International Journal of Current Trends in Engineering & Technology
Volume: 02, Issue: 01 (JAN-FAB, 2016)

ANALYSIS OF VARIOUS INTRUSION DETECTION TECHNIQUES

Sana Sheikh
Department of Information Technology.
NRI Institute of Science and Technology,
RGPV, Bhopal
san_2086@rediffmail.com

Angad Singh
Department of Information Technology.
NRI Institute of Science and Technology,
RGPV, Bhopal
angada2007@gmail.com

Abstract

In recent years, the utilization of mobile ad hoc networks (MANETs) has been extensive in many applications that include some task critical applications, and as such safety has become one of the major anxiety in MANETs. Because of some unique features ofMANETs, deterrence methods alone are not enough to make them secure; thus, detection should be added as another guard before an aggressor can violate the system. However, the intrusion detection techniques for conventional wireless networks are not well enough for MANETs. Here in this paper, we categorize the architectures for intrusion detection systems (IDS) that have been proposed for MANETs

I. Introduction

From some past years, mobile computing devices for example mobile phones, palmtops, laptops etc are very popular and brought a great and drastic change in medium of communication and this change in computing will not simply depend on the ability provided by the personal computers, and the concept of ever-present computing appears and becomes one of the research area in the computer field. The Mobile Ad-hoc network is wireless communication medium is a mobile network, which has also become a very fascinated area of research where there are no wired connections and there is no centralized coordinator. IN MANET location the security of each entity network node is very important because of the enveloping nature of MANETs. The node will not always be below the power of their holders and as a result the security of the node will turn into a very important issue .The links between wireless nodes are highly vulnerable to link attacks that include passive snooping, lively interfering, and seepage of secured information, data fiddling, imitation, message reply, and rejection of service. All these features and susceptibilities of MANETs, pretenses many confronts to build a secure MANET. [1]

II. Mobile Ad-Hoc Network

A Mobile Ad hoc Network (MANET) can be defined as the construction of wireless mobile nodes that can organize it and change dynamically in random and its network topologies. People and transportation can work and make use of internet without a defined communication infrastructure or in other words it can be said that when utilization of such infrastructure need wireless extension. Nodes in MANET converse with each other directly within their range of wireless network and those nodes that are bit faraway, converse with the help of intermediate nodes. [2]

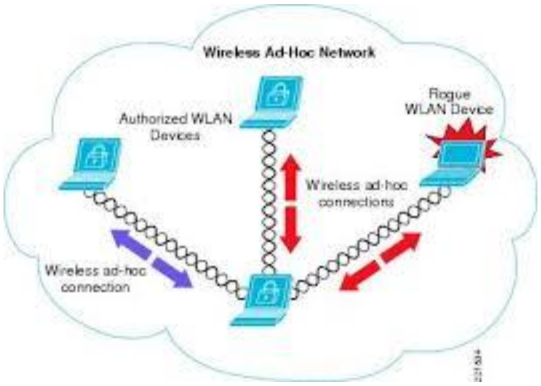

Figure 1 Mobile Ad-Hoc Network

The main point which needs attention is the security of Mobile Ad-Hoc network because it is more likely to have vulnerable attacks as compared to wired networks as the mobile networks does not have trusted central coordinator and the number of valuable resources. For maintaining security, few important objectives of security that needs to be addressed for maintaining a secure and trustworthy environment. They are:

- Authentication
- Reliability
- Confidentiality
- Non-Repudiation
- Integrity

Confidentiality consists in making data inarticulate to individuals other than those concerned in the operation.

Integrity means proving data integrity consists in deceiving if the data were distorted during transmission.

Availability aims to assurance access to a service or resources.

Non-Repudiation means data is the assurance that none of the parties concerned can reject an operation at a later date.

Authentication consists in confirming a user's identity, i.e. assuring for each party that their associates are truly who they think they are. An access control donating access to sources only to approved individuals [3].

III. Intrusion Detection System

Intrusion detection (ID) is a type of security supervision system related to computers and networks. An ID system collects and examines data from various places within a computer or a network to recognize possible security breaches that comprises both intrusions (attacks from outside the organization) and exploitation. ID uses *susceptibility assessment* that sometimes can be called as scanning that is a developed by technology to charge the security of a computer system or network. [4].

Many past situations have shown that intrusion prevention methods alone, for e.g. encryption and authentication, that normally be considered as a first method of defense, that are not enough. As the system become more intricate, there are also more flaws, which lead to more problems related to security. Another method to protect the network is the intrusion detection, from such problems. If the imposition is detected, a reply can be initiated to avert or minimize damage to the system. [5]

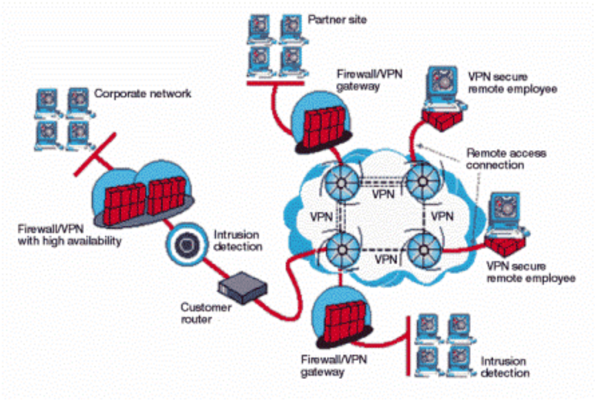

Figure 2 Intrusion Detection System

IV. Different types of Architecture of Intrusion Detection System

MANET can be organized in different type of infrastructure as in flat infrastructure or in multi-layer architecture. Depend on the infrastructure of MANET; Intrusion Detection System can be organized. Following are the different types of intrusion detection System: [5]

1. Simple Intrusion Detection System

In this simple architecture, the nodes in the network does not communicate to each other and to identify the intrusions, the detection system run individually on every node for recognizing the impositions. The conclusion will also be decided which is based on the data collected on every node after detecting intrusions. Thus in this way no information is exchanged among nodes. As this architecture is not so effective because of having so many shortcomings.

2. Dispersed and Supportive Intrusion Detection System

As it knows that the nature of Mobile Ad-Hoc network is based on cooperation among nodes, then the intrusion detection system that can also be organized on this principle. In this system each node can have an agent of IDS that will recognize intrusions and collect information related to it and start operation autonomously. Though the co-nodes also contributes in detecting the vulnerable attacks with the help of universal Intrusion Detection System when the proof is uncertain. This method is proposed by Zhang and Lee [6].

3. Multi -Layered Intrusion Detection System

For the networks that are divided into clusters, this hierarchal IDS is proposed. Unlike Distributed Intrusion Detection System which is developed for flat networks, Multi-layered Intrusion Detection System is proposed for Multi-layer architecture. In the cluster-based architecture, head cluster is responsible for routing and forwarding data packets. The same idea is applied in Multi -Layered Intrusion Detection where each node locally in its cluster will be liable for noticing intrusions and the head-cluster will detect intrusions first at its node point and also globally responsible for its group(cluster).Each node will be treated as IDS agent for all the participating members of a clusters. The head-cluster will monitor and instigate the reaction. [5]

V. Methodologies For Detecting Intrusion Detection

Different methods are used for detecting the intrusions based new technologies. Some methods are based on rule-based learning, artificial intelligence and other computational methods. Below are some methods for detecting intrusion detection.

➢ **Bayesian Network**-This network comprises of nodes and edges that stand for variables in the network, where some variables are chosen for observing the system. After that for constructing the Bayesian network, the evaluation of relationship between the variables is done. The third step is to define support for the variables that will define the present state of variables where support factor is defined as the possibility of happening of the states observed. If this value is less than threshold value then a signal is generated.

- **Neural Networks**

This network contains of Nodes and Edges. The cost of the weight on arcs describes how a node influences on adjoining node. A group of the nodes in the model is defined which is known as incoming nodes. The other group contains the outgoing nodes from which there is no association themselves, their outcome is the result of the analysis.

- **Expert System**

The Expert Systems working procedure is based on a formerly defined set of rules that defines an attack. All security connected occurrences included in an audit track are translated with the help of if - else rules.

- **Fuzzy Logic**

Fuzzy Logic denotes to the model of indecision of natural language. Here the logic depends on language which takes the smallest amount of set of happenings or highest instead of defining OR, AND or NOT condition in the if-then-else condition. Essentially, intrusion detection systems differentiate between two different types of actions, normal and irregular. Fuzzy logic could generate sets that have in-between values where the distinctions between the two sets are not defined well

- **Immune Based**

Intrusion Detection System based on the Immune is related to human immune system and can execute duties similar to native and adaptive immunity. The outline of normal behavior is produced by collecting suitable behavior of services corresponded to audit data. One confront is faced to distinguish between self and non-self data which tries to control reasons scaling problems and the continuation of errors in detector sets. [7]

VI. Related Work

Anand and Patel [8] have discussed about Intrusion and Detection and its various protocols. They discussed about the importance of intrusion detection and the number of attacks that can occur on various different type of protocols like UDP,TCP,ICMP and ARP. They have also proposed a method for fast detecting the intrusion based time detection. They further added that the proposed method will recognize anomalies on the basis of connections made in single second and for validation the method is applied on real traffic.

Ning and Jijodia [9] discussed about intrusion detection and types of detection as anomaly, misuse and detection in distributed systems. In their work they have put some light on all the existing techniques for intrusion detection they address that the detection of intrusion is still a problem .Finally they conclude that if the attack scenarios are reconstructed from alert of intrusions then the integration and performance of Intrusion detection will improve.

Anantvalee et.al [5] in their work have surveyed on techniques of intrusion detection in MANET. They have discussed about in brief about intrusion and the various architectures of it. Finally they have compared the previous and current intrusion detection architectures and conclude that along with the nature of MANET, IDs should be structured distributed and cooperated and prefer anomaly detection over misuse detection.

Wenjia Li and Anupam Joshi,in the paper," Security Issues in Mobile Ad Hoc Networks - A Survey " [5] tried to discover the issues of security in Mobile Ad hoc network. They state that due to increased use of mobility and open nature of media, Mobile Ad hoc network are likely to experience all kind of security risks. Thus more attention related to security must be given to wireless MANET on contrast to wired networks. In their work they first discussed about the features of Mobile Ad hoc network and its importance in today's network users. Secondly they elaborated some deceitful fears in Mobile Ad hoc network which can be originated by some own features like dynamically changing topology, mobility etc. Lastly they discussed about security solutions and criteria for security in Mobile Ad hoc network. It also convoluted about techniques that can help to defend the Mobile Ad hoc network.

VII. Conclusion

Mobile Ad-Hoc network is a always been an interesting issue for research .It is observed that MANET has been widely used in today's scenario and thus its security in MANET has also become a significant factor. Thus to improve the security, the concept of Intrusion Detection has been evolved for detecting and monitoring the network. Here in this paper we have presented a brief introduction of MANET and its security. We have also described about intrusion detection and about its different architectures and explained the different types of Intrusion detections .There are still more methods that can be elaborated in the intrusion detection system.

References

[1]. Eratul.L & Ibrahim. D," Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)".

[2]. http://www.slideshare.net/piyushmittalin/security-in-mobile-ad-hoc-networks

[3]. http://en.kioskea.net/contents/635-introduction-to-it-security

[4]. http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection

[5]. Anantwalee," A Survey on Intrusion Detection in Mobile Ad Hoc Networks" Springer pp. 170 – 196, 2006.

[6]. Y. Zhang, W. Lee, and Y. Huang, \Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[7]. Akbar et.al," Intrusion Detection System Methodologies Based on Data Analysis", International Journal of Computer Applications (0975 – 8887)Volume 5– No.2, August 2010

[8]. Anand and Patel," An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012

[9]. Ning and Jijodia,"Intrusion Detection Techniques".

[10]. Li. W & Joshi. A."Security Issues in Mobile Ad Hoc Networks- A Survey".