Analysis of Intrusion Detection System Techniques

Kanika Aggarwal, Dr. Amit Shrivastava
Dept.Computer Science and Engineering, SIRT, Bhopal, INDIA

Abstract - From past some years, the mobile ad hoc networks (MANETs) has been used extensively in many applications, that includes some mission critical applications, and because security has become one of the major focus area inMANETs. Due to some exclusivefeatures of MANETs, methods of prevention alone are not adequate to make them secure; thus, detectionshould be added as another protection before an attacker can violate the system. In general, the intrusion detection methods for traditional wirelessnetworks are not well fitted for MANETs. In this paper, this article has presented a description of intrusion detection system in brief. Along with it different components and the issues of intrusion in MANET are also presented.

Keywords: Intrusion Detection, MANET, Attackers.

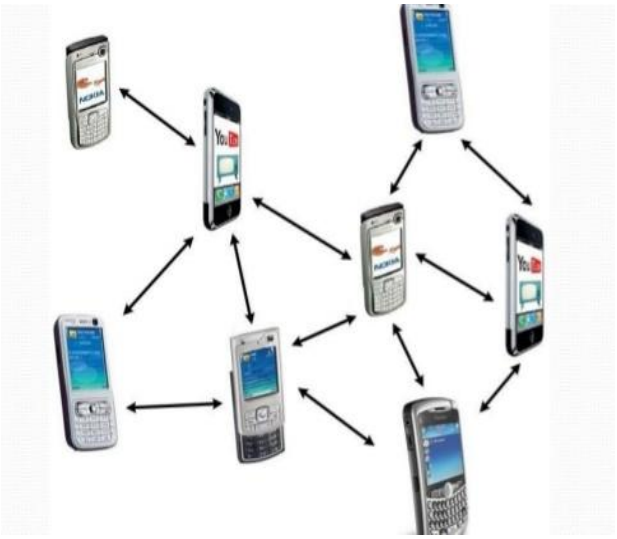
1. INTRODUCTION

Mobile Ad Hoc Networks are very common from past some decades and because of the great advancement in wireless network, it has becoming more and more area of interest from researchpoint of view.todays’s scenario, laptops, smart phones, Personal Computers, palmtops and other digital devices create a wireless network with the help of MANET and had become very popular and a way to solve the number of problems of communication out of which one is the fixed infrastructure and other is the centralized connectivity. From the definition point of view ,it can be defined as the clusters of mobile nodes and its linked hosts that all are connected with the help of wireless link and forms a network.The main feature of the MANET network is that the nodes can move freely and arrange themselves in arbitrary manner and therefore the topology of the network can change frequently and impulsively.

Each node in the MANET network behaves as independent router and will not guarantee about the rapidly changing topology and malicious nodes may occur between the paths of two nodes as the wireless links are extremely vulnerableto attacks.Because of these malicious attacks and vulnerabilities there is a need for the detection system and this leads to the Intrusion Detection System.[1]

2. MOBILE AD HOC NETWORK IN BRIEF

A mobile ad hoc network (MANET), is said to be a compilation of mobile nodes with wireless network border that creates atemporary network without any help of any fixed infrastructure or any central administration. A MANET is regarded asan no infrastructure network as the mobile nodes in the network vigorously set up ways among themselves to send packets for the short term. In other words a MANET is defined as self-configuring network that is shaped automatically by the group ofmobile nodes devoid of the help of a permanent infrastructure or centralized organization. Every node is prepared with a wirelesstransmitter and receiver thatpermit it to converse with other hosts in its range of communication. If a nodewants to transmit a packet to a node that is out of its radio range, there is need of cooperation required from other nodes in the network, thisis termed as multi-hop communication. Thus in MANET, every node must perform bothas a host and as a router at the same time. The topology of network repeatedly variesbecause of the mobility of mobile nodes as they go within, progress into, or shift out ofthe network. Nodes in wireless networks can communicate to each other that are directly connected in its range. And the nodes that are outsidethe range and wish to transmit data then they have to rely on another nodes for transmitting their data.Thus, a multi-hop situation occurs,where somemid hosts pass on the packets that are delivered by the source host before they approach the destination host. Each node behaves as a router. Thevictory of communication totally depends on other nodessupport.[2]



3. INTRUSION DETECTION SYSTEM

An intrusion-detection system (IDS) can be defined as the devices, techniques, and sources to help recognizing, charges, and to inform aboutunofficial or unapproved network actions. Intrusion detection is normally one component of a usually protection system that is put in the region of a system or device—it is not a only ashield measure.[3]. Intrusion is any group of behavior that try to cooperate the veracity, confidentiality, or ease of use of a resource,and an intrusion detection system (IDS) is a system for the recognition of such intrusions. Number of intrusion prevention techniques areproposed for a network, there are always some issues in the techniques that are not upto the mark. Here, the wireless and mobility are the main features of MANET that make up two very vulnerable characteristics for security. Therefore, it is essential to developed a systemwith the achievement of intrusion detection and response systems. These systems warn the network that an intrusion may occur and then take direct immediate and preventive steps to protect the network. It does not guarantee about neglecting attacks against ad hoc networks, but adds in improving the security policies and utilized to detect the possible hazards and points of failure in the network. The main task is to develop a intrusion detection system while protecting the desired network performance. Intrusion detection is a basic need in any high-survivability network.[4]

4. COMPONENTS OF INTRUSION DETECTION SYSTEM

The Intrusion detection System have three types of components:[clark]

- First component is the data collection that is responsible for collecting and for processing information and then transform the data into the another format. This system makes the use of different resources that works as inputs to the system.
- Second component is the detection component where data is evaluated to recognize vulnerable attacks after the data is passed the from data collection component.
- Last component is the response component where the results of intrusions are sent. The component is indicated by the responses.

5. IDS FOR MOBILE AD-HOC NETWORK ARCHITECTURE

Intrusion detection system and its components should be both distributed and cooperative for fulfilling the requirements of mobile ad hoc networks. In the design of every node in the mobile ad hoc network that takes part in intrusion detection and its response should be trustworthy. As every node cannot rely on its neighboring nodes, it is the duty for it to detect the signs of intrusion nearby and independently. Though, neighboring nodes can collectively exchange messages in the situation of a mistrustful situation or definite intrusion detection. Each IDS Agents are placed on each and every node. Each IDS Agent runs separately and observes local activities. Those local movements may contain user and system activities and communication actions with other nodes. The Agent of IDS runs its analysis module on the collected data to identify if there is any intrusion. If there is an imposition, the reply module is started. The IDS Agent must function within the source restraints on wireless networks, such as limited power. The IDS should have run-time efficiency. There is also an extra IDS architecture designed for multi-layered, wireless ad-hoc networks. In this design, cluster-head nodes merge routing for the cluster and may support extra security mechanisms[4]

6. TYPES OF INTRUSION DETECTION SYSTEM

There are two main types of categories in which intrusion detection system can be classified. They are host based and network based.

Host-based Intrusion Detection System-These system are designed for accumulating data about an activity on a single node or on a single system. These agents that are host-based sometimes regarded as sensors, those sensors would normally be installed on a computer that is considered to be vulnerable to possible attacks. The term “host” denotes to a singlesystem, thus a different sensor would be needed for every machine. Sensors are used in a different way where data is collected about the events that happen on the system that are monitored. After collecting the data, it is verified by the operating system that are known by the term audit trails. Host-based systems are confined to audit trails, because they are based on it and they are not provided by the producers who design the intrusion detection system itself.

Network –Based Intrusion Detection System-The strategy of network based intrusion detection system present a unique approach.In this method IDS collect information from the whole network and not from the individual host. Data is collected from traffic stream of network since the information is found in network segments. It detects for attacks or undesired behavior from the header or from the data of the packets that are broadcasted in the network. An

IDS based on network contains special type of “signatures” that will be applied on where attack are suspected.Some IDS come withspecial type of sensor that can built their own signatures that can present a way where the sensors can be developed related to each individual’s need .[5]

7. ISSUES OF INTRUSION DETECTION IN MANET

There are certain issues for developing a intrusion detection system in MANET.some are described as below:[6]

- Wireless Link-There is a limited bandwidth in wireless network as compared to wired networks and it is common nature of wireless network where links breakages takes place.Thus it is necessary for agents of the intrusion system to communicate with other linked agents for collecting information and to rely on them. Congestion may occur due to heavy traffic therefore it is important to put constraint on the data traffic for that IDS system need to reduce their data transfers.
- Inadequate Resources-Nodes in the network generally utilize battery power and have different capabilities. The computational and storing capabilities differ too. The range of nodes, generally with limited resources, it influences usefulness and efficiency of the IDS nodes they support.For example to conserve the resources ,mobile nodes may plunge packets. and memory restraints may stop one IDS agent to process a important number of attentive coming from others.
- Mobility- Nodes in MANET can disappear and connect the network and go independently, so that the network topology can change often. The highly lively operation of a MANET can cause conventionalways of IDS to be undependable. Due its mobile nature the architecture of IDS may also changes.
- Cooperation-Nodes in MANET networks are highly cooperated in nature that can target them for new vulnerable attacks. For example as in IDS nodes may depend on other nodes for communication to those nodes that are not in range, so in that case intermediate node may take part in decision system that can affect important parts of network.

8. RELATED WORK

Most of the work has been contributed towards Intrusion Detection in Mobile Ad-Hoc network. They have proposed and developed different types intrusion system, from which some are efficient and some are inefficient. Below are some proposed work presented by few researchers.

Fattah et al [7] discussed about Intrusion detection system that is based on distributed and cooperative which are hierarchal in nature. They analyzed that some intrusion detection that were developed before were not efficient to handle dynamic environments and unable to solve issues of ad- hoc networks and proposed a new intrusion detection architecture that can detect vulnerabilities in wireless network environment.The model that is proposed is based on distributed and cooperated nature.For achieving efficiency they have used machine learning techniques.Finally conclude that the model and the algorithm that is developed produces low false positive rate while detecting abnormality and achieves high detection rate when applied on various data sets.

Sangeetha et.al [8] in their work discussed about new method for intrusion detection system in mobile ad-hoc network with a name as EAACK-Enhanced Adaptive Acknowledgement. They analyzed that dropping of packet is the major risk to the security in MANET and thus designed a new method for the security. They also compared it against watchdog and other methods. Finally observed that simulation results produces positive results compared to other detection schemes.

Abdullah et.al[3] in their work presents a survey on the techniques of intrusion detection system.They have also compared the work of different researches and analyzed them on different parameters.According to the nature of mobile ad-hoc network,all the designed intrusion detection system are distributed and cooperative in nature. They conclude that the study of the protectionto such attacks should be investigated as well.

Murugaboopathi et al [10] discussed about the security of MANET and also discussed about new proposed method of intrusion detection called as EAACK and compared with other existing techniques. They have simulated in different situations as Packet dropping attack,against false misbehavior report and against attackers when they give false acknowledgement for negative results. They concluded that EAACK reveals superior malicious behavior detection rates in definite circumstances where as it does not greatly affect the performances network

Akbar et al [11] discussed about the attacks of different types that are used in data sets and also presented the classification of intrusion detection system.They have classified into different categories out which some are based on genetic algorithms, Bayesian networks, artificial intelligence, fuzzy logic and expert systems.They have a given a brief review of all the techniques that can be best applied on intrusion detection for detecting the anomaly and vulnerable attack.

9. CONCLUSION

Intrusion detection always to be a vigorous research field. Even after some years of research, the intrusion detection field still finds several hard problems. How to sense unidentified patterns of attacks without producing too many false warnings remains an unanswered problem, although recently, some researches have shown there is a possible resolution to this problem. The estimating and benchmarking of IDSs is also an significant problem, which, when solved, may provide useful direction for organizational decision producers and end users. This article discusses about the various aspect of the intrusion detection system along with the various work done in this category.

REFERENCES

[1] Ibrahim et.al," Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)".

[2] P.Virada," Intrusion Detection System (IDS) for Secure MANETs: A Study", *International Journal Of Computational Engineering Research Vol. 2 Issue. 6.*

[3] Abdullah et.al," A Survey on MANET Intrusion Detection"

[4] Obimbo et al," An Intrusion Detection System for MANET" *Communications in Information Science and Management Engineering,* Vol.2 No.3 PP.1-5, 2012

[5] Host- vs. Network-Based Intrusion Detection Systems,Global Information Assurance Certification Paper.

[6] *Clark.et.al,"*Intrusion Detection In Mobile Ad Hoc Networks"

[7] Fattaha et.al," Distributed and Cooperative Hierarchical Intrusion Detection on MANETs" *International Journal of Computer Applications (0975 – 8887)Volume 12– No.5, December 2010*

[8] *Sangeetha et.al,"* EAACK-A Secure Intrusion Detection System for MANET"*International Journal of Innovative Research in Computer and Communication Engineering,*Vol. 2, Issue 4, April 2014

[9] Murugaboopathi et al," A Recent Secure Intrusion Detection System For MANETS"*International Journal of Emerging Technology and Advanced Engineering,* Volume 3, Special Issue 1, January 2013)

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