ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

Intrusion Detection for the Malignant Activities in MANET

Pranshi Singh[1], Rashi Singh[2]

Dept. of Information Technology, Oreintal College of Technology, Bhopal (MP) India

Dept. of Electronics and Communication, UTD, Rajeev Gandhi Technical University, Bhopal (MP) India

ABSTRACT: An intrusion-detection-system (IDS) is the application-software which checks the activities of network or the system for the malignant activities. In current years, issues of security are very significant interest in the mobile-ad-hoc-network. As compared to wired-network, mobile-ad-hoc-network is exposed more to being got attacked. Besides the prevention methods, we need to find and apply appropriate actions to offer security to these types of networks. Due to some unique characteristics of the MANETs, the methods of prevention alone are not enough to make them protect hence, the detection must be merged to it as the other type of defense before the attacker may crack the system. Within this paper, the various characteristics have to be described of the ad-hoc-networks and few of attacks in the ad-hoc-networks. In addition to that, a comparative analysis regarding the previous IDSs is also being presented.

KEY WORDS: IDS, , mobile-ad-hoc-network, security, characteristics , MANET.

I. INTRODUCTION

Intrusion-Detection-System is a type of application which is used for observing network and securing it from an intruder. Along with the increased progress in internet dependent technology the new application domains for the computer network have raised [1]. In case, the fields like business, financial, industry, security and the health-care domains, the LAN applications and the WAN applications have advanced. All these areas of application have made the network an interesting goal for abuse and a huge susceptibility for community. Malignant users or the hackers utilize the company's internal-systems to gather details and create susceptibilities such as the Lapse in the administration, Software-bugs, leaving systems to default configuration [2].

Intrusion-detection is the basic techniques at the back of securing the network against the intruders. Intrusion-Detection-System attempts to find and alert on the tried intrusions into the system or the network, in which an intrusion is taken to be any illegal or unwanted activity on that system or network [3]. In the MANET, every terminal may communicate the information with the terminals in its range and those that are beyond their range may share the information by using the method of multi-hop communication where the other terminal may receive and send the packets [4]. Various multi-hop-routing-protocols have been suggested for MANET. The demand on the mobility forces the research and the development to the faster, new and the long-distance-communication approaches. In addition with this, the fundamental network with the infrastructure which demand on rapid and immediately deployable networks may get arises. The ad-hoc networks are not used only in which deployment has to be rapidly done, but also in which it is not be possible or not commercial to utilize or made up architecture. Currently, it is no issue to make an ad-hoc-network by using only the two portable/mobile devices, as an example the two notebooks. The only need is they should have a communication-interface. This type of development requires advances in security.

Therefore, intrusion detection can be very suitable for the wireless-networks. An intrusion-detection is referred as method to recognize "any type of set of actions which are tried to compromise the confidentiality, integrity or the availability of the resource" [5]. The intrusion-detection-system observes the network or the system activities stored in the audit-data and utilize the patterns of the well-known attacks or the usual profile to find the potential attacks. The intrusion-detection is utilized within networks through comparing set of the baselines of the system with the present behavior of the system [6]. Hence, a general assumption is the abnormal and normal behaviors of the system can be characterized [5].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

As security is the basic issue of MANET, and as the MANET is dynamic by nature there are generally two kinds of attacks within MANET. These attacks are passive-attack and the active-attack. A Passive-attack never disrupts an operation of network. It simply detects the data of without any type of alert from network and the confidentiality of data has been got lost. It is complicated to find the passive-attack within network. The active-attacks may destroy the data and also disrupt an operation of network. The Black-hole-attack is the example of active attack. But IDS is comparatively a new methodology of techniques for the intrusion-detection approaches which have risen in the current years. The intrusion-detection-system's major role within the network is to support the computer-systems to design and deal along with attacks of network.

This paper is targeted on brief study of the susceptibilities within ad-hoc networks that affects the intrusion-detection, attacks which are possible on the ad-hoc networks along with a detailed overview and the various techniques of intrusion detection.

II. MANET

A mobile-ad-hoc-network is the group of wireless portable hosts that are creating vibrant-network architecture without any type of standard-infrastructure or centralized administration. The different characteristics of MANET consists of lack of the centralized- administration, dynamically changed network-topology, limited resources, wireless-communication, limited bandwidth, limited power, etc. Because of these types of features, the mobile-ad-hoc-networks are more susceptible to the attacks.

Attackers may be of any type. Identifying the type of attack and offering the solution to real-time attacks may be get done within real-time, through creating the multiple numbers of the wireless terminal within cluster, cluster-head, and applying Dynamic-Source-Routing (DSR)-protocol, detection of attack types, prevention of attacks, etc.

2.1 Types of MANET

2.1.1 Closed MANET

In a closed MANET, all mobile terminals communicate with each other by cooperating with each other with a common target, like it may be utilized in the rescue, emergency-services, or in military-operations and law enforcement operation.

2.1.2 Open MANET

Within an open-MANET, several mobile terminals are having separate targets that share the resources along with the global connectivity. But in few situations the terminals rejected to share their data, referred as the selfish terminals or misbehaving terminals.

2.2 Types of Attacks

Passive-attacks and the active-attacks are both possible within the MANET. Passive-attacks will not modify the data. It will simply read data and get demolish the confidentiality through snooping. But within the active-attack, data will be modified through the attacker that consists of altering the data or entering the new malignant data. This includes the overloading of the network or protecting terminals from using networks services efficiently.

2.3 Routing Protocols in MANET

The routing-protocols in between any pair of terminals in an ad-hoc-network may be complicated as the terminals may randomly move and may also leave or join the network. This implies that an excellent route at the particular time cannot work the seconds later on. Here are the protocols which are utilized within MANET:

2.3.1 Dynamic source Routing Protocol

DSR utilizes the source-routing to deliver the packets by MANET. Such that, sender of the data-packet detects a source-route that is a full-path from sender to receiver and involved it within packet-header [7]. The intermediary terminals utilize this information to examine if they must accept the packet and at where to send it. The protocol that operates on the two components: the route-discovery and the route-maintenance.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

2.3.2 Ad Hoc on-Demand Distance Vector Routing Protocol

An ADHOC the on-Demand-Distance Vector-Routing (AODV) is an enhancement of the Destination-sequenced-distance-vector routing (DSDV) since it reduces the number of needed broad-casts as it prepares routes based on the on-demand, opposite to the Destination-Sequenced-Distance-Vector routing (DSDV) that maintains the complete-set of the routes [8].

2.3.3 Temporally Ordered Routing Algorithm

The TORA utilizes a metric addressed to as "height" of terminal to allocate a direction to the links for sending the packets to the provided destination. The terminals heights may be completely ordered lexicographically and hence referred as a directed-acyclic-graph rooted at destination.

2.4 Vulnerabilities of Mobile Wireless Networks

The features of the mobile-networking environment discover the susceptibility in it for several attacks. Different types of attacks are there on the wireless-link like the passive-eavesdropping and the active-interfering. Since in the wired-networks the communication is only possible by the physical access of network-wires or it passes via various devices as the gateways and firewalls, on the contrary, the wireless-network may be attacked through any terminal and from any directions and it also attack on any of the terminal. The attacks may consist of getting access to the private message, information scrambling, and the intermediate terminal perform as the sender or the receiver. Based on the above details it is cleared that the ad-hoc network don't have an exact line or way for security, so each terminal may be performed as the monitor.

III. Intrusion Detection System

An intrusion-detection-system (IDS) is the security-system which controls computer system and the traffic of network and observes that traffic for the possible antagonistic attacks derived from the outside of the organization or company and also for the system attack or misuse generating from inside of the firm or organization. An Intrusion-Prevention-System (IPS) is the network threat/security securing methodology which audits the flows of traffic of the network to prevent and detect the susceptibility exploits. Two kinds of prevention-system are there which are based on Network (NIPS) and based on Host (HIPS). These types of systems observe the traffic of network and implicitly take proper actions to secure the networks and the systems. The IPS problem is the false-positives and false-negatives. The False-positive is explained to be an incident that generates an alarm in the IDS in which no attack is there. The False-negative is explained to be an incident that does-not generates an alarm as when the attacks are takes place.

The inline-operation may generate the bottle-necks like signature-updates, single point of failure, and the encrypted-traffic. The actions found within the network or system is analyzed by the IDS [9].

The kinds of the IDS based on data-collection approach consists of Network-based IDS (NIDS) and the host-based-IDS (HIDS). The Network-based IDS executes on the gate-way of the network or on the router and gathers and determines the traffic of network which flows by it. It may be essential to find out the attack from the outside which is not fit for the MANETs as no central-coordination is there. The host-based IDS gather the local-network-traffic to particular host. It is efficient for finding the attack from the inside.

With in the process of the IDS two main variances are there which can have the chances to be found as the false-negative and the false-positive. The false-negative have more risk as compare to false-positive as if there was no attack and the IDS is categorized as the doubtful activity which is termed as the false-positive it is not very harmful but in case an attack was there and the IDS does not find it to be termed as the false-negative then it may be very disastrous. An intrusion is a deliberate, illegal tried to manipulate or access the information or the system and contribute them unusable or unreliable. To be very precise if a doubtful activity is occurred from the internal-network it can also be classified as misuse.

3.1 Categories of intrusion detection system

The Intrusion-detection-system is categorized into the three categories:

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

3.1.1 Signature based detection systems

The signature-based-detection system which is also termed as misuse-based, this kind of detection is more efficient against the known attacks, and it is based on receiving of the continuous updates of the patterns and may be not able to find out the unknown existing threats or the recent releases.

3.1.2 Anomaly based detection system

This kind of detection is based on classification of network to anomalous and normal as this type of classification is depend on the rules or the heuristics more than the patterns or the signatures and application of this system is first
required to understand the normal-behavior of network.An anomaly dependent detection-system dissimilar to the misuse-based detection-system as it may find out the existing unknown risks.

3.1.3 Specification based detection system

This kind of systems of detection is capable for checking the processes and then matching original data along with program and if any of the Abnormal behavior may be generated an alert and should be updated and maintained as when a modification was done on inspection programs to be capable to find out the earlier attacks unknown and number of the false-positives what may be less as compare to anomaly-detection-system technique.

IV. LITERATURE REVIEW

[10] MANET consists of mobile terminals, capable of communicating with other terminals, which are present in their surrounding and in this way forming the network. The network is formed on ad- hoc basis and this network is not having any centralized control which makes this network infrastructure less. The network formed in this way is vulnerable to security attacks due to its welcoming nature for any mobile device capable of communicating and nature of transmission. The transmission to different terminals is omni-directional. Any terminal can't be restricted from getting the messages sent from neighboring terminals and having a transmission range up to that particular terminal. In this paper, the structure of an Intrusion detection system is reviewed and tries to find out how each terminal can be equipped with such mechanism to avoid the security attacks.

IDS architectures discussed and reviewed are having their applicability to different networks. In standalone architecture like network, IDS is provided to each terminal having the mechanism to detect attacks. These mechanisms are secure, but have the limitation in energy consumption because the energy consumption itself is a big constraint in MANET. Distributed and collaborative IDS architecture requires the collaboration among different modes where the susceptibility comes along with collaborating-terminals. In few situations, it can result in the inclusion of the malicious or un-trusted terminal to take part in the security mechanism depending on the type of attacker. So, the structure of the IDS doesn't only depend on its type chosen to adopt, but also on mobile environment and support available from different mobile terminals.

In this paper, [11] suggested a recent IDS referred as EAACK – Enhanced-Adaptive-Acknowledgement. It is especially developed for the MANET that solved not only the receiver-collision and the restricted transmission-power but false-misbehavior issue also. An EAACK model makes the use of the digital-signature, to protect attacker from counterfeit the Acknowledgment-packet. It needs all the Acknowledgment-packet to be signed digitally. An EAACK may include of the three main parts called as S-ACK, ACK and MRA.

In first the ACK-mode, in starting the sender sends packet to destination, all intermediate terminal contributes to send the packet to the destination. After receiving the packet by destination it is required to send back Acknowledgment packets to receive, it waits for the Ack packet. Within a predefined time interval, if the source terminal received a acknowledgement from receiver, then the packet transmission is declared as successful. Or, the source-terminal may move to the S-ACK mode, by sending out an S-ACK data packet.

For IDS in Data mining, as the data-mining is a process of deriving the hidden-knowledge from databases so the IDS are very significant within data-mining. The Intrusion-detection consists of recognizing the set of the malignant actions which compromise the availability and integrity of the information-resources [12]. The Intrusion-detection within data-mining has the two-divisions, which are, the misuse-detection and the anomaly-detection. Within the misuse-

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

detection the labeled-data are made by using the anticipating-model [13]. In the anomaly-detection a deviation is there in between the models. To utilize the data first it should be converted into featured-data and data-mining schemed are implemented to it and which are summarized to produce the result.

[14] The migration to wireless network from the wired-network has been the universal trend within last some decades. An open-medium and the huge distribution of the terminals build the MANET susceptible to the malignant attackers. The recent approach EAACK (Enhanced-Adaptive-Acknowledgement) technique was designed for the MANET was suggested for the intrusion-detection. The EAACK represents the higher malignant behavior-detection rates in specific situations whereas does not affect greatly the performances of network.

The attack type of packet-dropping always has been a main risk for security in MANETs. In the new technique the Intrusion Detection Systems named EAACK protocol specially designed for the MANETs and also compared it against the other famous schemes like Watchdog scheme in different scenarios through simulations. The outcome represented the positive performances against the Watch-dog in the cases of receiver collision and false misbehavior report.

In the IDS for cloud computing, the Cloud-computing is illustrated as the internet dependent computing cloud in which, the virtually shared servers offers the software-infrastructure platform-devices and the other resources, hosting to the customer as the service on pay-as you-use based[15]. The customer of cloud never holds any of the physical architecture in place of this they hire from mediator or third-party. They charge only for usage of resource. The Intrusion-detection-system performs a vital role within security and the perseverance of the active-defense-system against the intruder adverse attacks for any of the business and an IT firm. Within the cloud-computing, applications are achieved on remote-server of provider and have control for the handling of data. The IDMEF (Intrusion-detection-message-exchange-format) is a standard utilized within cloud for communication objective.

V. CONCLUSION

Within this paper, initially survey on several attacks, issues and the solutions within MANET have been discussed, then here suggested an intrusion-detection-system that may detect the misbehaving connection in the decent manner and within the short-time also the IDS is applied on that terminal is also reliable. Due to this vulnerability, intrusion-prevention techniques like an encryption and authentication are not able to eliminate the attacks. Therefore, IDS has become an unavoidable and important component to provide defense-in-depth security mechanisms for MANETs. In terms of the performance, the intrusion-detection-system has now becomes very exact as it finds out more attacks and generates less false-positive-alarms. Intrusion detection systems must integrate with such networks and devices and provide support for advances in a comprehensible manner. In this paper we have presented the characteristics of MANET, attacks in MANET and comparison of previous IDSs.

REFERENCES

[1] Tripathi,S.S. and Agrawal,S.- "A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network"-International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012.

[2] Jaleel,A. -"Security Challenge in Cloud Computing"- Provided by International Journal of Engineering Sciences & Research Technology (IJESRT), Feb 2014.

[3] Kachirski,O. and Guha,R. "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN'02) 2002 IEEE.

[4] Sahu,S. and Shandilya,S.K ―A COMPREHENSIVE SURVEY ON INTRUSION DETECTION IN MANET‖ International Journal of Information Technology and Knowledge Management July-December 2010, Volume 2, No. 2, pp. 305-310.

[5] Nakkeeran,R. Albert,A.T, and Ezumalai,R "Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc Networks", IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[6] Saminathan,R. Selvakumar,K. "PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network", International Journal of Computer Applications (0975 – 8887) Volume 7– No.14, October 2010.

[7] Baisakh, "A Review of Energy Efficient Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", International Journal of Computer Applications Volume 68– No.20, April 2013.

[8] Ramprakash,S. Jayaraj,S. and Vigneswaran ," Energy Savings in Mobile Adhoc NETworks (MANET) Using Routing Protocols", Journal of Engineering And Technology Research, 2014.

[9] Ashoor,A.S, Gore,S. – "Importance of Intrusion Detection System"-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 2, February 2016

[10] Munjal,R. Kansal,G. "A Review On Intrusion Detection System Applicability And", International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 6, 2015.

[11]. Elhadi M. Shakshuki, Nan Kang, and Sheltami,T.R "EAACK- A Secure Intrusion Detection System for MANETs" IEEE trans. Vol.60, no.3, MAR, 2013.

[12] Parag K. Shelke, Sneha Sontakke, Dr. A. D. Gawande – "Intrusion Detection System for Cloud Computing". International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012 ISSN 2277-8616 67 IJSTR, 2012.

[13] Abhaya, Kumar,K. , Jha,R. and Afroz,S. "Data Mining Techniques for Intrusion Detection: A Review", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014.

[14] Chelvan,K.C, T.Sangeetha, V.Prabakaran, AND D.Saravanan, "EAACK-A Secure Intrusion Detection System for MANET", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 2, Issue 4, April 2014.

[15] A. Kumbhare, M. Chaudhari, "IDS: Survey on Intrusion Detection System in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014.