Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Analytical Study of Various Types of Intrusion Detection System for Securing MANET

Jyoti*
Research Scholar
Department of Computer Science (M.E. 4th Sem)
Haryana Engineering College,
Jagadhari, KUK, Haryana, India

Er. Richa Gupta
Senior Lecturer
Department of Computer Science
Haryana Engineering College,
Jagadhari, KUK, Haryana, India

Abstract— Due to the vulnerable nature of MANET (Mobile Ad hoc Network) there will be the necessity of protecting the data,information from the attackers whom evil eyes on MANET as it is infrastructure less network.So, it is applicable in various fields for the communication purposes such as in rescue operations, tactical operations.Thus, securing the such demanding network is a big challenge in itself. At this point IDS (Intrusion Detection System) came into existence to secure MANET in detecting at what point they are getting weak?

Thus, this thesis will discuss the three main approaches:-

1. ***The first approach include the analytical study of various types of intrusion detection system with their environment.In addition to this we will also discuss the points where intrusion detection system are came under question mark?***
2. ***The second approach deals with what are the desirable tools for the intrusion detection system which makes them ' Comfortable '.What type of security a particular user wants for securing his confidential environment from being attacked?***
3. ***The third approach deals with the implementation of the most widely used open source intrusion detection system ' Bro '.Here we not only deals with how the installation of bro is done for security purposes but also there will be brief discussion about two of the main challenges in intrusion detection system will include :-***
   - ✓ ***Analysing big amount of packets***
   - ✓ ***Encrypted traffic within the network***

Finally, there are some suggestion which will make bro a more user friendly and built-in programme package which include web server , database and other libraries that are needed to run it properly with all its features.

Keywords— MANET, Intrusion Detection System,Vulnerable nature of MANET, Bro, Web Server

I. INTRODUCTION

Security is the major concern to mobile ad hoc networking because a MANET system is much more vulnerable to malicious exploits than wired (traditional) network.First of all,the use of wireless links makes the network susceptible to attacks ranging from passive eavesdropping to active interfering. In the MANET network the attacks can be on all different direction and they can easily target anyone node. The damaging include the leaking of secret information , message contamination and node impersonation. All these mean that MANET will not have a clear line of defense, and every node must be prepared for encountered with an adversary directly and indirectly.

Second, mobile ad-hoc networks are autonomous units that are capable of roaming independently. This means that the nodes with inadequate physical protection are receptive to being captured, compromised and then hijacked among networks.Since noting a particular mobile node in large scale ad-hoc network may not be easily done, attacks by a compromised node from within the network are far from damaging and much harder to detect . Therefore , mobile nodes and the infrastructure must be prepared to operate in a mode that trusts no peer.

Third ,decision making in MANET is not centralised and some wireless network algorithms rely on the cooperative participation of all nodes and the infrastructure. This vulnerabilities for new types of attacks designed to break the cooperative attacks.

Thus, due to the above mentioned vulnerable nature of MANET these system are always the prime target for the various intruders who seeks to gain valuable information from these network in the form of various attacks.

II. VARIOUS TYPES OF ATTACKS ON MANET

The attacks on MANET can be distinguish below :-

1) Attacks on the basic mechanisms such as routing of the ad hoc networks
2) Attacks on the information in Transit in the ad hoc networks

Alternatively, attacks against mobile ad hoc networks can again be divided into two groups in a different way:

Attacks on Information in Transit

In addition to exploiting vulnerabilities related to the protection and enforcement of trust levels,compromised or enemy nodes can utilize the information carried in the routing protocols packets to launch attacks.These attacks can lead to corruption of information,disclosure of sensitive information,theft of legitimate service from other protocol entities,or denial of network service to protocol entities.Threats to information in transit include :

Interruption (The flow of routing protocols packets,especially route discovery messages and updates,can be interrupted or blocked by malicious nodes.Attackers can selectively filter control messages and updates, and force the routing protocol to behave incorrectly.)

Modification (The integrity of the information in routing protocol packets can be compromised by modifying the packets themselves.False routers can be propagated, and legitimate nodes can be bypassed.)

Fabrication (False route and metric information can be inserted into legitimate protocol packets by malicious insider nodes.)

Attacks Against Secure Routing

These attacks are basically of two types : Internal and External. In this external attacks can again be classified as active and passive attacks.Here we are briefly going to discuss these kinds of routing attacks.

Internal Attacks (An internal attack is a severe threat to ad hoc networks.The attack may broadcast wrong routing information to other nodes within the network. A compromised node is categorized as an internal attack.Detecting such wrong information in routing information is difficult because compromised nodes are able to generate valid signatures using their private keys.Also distinguish between an actual attacker and a change in topology may be problematic because the topology of the ad hoc network dynamically changes.)

External Attacks: These attacks can be classified into the two categories :passive and active

Passive attacks involves unauthorized '' Listening'' to the routing packets.The attack might be an attempt to gain routing information from which the attacker could extrapolate data about the positions of each node in relation to the others.

Active attacks on the network from outside sources are meant to degrade or prevent message flow between the nodes.Active external attacks on the ad hoc routing protocol can collectively be described as denial-of-service attacks,causing a degradation or complete halt in communication between the nodes.This type of attack involves insertion of extraneous packets into the network in order to cause congestion. Some types of active attacks that can usually be easily performed against an ad hoc network are :

A. Black hole*:* In this attack,a malicious node uses the routing protocols to advertise itself as having the shortest path to the node whose packets it wants to intercept.In a flooding based protocol,the attacker listens to requests for routes.When the attacker receives a request for a route to the target node,the attacker creates a reply consisting of an extremely short route.If the malicious reply reaches the requesting node before the reply from the actual node does,a forged route has been created.Once the malicious device has been able to insert itself between the communication nodes,it is able to do anything with the packets passing between the communication nodes, it is able to do anything with the packets passing between them.It can choose to drop the packets to perform a denial-of-service attack or alternatively use its place on the route as the first step in a man-in-the middle attack.

B. Routing table overflow: In this attack, the attacker attempts to create routes to non existent nodes.The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation.

C. Sleep deprivation*:* This attack is practical only in ad hoc networks where battery life is a critical parameter.Battery powered devices try to conserve energy by transmitting only when absolutely necessary.An attacker can attempt to consume batteries by requesting routes or by forwarding unnecessary packets to the node using black hole attacks.

D. Location disclosure*:* A location disclosure attack can reveal something about the locations of nodes or the structure of the network.The information gained might reveal which other nodes are adjacent to the target or the physical location of a node.Routing message can sent with inadequate hop-limit values and the addresses of the devices sending the Internet Control Message Protocol error messages are recorded.

III. SECURITY NEEDS OF MANET

This term is liberally used in computer network terminology .The basic security needs ,more or less, are the same as those for wired networks and wireless networks.In the following,we briefly introduce the standard terms that are used when security aspects of the network are discussed :-

Availability

Availability means that services provided by a node continue to be provided irrespective of attacks .Nodes should be available for communication at all times.

Authenticity

Authenticity is essentially confirmation that parties in communication with each other are genuine and not impersonators. This would require the nodes to somehow prove that their identities are what they claim to be.

Confidentiality
An outsider should not be able to access information in transit between two nodes. This ensured that information is not disclosed to unauthorised entities. For confidentially,it is necessary to prevent intermediate and non trusted nodes from understanding the content of the packets being transmitted.

Integrity
Integrity is the guarantee that the message or packet being delivered has not been modified in transit or otherwise,and what has been received is what was originally sent.

Non repudiation
Non repudiation means that the sender of a message cannot later deny sending the information and the receiver cannot deny the reception. This can be useful while detecting and isolating compromised nodes.Any node that receives an erroneous message can accuse the sender with proof and,thus,convince other nodes about the compromised nodes.

Ordering
Updates received from routers are in order ,the non occurrence of which can effect the correctness of routing protocols.Messages may not reflect the true state of the network and may propagate false information.

Timeliness
Routing updates should be delivered in a definite interval of time.Update messages that arrive late may not reflect the true state of links or routers on the network.They can even propagate false information and weaken the credibility of the update information.

Isolation
Isolation requires that the protocol be able to identify misbehaving nodes and render them unable to interfere with routing.Alternatively, the routing protocols should be design to be immune to malicious nodes.

Authorization
An authorized user or node is issued an unforgeable credential by the certificate authority which indicate that the communication with that particular user is authorised.These credentials with certificate specify the privileges and permission associated within the users or the nodes.

Location Privacy
Often.the information carried in message headers is just as valuable as the message itself.In network structure the routing protocol should maintain privacy regarding information about the location of the nodes within the network.

Anonymity
The mobile node must not be expose any information that allows any conclusions on the owner or the current user of the node.

IV. OVERVIEW OF INTRUSION DETECTION SYSTEM

Intrusion Detection System(IDS) are software/hardware systems which are design to monitor network traffic or computer activities and alerts alarms to administrators when some suspicious intrusion activities are detected.They plays a very important role in securing MANET from becoming the target of any intruder whose aim is to gain confidential information by attacking on the system.

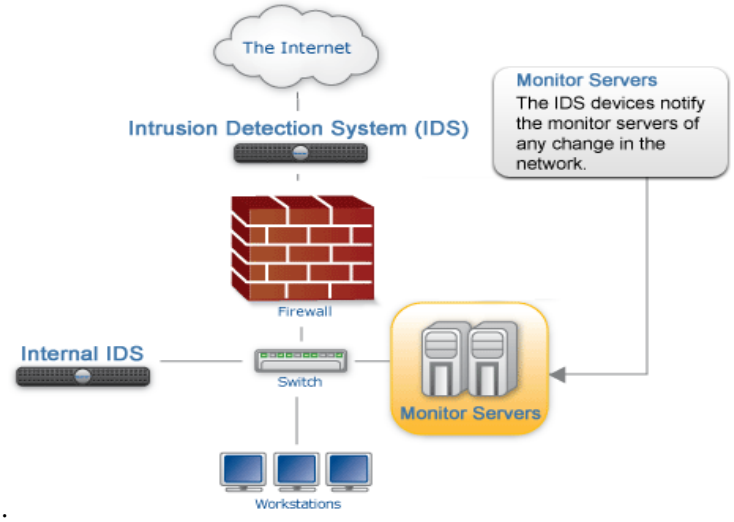

Figure 1:-Intrusion Detection System

The various intrusion detection system used for securing MANET (which are taken for analytical study) are listed below :-

A. Signature Based Intrusion Detection System
B. Anomaly Based Intrusion Detection System
C. Specification Based Intrusion Detection System
D. Network Based Intrusion Detection System
E. Host Based Intrusion Detection System
F. Distributed Intrusion Detection System

All of the above listed IDS will be briefly discussed below :-

***A. Signature Based Intrusion Detection System* :-**These analyse system activities looking for events matching a predefined pattern or signature that describe a well known attack.They collected network traffic and then proceed to analyse it.

***B. Anomaly Based Intrusion Detection System* :-** This anomaly detection focus on identifying unusual behaviour in a host in the network.They operate assuming that the attacks are different from normal activities. They construct profiles representing the normal behaviour of the users,hosts or network corrections.These profiles are constructed from the historical data collected during normal operation.

***C. Specification Based Intrusion Detection System* :-** In this system defines a set of constraints that describe the correct operations of the program or the protocols.Then it is going to monitor the execution of the program with respect to the defined constraints.

***D. Network Based Intrusion Detection System* :-** The network based IDS are often formed by a set of sensors located at various points of the network. These sensors monitors traffic doing local analysis and reporting attacks carried out to management console.

***E. Host Based Intrusion Detection System* :-**These are the first type of IDS developed and implemented.They run on the information acquired from inside a computer, such as audits files of the operating system.This allows the IDS to analyse actual activities with great precision.

***F. Distributed Intrusion Detection System* :-** These are those which combines distributed monitoring and data reduction with centralized data analysis to monitor a heterogeneous networks

V. LITERATURE SURVEY

Amrita Anand et al. [1] in this paper it is concluded that IDS is used for defending networks from intrusions and desirable to understand the security risks and threats including rocognizing incoming and running network attacks.Though the research has introduced a new methodology to identify a fast attack intrusion using time based detection.There is a need to plan and investigate the use of other protocol and other flag to recognize the fast attack intrusion activity. This research introduces an approach that will be implemented on a production network for accessing the performance on the anomalies using time based detection.

Manjeet Singh et. al [2] in this paper they said that after anlyzing the security threats faced by network, it finds that there is a need to make them more secure by developing a multilayer security system resulting in depth protection and defanse against both known and unknown threats.

Arun Kumar et. al [4] in their paper summaries challenges and attacks in MANET such as black hole attack,DOS attack and warmhole and gives brief barriers of MANET, yet this paper gives a deep understanding regarding security threats in MANET and acts as a source for people working towards MANET.

S. Sujata et. al [5] provides a study of a new intrusion detection system named EAACK protocol which gives positive performance against Watchdog, TwoAck and AACK. But no system is perfect so there is need to develop new security policies that can be deployed into MANET. Attackers attacks with new ideas and to defend them there is a need of constant research on the nature of new attacks.

Mughda A. Kirkire et. al [9] on surveying different types of attacks, problems and solutions in MANET hopes for a detection system that finds out a misbehaving link in short time in a reliable manner and removing the misbehaving node to avoid the future network damage.

Ashish Kumar et. al [12] they comparatively evaluated that despite of many open source IDS, Snort is the best alternative system to ensure network security. Snort should detect the attack and at the same time it should trigger some action that alerts the user about the attack.

VI. CONCLUSION

Securing Mobile Ad hoc Networks by Intrusion Detection Systems are the very much popular area of research among the researchers. The vulnerable nature of MANET makes it in the target list of attackers. In this paper we have discuss not only the characteristics of MANET but also the various attacks on it and analytical study of the various types of Intrusion Detection System (IDS) are done.This paper also deals with the various additional tools used in IDS to make them comfortable to work for securing MANET. In this proper installation of BRO Intrusion Detection System is done along with the two main problems like analysing big amount of packets and encrypted traffic within the network.

VII. FUTURE WORK

In future our main aim is to design and implement an Intrusion Detection & Prevention System using open source product which can be applied to small sized to large size network.

REFERENCES

[1] Amrita Anand and Brajesh 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 ISSN:2277 128X

[2] Manjeet Singh and Gaganpreet Kaur ‘‘ A Surveys of Attacks in MANET ’’ International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 3, Issue 6, June 2013 ISSN:2277 128X

[3] Ms Priyanka P Kulkarni ‘‘ A Survey of Secure Intrusion Detection System for MANET ’’ International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 5, Issue 1, January 2015 ISSN:2277 128X

[4] Arun Kumar. R, Abhishek M.K, Tejaswini A.I, Niranjan J.T, Pradeep R.P‘‘ A Review of Intrusion Detection System in MANET ’’ International Journal of Engineering Science and Innovative Technology, Volume 2, Issue 2, March 2013 ISSN:2319 5967

[5] S. Sujata and B. Lakshmi, Radhika ‘‘ A study on Enhanced Adaptive Acknowledge (EAACK) Schemes in Receiver Collision- An IDS in wireless Mobile Ad-hoc ’’ International Journal of Engineering and Science ,Volume 2, Issue 9, 2013 , ISSN (e): 2319-1813 ISSN(p) :2319-1805

[6] Usman Asghar Sandhu, Saajjad Haider,Salman Naseer, and Obaid Ullah Ateeb , ‘‘ A study of the novel approaches used in Intrusion Detection and Prevention Systems ’’ International Journal of Information and Education Technology ,Volume 1, No. 5, December 2011

[7] Sakil Ahmad Ansari and Mohammad Danish ‘‘ An Analytical Approach on Intrusion Detection System in MANET for attacks ’’ International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 3, March 2014 ISSN:2277 128X

[8] Chintan Kacha, Kirtee A. Shevade , ‘‘ Comparison of Different Intrusion Detection and Prevention Systems ’’ International and Journal of Emerging Technology and Advanced Engineering , Volume 2, Issue 12, December 2012 IISN 2250-2459

[9] Mughda A Kirkire, Poonam Gupta , ‘‘ Intrusion Detection in Mobile Ad hoc Network ’’ International Journal of Industrial Electronics and Electrical Engineering, Volume 2,Issue 4,April 2014, ISSN :2347-6982

[10] Zougagh Hicham, Toumanari Ahmed , Latif Rachid and Idhoufker Noureddin , ‘‘ Evaluating and Comparison of Intrusions in Mobile Ad hoc Networks ’’ International Journal of Distributed and Parallel Systems , Volume 3, Number 2, March 2012

[11] Pritika Mehra , ‘‘ A Brief Study and Comparison of Snort and Bro Open Source Network Intrusion Detection Systems ’’ International Journal of Advanced Research in Computer and Communication Engineering ’’ Volume 1,Issue 6, August 2012, ISSN: 2278-1021

[12] Ashish Kumar, Shrikant Chandak , Rita Dewanjee , ‘‘ Recent Advances in Intrusion Detection Systems : An Analytical Evaluation and Comparative Study ’’ International Journal of Computer Applications, Volume 86, Number 4, January 2014, ISSN: 0975-8887

