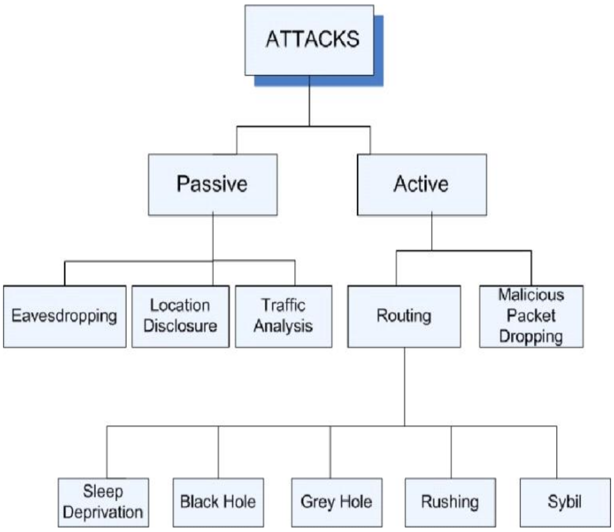

Figure 3 Classification of attacks in MANETs

3. 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 [10].

3.1 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 [10].

3.2 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.

3.3 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 [11].

3.4 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 [10].

3.5 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

DOI 10.17148/IJARCCE.2016.54284

at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions [10].

3.6 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. [6]

3.7 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.

3.8 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 [10].

A. DSR and AODV

The Dynamic Source Routing (DSR) is an on demand Source routing protocol that employs route discovery and route maintenance procedures same as that of AODV. In DSR, each node maintains a route cache with entries that are continuously updated as the node learns new routes. Similar to AODV, a node wishing to send a packet will first examine its route cache to see whether it already has a route to the destination.

If there is no valid route in the cache, the sender initiates a route discovery procedure by broadcasting a route request packet, which contains the address of the destination, the address of the source, and a unique request ID. As this request propagates through the network, each node inserts its own address into the request packet before rebroadcasting it.

As a consequence, a request packet records a route consisting of all nodes it has visited. When a node receives a request packet and finds [7]

A. Performance analysis of DSR, AODV

Dynamic network topologies:
In this, nodes move frequently and unpredictably. This leads to network partitioning, change in routes, packet drop at a reasonable price [8]

Table 1: Performance analysis of DSR, AODV

No	Performance Constraints	DSR	AODV
1	Proactive	No	No
2	Active	Yes	Yes
3	Hybrid	No	No
4	Loop Free Routers Available	Yes	Yes
5	Scalability	Yes	Yes
6	Distributed Environment	Yes	Yes
7	Unidirectional Link	Yes	No
8	Multicast	No	No
9	Periodic Broadcast	No	Yes
10	QoS Support	Less	Less
11	Route Maintenance	Yes	No
12	Type of Protocol	Distance Vector	Distance Vector
13	Message Overhead:	Less	Less
14	Delay in New Route Discovery	Less	More

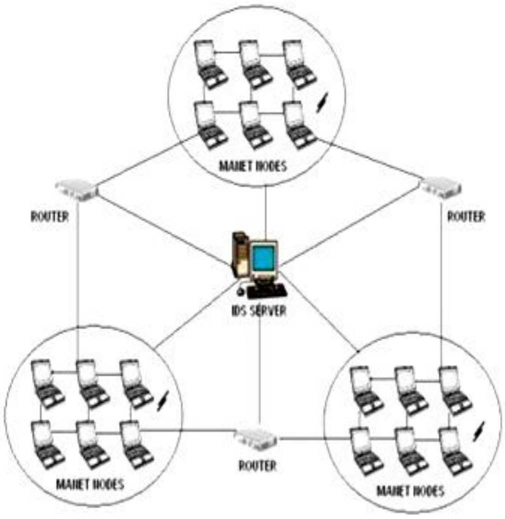

Figure 4.1 Intrusion detection system

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.

IV. RELATED WORK

The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV & DSR.

Table 2: Authors and concepts

No	Authors	concepts
1	Author: Wei-Shen Lai et al	a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks

2	Shabana Mehfuz1 et al	a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique
3	Giriraj Chauhan and Sukumar Nandi	proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics

V. 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
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 [12]. Then IDS cannot be able to detect attack. For this periodically updating of database is compulsory [10].

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 disadvantageous activity [9]

VI. 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 ad hoc 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] 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
[2] 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.
[3] Prajeet Sharma, Niresh Sharma, Rajdeep Singh , A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network, International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012
[4] Yashashree A. Jakhade, Nitin R. Gavai "Comparative Study of AODV, DSR and AOMDV Routing Protocols in MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 10, October 2015
[5] Yashashree A. Jakhade, Routing Problems and Solutions for Location-Based Routing in MANETs, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016
[6] Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology, 2249 – 8958, Volume-1, Issue-5, June 2012
[7] 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.
[8] 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
[9] 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.
[10] Pintu Vasani, Parikh Dhaval "Impregnable Obtrusion Recognize System Across DDOS attacks in Wireless Mobile Ad-hoc Network" International Journal of Emerging trends in Engineering and Development, Issue 3, Vol.5 (September 2013)
[11] Hemant Sonawane, Hitesh Gupta "An Intrusion Detection System Algorithm for Defending MANET against the DDoS Attacks" International Conference on Recent Trends in engineering & Technology – 2013
[12] D.Lakshmi sailaja, G.N.Vivekananda, G.B. Himabindu, Impregnable Obtrusion Recognize System across DDOS attacks in Wireless Mobile Ad-hoc Network", International Journal of Emerging trends in Engineering and Development,
[13] f. H. D. Sonawane, D. B. Bagul2, Badgujar3, S. R. Jadhav, Pro International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 2 Issue: 12 4075 – 4077
[14] Mieso K. Denko "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme" Systemic, cybernetics and informatics, Vol 3.

DOI 10.17148/IJARCCE.2016.54284