Intrusion Detection System in Mobile Ad-hoc Network

Trupti .P. Patil
Lecturer
RAIT, Nerul, Navi-Mumbai
Maharashtra

Bharti Joshi, Ph.D
Professor
Sarswati College of Engg. Kharghar,
Maharashtra.

ABSTRACT

In recent years, the security issues on MANET have become one of the primary concerns. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile connected without wires. IDSs are designed for wired networks and work only under certain conditions, i.e. having an infrastructure with central authority, no cooperative algorithms. Security is mainly achieved by prevention, i.e. to make attacks as difficult as possible These conditions are not or only partially fulfilled by MANETs. The MANET is more vulnerable to be attacked than wired network. For this reason, there is a need of mechanism to detect and response these newer attacks, i.e. "intrusion detection". The disadvantage of misuse detection is unable to detect Unknown attack and anomaly detection generates the false alarm any time traffic. To solve this problems we are combining anomaly and misuse detection technique to explore and to classify current techniques of Intrusion Detection System that aware MANET. This Paper organized into four part first part contains introduction of IDS,MANET ,second part contains attacks on MANET ,third part contains proposed model and last part contains conclusion and references.

General Terms

Intrusion Detection System, MANET

Keywords

IDS, Attack, MANET, Security

1. INTRODUCTION

The intention or purpose of an attack is in the following named as the target. Most attackers have an object while attacking a network, e.g., getting access to confidential information, spoofing the own identity. The target of an attack to networks may vary widely. Stajano and Anderson name four targets: Availability, authenticity, confidentiality and integrity. IDSs differ from one another quite largely. However, there are three main components in which an intrusion detection system can be classified[12].

1.1 Network -based IDSs

The commercial intrusion detection systems are implemented as network-based IDSs. The sensors gathers the information which are stored in segments of the network. The sensors are well hidden.The fig.1.1 shows architecture of Network IDSs[12]

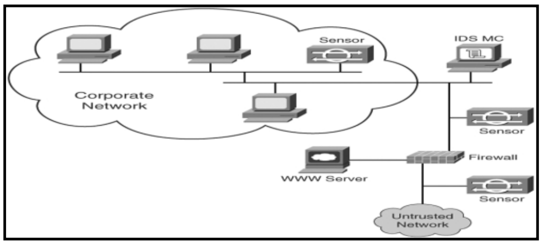

Fig.1.1 Network IDS

Advantages

- Network-based IDSs are almost invisible, It makes them secure against attacks.
- In the network-based IDSs there are no changes .There is small change in architecture infrastructure.
- The sensor are placed at crucial points, large network can be monitored by few sensors

Disadvantages

- Due to a large and busy network the sensors have to analyze massive amount of data, which makes them more likely to fail.
- Network-based IDSs failed in networks where the traffic is encrypted.

1.2 Host-Based IDSs

The collection of the data takes place at the individual participants of the network in the Host based IDSs. It uses either the operating system audit trails or the system logs. Audit trails are generated by the kernel of the OS. They are much more detailed than the system logs. Even It is using the less accurate system logs which allows a better analysis of the network than with network-based IDS. It exist decentralized host-based IDS solutions, where the hosts report their outcomes to a single management console.The fig.1.2 shows the architecture Host IDSs[12].

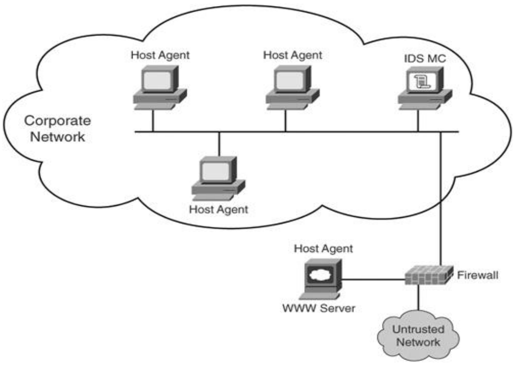

Fig.1.2 Host IDS

Advantages

• The Host IDS ability to gather information nearby, host-based IDSs detect attacks as compared to network-based would not detect the attack.

• In distinction to network-based IDSs, encrypted network traffic exploited in host-based can be .

Disadvantages

•More complexity to administration of system, because the administration and configuration should be done on every host individually.

• An attack may not only hit the node, but also disable a part of the IDS,

• The investigation is made by the hosts, using their reckoning power for intrusion detection instead of their main purpose.

2. IDS ANALYSIS

After congregated a lot of data from the activities and events in the network, the information has to be administered to detect attacks. This should be done by the IDS analysis [1][8][12]. These three methods are as follows:

2.1 Misuse Detection

In misuse detection attack should be detected. It uses a large database of known attacks and matches them with the going on events. If the known attacks the system appearances for a unique pattern, the so called signature. Therefore, this technique is sometimes also named as signature-based detection. The database has to be updated, recurrently. For IDS Analysis this technique is the most widely spread method in commercial system. However, most of them are combining misuse detection with anomaly detection, because misuse detection detects only attacks that are already present in the database.

2.2 Anomaly Detection

Anomaly detection works with a profile which represents the status of normal activities, i.e. activities that do not fit to an attack or to the preparation of one. Whenever an event monitoring is going on that does not belong into the profile, the system has to select whether it is an attack. For this purpose it works with a threshold: once the threshold is exceeded, it raises an alarm.

For instance, the system has monitories the behavior of users over a period and intended a profile of normal activities concerning accessing less on the hard drive. Anomaly many files on the hard drive, user that access those files viewed as misbehaving user. The systems has a much higher false positive rate than misuse detection, it also produce more false negative. This is because it does not detect attacks that behave "normal" and it defendant authentic actions.

2.3 Specification-based Detection

In the system which uses specification-based detection defines a set of restrictions for a correctly behaving program or protocol. These restrictions define exactly, what an application is allowed to do. It monitors the operations of the program or protocol against the restrictions. To detect unknown attacks with a lower false positive rate than the anomaly detection that’s the advantage.

3. INTRUSION RESPONSE

Intrusion response is nothing but detecting an attempt of an attack or only suspicious activities, the IDS activate countermeasures. The responses can be categorized into two types [12].

3.1 Active Response

The action that are automatically triggered by the IDS which is calledas Active response. Once an intrusion has been detected, there is no need of human collaboration[12].

3.2 Passive Response

In the passive response actions the IDS has only a secondary role, it provides information to humans. The IDS generate reports for administrators based on the collected information[12].

3.3 Control Strategy

The control strategy of an intrusion detection system defines how the elements and how the input respectively output of IDS is managed. It names three different possibilities of control strategies: centralized, partially distributed and fully distributed[12].

4. MANET

Mobile Ad-Ho Network(MANET) are networks that are made from mobile phones and power infrastructure nodes under controlled self-organization, all nodes share the same functions respect to the operation of the network. It is vulnerable to security attacks due to its characteristics of open environment, dynamic topology changes, the cooperative algorithms, lack of centralized monitoring, management point, and the lack of a clear line of defense .Attacks on mobile ad hoc networks can be classified into following two categories [13].

4.1 Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it[13].

4.2 Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks External attacks are carried out by nodes that do not belong to the network.

4.3 Black hole Attack

Black holes refer to places in the network where incoming traffic is silently discarded, without informing the source that the data did not reach its intended recipient. In this attack, an attacker or malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a false reply consisting of an extremely short route. If the malicious reply reaches the source node before the reply from the actual node, a fake route gets created[13].

4.4 Wormhole Attack

A wormhole attack is composed of two attackers and a wormhole tunnel. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnels can be established by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel.[11][13].

4.5 Denial of Service (DoS)

Denial of service attack, aims to crab the availability of certain node or even the services of the entire ad hoc networks. Denial of service attack, aims to crab the availability of certain node or even the services of the entire ad hoc networks[13].

5. PROPOSED MODEL

IDS solutions for ad hoc networks cannot be applied directly to MANET. Therefore, the proposed intrusion detection system must meet the demands and restriction of WSNs.

Hybrid approaches may also prove of significant use. So we proposed one hybrid system for IDS in MANET. Regarding MANAET security issues, none of the systems are complete. They usually emphasize just a few specific MANET concerns. The range of MANET issues should be considered during design to ensure effective and efficient intrusion detection suited to the environment at hand.

5.1 IDS Architecture with Cloud Secures Database

A distributed architecture consisting of IDS agents and a cloud secure database (SSD) is proposed here[5][6]. All nodes have IDS agents responsible for local detection and collaborating with other agents in need. IDS agents have five components: local audit trail; local intrusion database (LID); secure communication module; anomaly detection modules (ADMs); and misuse detection modules (MDMs). The local audit trail gathers and stores local audit data network packets and system audit data. The LID is a database that keeps information for IDS agents such as attack signatures, patterns of normal user behavior, etc. The secure communication module is used only by IDS agents to communicate securely with other IDS agents. ADMs use anomaly-based detection techniques to detect intrusions.

The Cloud secure database (CSD) maintains the latest attack signatures and latest patterns of normal user behaviors. It is to be held in a secure environment. Mobile agents get the latest information from the CSD and transfer their logs to the CSD for data mining. The CSD has more storage and computation power than mobile nodes, so it is capable of mining rules faster than the nodes in the network and can keep all nodes logs. Moreover, updating the CSD rather than all nodes in the network is easy. On the other hand, a cloud database is suited to all kinds of networks. However, nodes in hostile environments can be attached to the CSD.

5.2 Framework

In other section, we propose a distributed cooperative trust based intrusion detection architecture for MANETs. The architecture is based on running Local Intrusion Detection engines in each node independently. The objective is to monitor all network activity within wireless range to detect misbehaving nodes on promiscuous mode. That means, if node A is in wireless range of node B, it can watch communication activity to and from B even node A is not involved in. Intrusion detection data in this manner has significant advantage. First, it allows local data collection without consuming any additional communication overhead. Second, it provides first hand observations, which means no need to rely on observations from other nodes, which might be false. Flooding algorithm is used to share IDS alert messages. Flooding is the mechanism by which a node receives a flooded message for the first time, it rebroadcasts that message once. Each node is responsible to deliver the message to its neighbor within wireless transmission range. A compromised node can disseminate false IDS alert messages or drop the IDS alert message flooded by other nodes. Therefore, a trust mechanism is established in the network[5][6]. Such as dropping messages o unwillingness for cooperation. Reputation mechanism is used as a dynamic rating system. Once, a node detects misbehavior of a neighbor node or suspicious activity, it starts a distributed IDS algorithm by Broadcasting IDS alert messages. If a trustworthy node broadcast an IDS alert message, intrusion response is activated even if the relevant node is not directly involved in IDS assessment Figure 1.6 depicts the components of the framework.

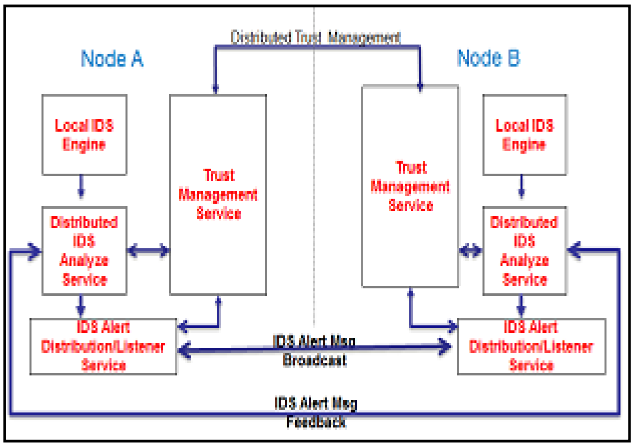
Distributed Trust Management
Node A
Node B
Local IDS Engine
Trust Management Service
Trust Management Service
Local IDS Engine
Distributed IDS Analyze Service
Distributed IDS Analyze Service
IDS Alert Distribution/Listener Service
IDS Alert Msg Broadcast
IDS Alert Distribution/Listener Service
IDS Alert Msg Feedback

Fig. 1.3 Components of framework

5.2.1 Local IDS Engine

The first phase of the intrusion detection process starts at Local Intrusion Detection engine[1][8]. It sniffs the neighbor nodes network activity in promiscuous mode. The engine runs a popular network-based IDS, which is the open-source Snort Snort is able to sniff the network activity in promiscuous mode and configured with a rule set it can function as a real-time IDS. A Snort rule set is a file of attack signatures. A match to a signature means that an attack is recognized. Each node assumed to have the database of these rule sets and functions as a real-time detection system. Once an intrusion attempt or a suspicious activity is determined, all relevant data is passed to distributed IDS analyze service.

5.2.2 Distributed IDS Analyze Service

IDS analyze service will use outputs of the Local IDS engine as well as IDS alert messages disseminated from other nodes[5][6]. If there is enough evidence for intrusion, this service will put intrusion prevention measures into effect and forward the related information to IDS alert distribution service to inform the other nodes in the network. If there is weak or inconclusive evidence of anomaly IDS analyze service will request global analysis. Only the replies from the trusted nodes will be taken into consideration. The service will also try to verify the attack by additional IDS Alert messages originated from other nodes in the network. If the evidence comes via IDS alert message from another node in the network, first the trust level of the sender node is checked:

1. If the message is from a trusted node and there is more than one trusted node disseminating IDS alert message, than there is strong evidence for an intrusion attempt.

2. If the IDS alert message is from an untrustworthy node, the IDS message is ignored.

3. If the message is from a node, which the trust level has not been evaluated yet, then special interest is performed.

4. If the intrusion alert is supported more than a single node or an intrusion is also approved by local IDS, the service may conclude of an intrusion.

5.2.3 IDS Alert Listener / Distribution Service

This service is responsible to broadcast the IDS alert messages within wireless radio range and watches for the neighbor nodes if they rebroadcast the message within a time frame. Each message will have a unique message number and detected intrusion related information. IDS alert message contains:

1. Originator Message ID Sender Node ID
2. Sender Message ID
3. Compromised/Attacker node's ID/IP
4. Attack Type
5. Classification
6. Priority
7. Date/time

Immediately after, this service will inform the trust management service to evaluate reputation values. In addition, if this does not occur in a limited time frame or the rebroadcasted IDS alert message is corrupted then reputation and trust assessment is evaluated.

5.2.4 Trust Management Service

Trust management service is responsible to maintain relationships among nodes in the network.[1][5][6] This service will mitigate misbehaving of nodes and enforce cooperation. Projected trust management is derived form a reputation based scheme proposed by Jiangy hu. Trust in a node is associated with its reputation value. There are three trust levels and we use a trust value T, to represent the trustworthiness of a node. A node considers another node B either

1) Trustworthy, with T = 1,
2) Untrustworthy, with T = -1
3) Trustworthy undecided, with T = 0

A trustworthy node is a well-behaved node that can be trusted. An untrustworthy node is a misbehaved node and should be avoided in distributed IDS evaluation process. A node with undecided trustworthiness is usually a new node in the network and special interest should be taken in IDS evaluation process. Each node keeps a reputation table, which associates a reputation value with each of its neighbors. It updates the table on direct observation only. Reputation value of a neighbor node will not be distributed globally and will be stored locally. Reputation values will be shared only if requested by other nodes.

For a new node N with reputation value R and trust value T,

1. $T = 1$, if $R \geq Rt$
2. $T = -1$, if $R < Rt$
3. $T = 0$, if $R < 0$

Reputation values depend on the behaviors of the node. If a node broadcasts an IDS alert message, then it sniffs the neighbor nodes in promiscuous mode. If that node rebroadcasts the IDS alert message, the originator node promotes the reputation value for that node; otherwise, the reputation value is downgraded. If the rebroadcasted message is modified the nodes trust value will be in untrustworthy state. *R* is the proportion of the total number of forwarded messages to the total number of sent messages. Each node keeps track of the neighbor nodes and establishes reputation values directly. If a node needs to query a specific node that is beyond the wireless radio range, it will ask for reputation values to all the trusted nodes in the network. The average of the replies will set the reputation value for the requested node. Another factor for a node that will affect it is trust level is the correctness of the IDS alert message. All the nodes that receive an IDS alert message will also monitor the evidences. If there is not enough evidence, the IDS message is concluded to be false. So that the trust level for the disseminating false messages node will be untrustworthy.

6. ADVANTAGES AND DISADVANTAGES

A trust based distributed intrusion detection framework is proposed in order to protect nodes from performing misbehavior or selfish behavior in MANETS. Trust, in the framework, is mainly based on direct observation, but indirect observations are also applied. The proposed infrastructure provides robustness against the propagation of false trust information by malicious nodes. A dynamic and collaborative ad hoc intrusion detection system has been proposed. Our approach does not modify or restrict the network discovery or routing protocols. The concepts discussed in this paper are in broad sense that they can easily be integrated to existing routing protocols.

7. CONCLUSION

An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. In this survey paper, we try to inspect the security issues in the mobile ad hoc networks and the Misuse and Anomaly Detection can be used to detect the attack and also drawbacks are also overcome. The Model Proposed in this paper avoid the problem of SSD (cloud secure database)and add more portability for intrusion detection. Cloud database is suited to all kinds of networks. Military strategic environments with control centers are given as examples of the architecture suitable for CSD. The nodes in antagonistic environments can be attached to the CSD. Authorizing the nodes update themselves with the help of other nodes (which can consume significant bandwidth) is proposed as a solution. In real time we can apply this model to any routing algorithm like DSR, DSDV, AODV.

8. REFERENCES

[1] Anantvalee T, Wu J (2006) A Survey on Intrusion Detection in Mobile Ad Hoc Networks. Wirel/MobilE Netw Secur, Springer:170-196 .

[2] Axelsson S (2000) Intrusion Detection Systems: A Survey and Taxonomy. Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology .

[3] Buchegger S, Le Boudec J (2002) Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Network. In Proc of 10th Euromicro Workshop on Parallel, Distrib and Netw-based Process:403-410 .

[4] Heady R, Luger G, Maccabe A, Servilla M (1990) The architecture of a net-work level intrusion detection system Technical Report, Computer Science Department, University of New Mexico.

[5] Huang Y, Lee W (2003) A Cooperative Intrusion Detection System for Ad Hoc Networks. In Proc of the 1st ACM Workshop on Secur of Ad Hoc and Sens Netw:135-147.

[6] Huang Y, Lee W (2004) Attack Analysis and Detection for Ad Hoc Routing Protocols. In Proc of Recent Adv in Intrusion Detect LNCS 3224:125-145 .

[7] Parker J, Undercoffer Jetal (2004) On Intrusion Detection and Response for Mobile Ad Hoc Networks. In Proc of 23rd IEEE Int Perform Comput and Commun Conf .

[8] Smith AB (2001) An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks. In Proc of 5th Natl Colloq for Inf Syst Secur Educ.

[9] Zhang Y, Lee W (2011) Intrusion Detection Techniques for Mobile Wireless Networks. Wirel Netw : 545-556 .

[10] Intrusion detection system:Acomprehensivereview Hung-Jen Liao, hun-HungRichardLin ,Ying-ChihLin Kuang-Yuan Tun. Wormhole Attack in Wireless Ad-Hoc Networks Yahiya Ghanbarzadeh, Ahmad Heidari, and Jaber Karimpour. International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012.

[11] ISOLATION OF MALICIOUS NODE IN DOS SCENARIO IN MANET Pooja Er. Deepika Khokhar-ISSN:2229-6093

[12] Attacks and Intrusion Detection in Mobile AdHoc Network Assignment in Computer Science, Philippe Hunberbühler Supervisors Prof. Dr. Burkhard Stiller, Dr. Hasan Greg Schaffrath,University of zurich.