ISSN:0975-9646

A Survey on Different Available Detection Techniques of IDS and Attacks at Different Layers of MANET

Mahesh Gosavi, Prof. E. Jayanthi

Sinhgad college of Engineering,
University of Pune, India.

Abstract— Security is a vital service for wired and wireless network communications. The success of Mobile Ad hoc networks (MANET) powerfully depends on people's confidence in its security. Current technologies can form Ad hoc networks but it is not reliable. However the multi-hop nature, the lack of physical protection, the dynamic topology and Ad hoc connectivity amongst end user nodes are such characteristics of MANET, which expose it to much securities vulnerability. In this paper we provide different available detection techniques and analyze them comparatively. Then we discuss different attacks according to protocol stack.

Keywords— MANET, Attacks, IDS, Security.

I. INTRODUCTION

The increasing popularity of wireless portable devices, such as mobiles, laptops, PDAs, wireless telephones or wireless sensors, has highlighted the importance and the potential of mobile ad hoc networks. Currently, due to Internet service facilities and the convenience of portability, many people employ mobile networking in their professional and domestic activities.

Mobile ad hoc network (MANET) is the collection of mobile nodes which are communicating with each other. It is a infrastructure less, self configuring network. The network topology of MANET is not fix because of nodal mobility. Due to its such characteristics MANET is vulnerable to various attacks.

Intrusion detection System:

Intrusion detection system is used to detect intrusion and then alerting to the administrator. Intrusion detection system is the presses of identifying computing or network activities that are malicious or unauthorized.

II. CATEGORIES

There are different types of IDS. We can categories them on the basis of Architecture and technology [1].

A. Architecture

There are two types of IDS architecture Host based IDS and Network based IDS. In case of Host based IDS the IDS is located in the Host while in case of Network based, the IDS is located in the network. The host based IDS is also known as HIDS, every host has its own IDS. HIDS is only examine traffic within a particular host by gathering information from the host's system calls, application logs, database, operating system audit trails, and so onward [1].

B. Technology

IDS can be classified based on the technology used to detect the attacks. There are three main technologies Anomaly, Misuse and Specification.

1) Anomaly: In this method it is assumed that attacks or threats are different from the normal usage or behaviour of a host, network or network connection. Hence any abnormal behaviour (anomalies) or usage of a host, network or network connection will cause the IDS to identify it as an attack. Anomaly detection systems flag observed activities that deviate significantly from the established normal usage proles as anomalies [4]. This paradigm takes the attitude that something that is abnormal is probably suspicious. The construction of such a detector starts by creating a model of what constitutes normal for the observed network, and then deciding on what percentage an activity must be flagged as abnormal.

The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have high false positive rate.

2) Misuse: Misuse of analysis is similar to the way antivirus works that is by having a huge database of known attacks. The IDS will then compare the data collected with that of the database. If there is a match then the IDS will assume an attack has occurred. Misuse is sometimes called signature-based IDS because the pattern contained in the database is called signatures. Misuse method doesn't give lots of false alarm compared to Anomaly method because if the data collected doesn't match the signature of known attacks then no alarm will be produced. Unlike Anomaly method where if a user is doing something which is not of his or her normal activities such as chatting, a false alarm will be generated because the harmless abnormal activity is considered a threat by the IDS.

3) Specification: The main advantage of misuse detection is that it can accurately detect known attacks, while its drawback is the inability to detect previously unseen attacks. Anomaly detection, on the other hand, is capable of detecting novel attacks, but suffers from a high rate of false alarms . This occurs primarily because previously unseen (yet legitimate) system behaviours are also recognized as anomalies, and hence flagged as potential intrusions.

Specification-based detection techniques have been proposed as a promising alternative that combine the strengths of misuse and anomaly detection [2]. In this

approach, manually developed specifications are used to characterize legitimate program behaviours. As this method is based on legitimate behaviours, it does not generate false alarms when unusual (but legitimate) program behaviours are encountered. Thus, its false positive rate can be comparable to that of misuse detection. Since it detects attacks as deviations from legitimate behaviours, it has the potential to detect previously unknown attacks.

III. TYPES OF SECURITY ATTACKS

A. *On the basis of nature*

1) Passive Attacks: In passive attack, the message which is transmitted is not changed. There is an attacker (intermediated node) between sender & receiver which reads the message. The attacker obtains data exchanged in the network without disrupting the operation of communications. This intermediate attacker node is also doing the task of network monitoring to analyze which type of communication is going on [5].

2) *Active Attacks:* 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 RREQ (re request) though it is not an authenticated node so the other node rejecting its request due these RREQs the bandwidth is consumed and network is jammed [5].

B. *On The Basis Of Domain*

1) External attacks: External attacks are carried out by nodes that do not belong to the domain of the network. In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services.

2) *Internal attacks:* Internal attacks are from compromised nodes, which are actually part of the node. In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a current node and using it as a basis to conduct the attack [5].

IV. ATTACKS CORRESPONDING TO DIFFERENT LAYERS IN MANET

A. *Attacks At Application Layer*

1) Repudiation attack: Repudiation is referred to denial of participation in all or part of communication. For example, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system.

2) Attack by virus & worms: Viruses are self-replicating computer programs. These programs infect the files and propagate. Virus is activated in the system by simply opening the file.

Worms are similar to viruses but it does not require a file to allow it to propagate. There are two types of worms network-aware worms and mass-mailing worms [3].

The following table gives various attacks corresponding to various layers of MANET.

TABLE I
ATTACKS CORRESPONDING TO DIFFERENT LAYERS.

MANET Layer	Type of Attack
Application Layer	1. Repudiation attack, 2. Attacks by virus & worms
Transport Layer	1.SYN Flooding attack (DOS in nature), 2. TCP/IP Spoofing
Network Layer	1. Route tracking, 2. Flooding attack, 3. Message Fabricate, modification, 4.Blachhole Attack, 5.Wormhole attack, 6. False routing attack
MAC Layer	1. Mac DOS (Denial of service) attack, 2. Traffic monitoring & analysis, 3. Bandwidth stealth, 4.WEP targeted attack 5. MAC Spoofing:
Physical Layer	1. Jamming attack (DOS in nature), 2. Stolen or compromised attack, 3. Malicious massage injecting, 4. Eavesdropping attack

B. *Attacks At Transport Layer*

1) SYN Flooding attack (Denial of service attack): This attack target the TCP/IP stack. This attack is origin for the DoS, that is causes system to crash or became unavailable to other connections. In this attack SYN flood sends a huge number of TCP connections requests without sending anything else, making system unavailable.

2) TCP/IP Spoofing: To obtain a disguise an attacker can use IP Spoofing. Using this attack an attacker gains authorized access to mobile nodes or network. An Attacker can alter source address by manipulating an IP header, hence making a packet true source. A similar attack which is specific to TCP is Sequence number prediction.
There are several attacks subtypes like Non-blind TCP spoofing, Blind TCP spoofing, Man In the Middle (MITM) and DoS.

C. *Attacks At Network Layer*

1) Route tracking : In this attack the sensitive information is obtained which is routed through different intermediate nodes.

2) Flooding attack (Denial of service attack): Attacker exhausts the network resources, i.e. bandwidth and also consumes a node's resources, i.e. battery power to disrupt the routing operation and to degrade network performance. A malicious node can send a large no. of RREQ (re request)

in short duration of time to a destination node that dose not exist in the network. Because no one will replay to these RREQ so they will flood in the whole network. Due to flooding the battery power of all nodes as well as network bandwidth will be consumed and could lead to denial of service attack.

3) Message Fabricate, modification: In this attack the attacker inserts fake stream of data into the original message stream which is communicated or some kind of change is done in information.

4) Blackhole attack : This attack has two main properties. First, the attacker advertise itself as having valid route to a destination node, even if the route is fake so as to capture the packets. Second, just like a black hole absorbing everything passing by it, the attacker does not forword all the messages which he receives or sometime the attacker selectively forword the packets. Because of this the throughtput of the network is decreses [6].

4) Wormhole attack: It contains two or more adversaries, these adversaries has better communication resources than normal nodes and then establishesh better (higher power and long-rang link) communication channel between them. This chnnel i.e. Tunnel between two joining attackers is known as wormhole. This attack distrupt the routing mechanism and can be used as basic for eaves dropping [7].

5) False routing: In this attack the attacker routes the packet at false destination which creates the loop in the network. Because of this false messages are generated, the performance of the network is degraded and resource exhaustion is happened.

D. Attacks at MAC layer

1) MAC Denial of service attack (DOS) : At the MAC layer DOS can be attempted as:

An attacker node continuously sending fake packets or huge number of requests to a particular network node so as to keeping the channel busy and to drain out the battery power of that particular node, this leads to denial of service attack to that particular node. It can be achieved by keeping large value of NAV and keeping low value of DIFS parameter of Attacker node.

2) Traffic monitoring & Analysis : Traffic analysis is a passive type of attack in nature. Traffic monitoring and analysis can be used to identify the communication nodes and functionalities, This information is used to launch further attacks. Since these attacks are not specific to the MANET, other wireless networks, such as the cellular network, satellite network, and WLAN also suffer from these potential vulnerabilities [5].

3) Bandwidth Stealth : In this attack the huge fraction of bandwidth of a channel is stealth illegally by an attacker node and because of this congestion is happened in the network

4) WEP targeted attacks: The wired equivalent privacy (WEP) is designed to enhance the security in wireless communication that is privacy and authorization. However it is well known that WEP has number of weaknesses and is subject to attacks. Some of them are:-

(i) WEP protocol does not give key management.

(ii)The initialization vector (IV) is a 24 bit field which is the part of the RC4 encryption key. The reuse of IV and weakness of RC4 help to produce analytic attacks.

(iii)The combined cure of non cryptographic integrity algorithm, CRC32, with the stream cipher has a security risk [5].

5) MAC Spoofing: An attacker tries to modify the MAC address in transmitted frames".

E. Attacks At Physical Layer

1) Jamming attack (Denial of service attack): Jamming attack is targeted to disrupt the legitimate communication and this can be achieved by the overpowering frequencies of illegitimate traffic. The best example of this attack is Pulse and random noise. The Jamming attacks can be classified as external and internal Jamming attacks.

2) Stolen or compromised attack: These attacks are happened from a compromised entity or stolen device like physical capturing of a node in MANET.

3) Malicious message injecting: In this attack the attacker inserts fake stream of data into the original message stream. Now this message is routing through the intermediate nods. Because of this injected malicious message the functionality of network is disrupted by the attacker.

4) Eavesdropping attack: Eavesdropping is the reading of messages and conversation by unintentional receivers. The nodes in MANET share a wireless medium and the wireless communication use RF spectrum and broadcast by nature which can easily intercepted with receivers tuned to proper frequency. As a result transmitted messages can be overheard as well as fake messages can be injected into the network).

V. CONCLUSIONS

In this paper, we try to analyze the different detection technique in MANET and study them comparatively. Then we evaluate security attacks at different layers of MANET, which produces lots of difficulties in the MANET operations. Due to the dynamic nature of MANET it is more prone to such kind of attacks. In MANET the solutions are designed corresponding to specific attacks they work well in the presence of these attacks but they fail under different attack scenario. Therefore, our aim is to develop a multi-functional security system for MANET, which will cover multiple attacks at a time and also some new attacks.

REFERENCES

[1] Kamaruzaman Maskat, Mohd Afizi Mohd Shukran, Mohammad Adib Khairuddin & Mohd Rizal Mohd Isa,"Mobile Agents in Intrusion Detection System: Review and Analysis" ,Accepted: September 19, 2011 Published: December 1, 2011.

[2] P. Uppuluri and R. Sekar Department of Computer Science SUNY at Stony Brook, NY 11794 "Experiences with Specification-based Intrusion Detection"

[3] Mohammad Wazid, Rajesh Kumar Singh, R. H. Goudar "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques", International Conference on Computer Communication and Networks CSI- COMNET-2011.

[4] Gaia Maselli, Luca Deri, Stefano Suin," Design and Implementation of an Anomaly Detection System: an Empirical Approach",

[5] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei Department of Computer Science and Engineering Florida Atlantic University "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, "wireless/mobile network security" Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. °c 2006 Springer.

[6] Rashid Hafeez Khokhar, Md. Asri Ngadi, Satria Mandala, "A review of current routing attacks in Mobile Ad-Hoc Networks", International Journal of Computer Science & Security, Vol.(2) Issue (3).

[7] Y-C. Hu, A. Perig, and D. Johnson, "Wormhole attacks in Wireless networks", IEEE JSAC, Vol-24, no.2, Feb20061.
.