Co-operative Wireless Intrusion Detection System Using MIBs From SNMP

Ashvini Vyavhare, Varsharani Bhosale, Mrunal Sawant, Fazila Girkar

B .Tech Information Technology
Department of Computer and Information Technology
College of Engineering, Pune-5, MS, India.

{ashviniv9, varsharanibhosale145, mrunal08, fazilagirkar04}@gmail.com

Abstract.

In emerging technology of Internet, security issues are becoming more challenging. In case of wired LAN it is somewhat in control, but in case of wireless networks due to exponential growth in attacks, it has made difficult to detect such security loopholes. Wireless network security is being addressed using firewalls, encryption techniques and wired IDS (Intrusion Detection System) methods. But the approaches which were used in wired network were not successful in producing effective results for wireless networks. It is so because of features of wireless network such as open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense etc. So, there is need for new approach which will efficiently detect intrusion in wireless network. Efficiency can be achieved by implementing distributive, co-operative based, multi-agent IDS. The proposed system supports all these three features. It includes mobile agents for intrusion detection which uses SNMP (Simple network Management Protocol) and MIB (Management Information Base) variables for mobile wireless networks.

Keywords: Multi- agent, MIB, SNMP, Security

1. Introduction

Security is important in any environment. As large information is available on the network and it is possible to share this data through it, it should be secure. It is somewhat defined in wired network but in wireless there is great challenge of different attacks. People and organizations have been protecting their data from harmful activities using rules that identify and block such things. However current and future threats require development of more adaptive defensive tool.

Attack is an assault on system security that derives from an intelligent threat. It can be mainly classified as Active attacks and Passive attacks. Active attacks are in the nature of eavesdropping on, or monitoring of, transmissions while passive attacks involves some modification of the data stream or creation of false stream.[6]

Intrusion detection is the act of identifying intruders who attempt to compromise the integrity, confidentiality or availability of resource. It is used to secure the systems in the networks.[1] There is a common misunderstanding that firewalls do the same thing of detecting and blocking of attack by shutting off everything and then turning back on only some well-chosen items.[8] It just restricts access to the designated points. Securing the computer

DOI : 10.5121/ijnsa.2012.4211

networks with firewalls or using strong encryption algorithm keys are longer effective. This leads to the development of new architecture and mechanisms to protect wireless and mobile networks.

An IDS is a software or hardware tool that monitors traffic on network looking for and logging threats. The purpose of IDS is to monitor the computer networks, detect intrusions and alert the concern person. Network based (NIDS) and Host based (HIDS) are types of IDS. In NIDS traffic flowing through network is analyzed. In HIDS activities on each individual computer are examined.[3,8]

There are two ways on which basis we can implement IDS. The first one is signature based in which the attacks have unique signature that can be detected. Known attacks can be detected by looking for these signatures. Second approach is anomaly based in which a system develops a base line what it considers a normal traffic. Any activity which is recorded beyond this traffic is considered as anomaly and alert is generated.

2. Wireless Intrusion Detection System

The organizations invest in wireless networks as compare to traditional wired LANs because of its low cost and relative ease of use. Although the wired-IDS are powerful systems, unfortunately they do little for the wireless world. The main difference between wired and wireless networks is their nature of transmission medium, different protocol specification in lower layer, different lower layer functionality of the intruders etc. [4] The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The nature of mobility creates new vulnerabilities due to open medium, dynamically changing network topology, co-operative algorithms, lack of centralized monitoring and management points that do not exist in a fixed wired network, and yet many of the proven security measures turn out to be inactive. This has led to the development of new architecture and mechanism to protect the wireless networks and mobile computing applications. [5]

The various approaches like IDS using Neural Networks, Artificial Immune Systems, MANET based, Clustering, System calls based, co-operative agent based etc. are developed and implemented so far.

3. Problems related to wireless networks

Till now little research has been done in area of wireless IDS. Because of its structural and behavioral differences, IDS designed for wired networks is not that applicable to the wireless network.[7]

In case of wireless networks communication is done through an open air environment and the medium is not well protected .So it is impossible to monitor network traffic at bottlenecks. It is necessary to do monitoring at each and every network node. But it is inefficient due to high network bandwidth requirement and increased power resources that are not easily available.[7]

Ad hoc wireless networks are very dynamic in structure, giving rise to apparently random communication patterns, thus making it challenging to build a reliable behavioral model. Misuse detection requires maintenance of an extensive database of attack signatures, which in the case of ad hoc network would have to be replicated among all the hosts.[2] This will result in an extended initial setup time and decrease in useful computational power of each host.

Another problem is monolithic IDS design. Each node must have an IDS client and should take part in global detection process. To get rid of this problem modular IDS should be

implemented using mobile agents. By this we have many advantage of increase in fault tolerance, reduced communication cost, and improved performance of whole network and scalability.[7]

4. Architectures of Wireless IDS

The structure for the wireless mobile network can be configured depending on various applications. The optimal IDS architecture for a mobile network will totally depend on the network infrastructure itself. In a flat infrastructure, all the nodes are to the same level of priorities and in multi-layered network infrastructure nodes may be separated into different clusters for communication.

4.1 Stand-alone IDS

As its name suggests data is collected on each and every independent node. Depending on this information, decision is taken for detecting intrusions. In this architecture, each node runs separate IDS. No information or message is passed to each other. Even though restricted by its limitations, it is more adaptable in situation when each node can run an IDS on their own or have IDS installed it is much more preferred for a flat network architecture which will unfortunately not suitable for wireless mobile network.[2]

4.2 Co-operative and Distributed IDS

It is mentioned earlier that stand-alone IDS does not work properly. So, co-operative and distributed intrusion detection system architecture should be implemented. For this there are IDS agents running on each node. IDS agent has complex design but by analyzing it properly and closely it can be viewed as having six different modules.

In this type every single node plays an important and critical role. Each node contributes individually or on entire network for the process of detection. It scans for any sign of intruder. Using six different modules such as local data collection, local intrusion detection, cooperative message passing, secure communication etc. the above explained approach can be achieved. The IDS also triggers response if intrusion is detected. The isolated IDS agents are entirely linked together to form the IDS system defending the mobile wireless network.[2]

5. Proposed Work

Intrusion detection systems are burglar alarms of computer security field. Here other than alerting the host system on which IDS is installed, this system forwards information of detected intruders to other nodes in the network. The aim is to warn other nodes prior about the intruder so that they can take precaution.

5.1 System Design

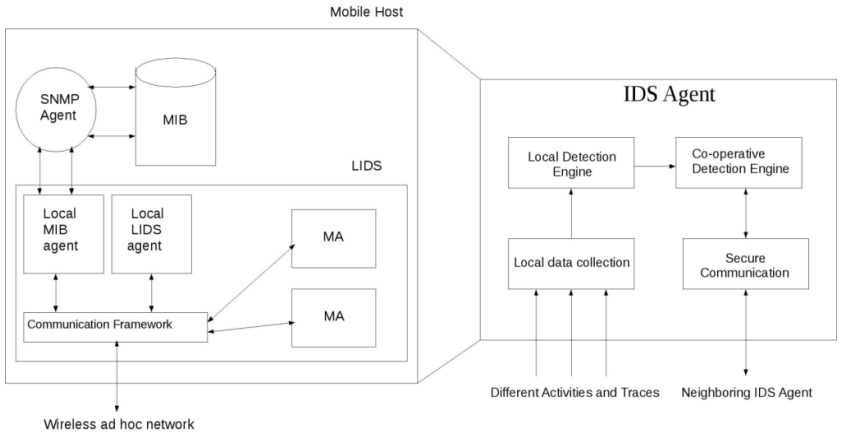

Fig.1 System Design

Fig.1 shows overall system design of Co-operative Multi-agent Based Wireless IDS Using MIBs. IDS agent is present on each system. Internal of this IDS agent can be shown as above diagram which has four modules in it.

- Local data collection module collects audit traces and activity logs.
- Local detection engine module uses information collected by local data collection module for detection of anomaly.
- Co-operative Detection Engine module alerts other nodes when any node detects intrusion locally.
- Secure communication module provides communication channel between two IDS agents.

IDS agent can be viewed as mobile host shown in the above diagram. This includes LIDS, SNMP agent, mobile agent and MIB. LIDS, mobile agent and MIB agent come under Local Detection engine, co-operative detection engine and Local data collection module respectively.

- MIB agents collect information from MIB variables.
- LIDS and mobile agents use information collected by MIB agents for their specific work.
- LIDS detects attack locally at that particular system and reacts to alerts by other IDS nodes.
- LIDS hands over the special task of transporting information about the intruder to other IDS, to mobile agents in that network.

5.1.1 SNMP

In complex network environment it is very difficult task to manage all the devices like routers, switches and servers. They should be up and perform optimally. SNMP helps to do this. It is application level protocol and set of rules that allows computer to get statistics from another computer across the network. This is a standard for managing Internet Protocol (IP) devices. Here a few manager stations control a set of agents. The manager station is a host that runs the SNMP client on it and agent, which is a managed station, is a router that runs the SNMP server program on it.

Computers keep track of information present in routers like information about packets, number of bytes and errors that are transmitted and received through each interface. All this information is kept in a database called MIB. For management tasks SNMP uses this MIB along with Structure of Management Information (SMI).

An agent has a list of objects that it is tracking. This list contains all the information that Network Management System (NMS) can use to determine health of the device on which this agent resides. These objects that agent tracks are managed in MIB defined above. The objects in MIB are categorized under 10 different groups as system, interface, address, translation, ip, icmp, tcp, udp, egp, transmission and snmp.The information from MIB variables can be read by using languages like JAVA.

5.1.2 MIB

The SMI provides a way to define managed objects and their behavior. An agent has in its possession a list of the objects that it tracks. One such object is the operational status of a router interface. This list collectively defines information that NMS can use to determine the overall health of the device on which the agent resides.

The MIB can be thought of as a database of managed objects that the agent tracks. Any sort of status or statistical information that can be accessed by the NMS is defined in a MIB. The SMI provides a way to define managed objects, while the MIB is the definition of the objects themselves. MIB creates a collection of named objects, there types, and their relationships to each other in an entity to be managed. MIB creates as set of objects defined for each entity similar to a database.

The various values that can be retrieved from a MIB are called MIB variables. These variables are defined in the MIB for a device. Each MIB variable is named by an Object Identifier (OID), which usually has a name in the form of numbers separated by periods ("."), like this: 1.3.6.1.xxxx.x.x.x.x... e.g. the MIB-II has a variable that indicates the number of interfaces (ports) in a router. It's called the "ifNumber", and its OID is 1.3.6.1.2.1.2.1.0. Network monitoring tools will query a device for the MIB variables and display the results. When a device receives a SNMP Get-Request for this ifNumber OID, it will respond with the count of interfaces.

- Querying MIB variable by Intermapper :

  There are two kinds of MIB variables: scalar values and table entries. Scalars have a single value, such as the interface number shown above. For example, the ifNumber MIB variable of a router is a single number that represents the total number of its interfaces. Table values, on the other hand, provide the same pieces of information for different items, such as the traffic for each of a router's ports, or information about each of the TCP connections in a device.

- Specifying and Accessing MIB variables :

  SNMP MIB variables are referenced by an OID, a sequence of digits and dots. This specifies the position of the variable in the MIB tree. Almost all the MIB variables you see commercially will start with 1.3.6.1 (iso.org.dod.internet) and will then either take the proprietary limb of the tree (.4.1: private.enterprise) the standard limb (2.1: mgmt.mib).

5.2 System Functions

Fig.2 gives the static implementation of the system. It shows how the various classes are related to each other using relationships like association and dependency.

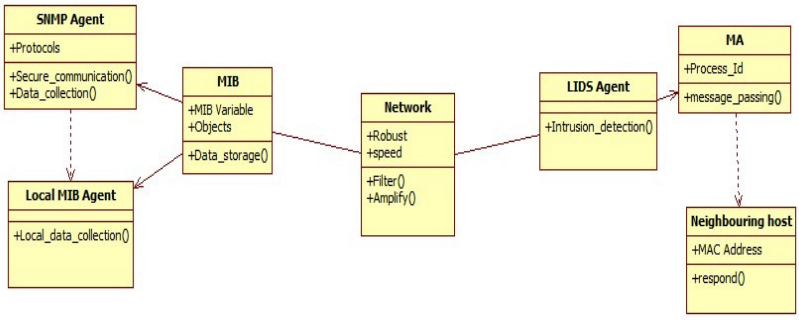

Fig. 2 UML Class Diagram

On larger scale system functions for this co-operative agent based WIDS can be divided into two main functions as intrusion detection and message passing to other nodes. Intrusion detection includes local data collection and local detection of intrusion as sub functions. Message passing contains secure communication channel and transfer of messages.

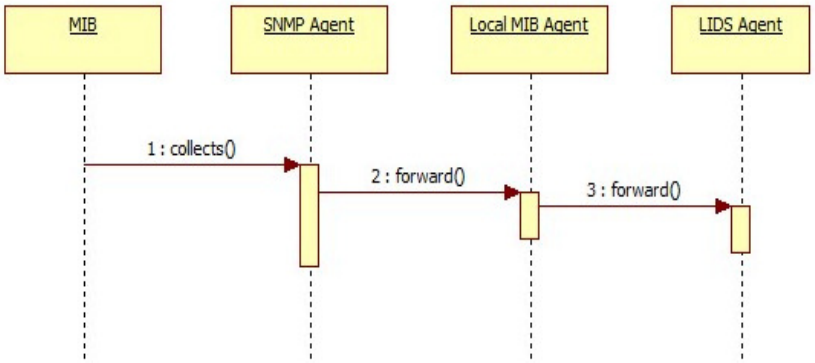

Fig. 3 UML Sequence Diagram

UML sequence diagram in fig.3 shows first main function of local intrusion detection. For this first data gets collected from MIB forwarded to local MIB agent and then to LIDS.

UML sequence diagram in fig.4 shows further main function of message passing to other neighboring nodes in the network. Responsibility of this transfer of message is given to MA. LIDS forwards message to MA which in turn passes it to other nodes.

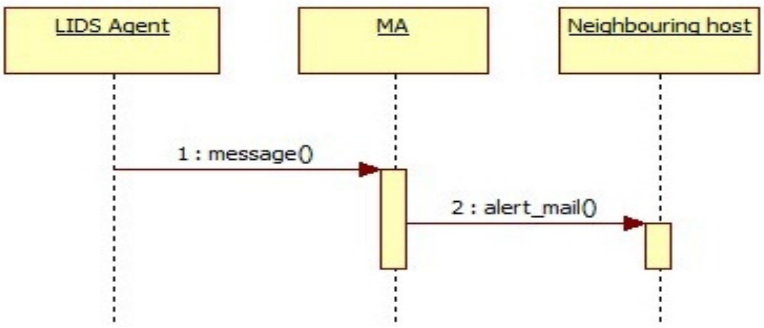

Fig. 4 UML Sequence Diagram

6. Experimentation and Results

Initial requirement will be the installation of SNMP on all the nodes present in ad-hoc network. SNMP agent will extract the information from MIB variables. MIB includes network related information. Thus approach is network based IDS. This information will be analyzed by LIDS agent using either Misuse Based Detection module or Anomaly Based Detection module.

If the intrusion is detected by LIDS, then it will generate alarm locally and then message will be passed to all the nodes present in ad-hoc network using mobile agent. Whenever any such type of message arrives at any node, then corresponding LIDS will generate alarm or will display warning message.

7. Conclusion

All networks are vulnerable to different attacks. Regardless of whether the network is wired or wireless, network security and integrity should always be preserved. As it said that wired IDS are not capable of taking care of things in wireless there is strong demand of effective IDS for wireless networks. Due to dynamic nature of wireless networks it is a challenging topic of research. We have shown that architecture for wireless IDS should be distributed and cooperative in nature. So, in the proposed system using information from MIB variables intrusion will get detected and mobile agents will alert other nodes by passing the message. It works in co-operative way.

We propose to use SNMP data located in MIBs, as an audit source for LIDS. Such a data source provides several advantages:

- It is independent from the operating system.
- It can be extended in order to collect and store additional data relative to network activities, operating system or applications.
- If an SNMP agent runs on a node, the cost of the collection of local information needs no additional resources.
- The standard representation of the data collected on each no de facilitates co-operation between LIDS.

References

[1] J Arokia Renjit and K. L. Shunmuganathan, "Distributed and cooperative multi-agent based intrusion detection system". Indian Journal of Science and Technology Vol.3 No.10 (Oct 2010) ISSN: 0974- 6846

[2] Krishnun Sansurooah, Edith Cowan University, “Intrusion Detection System (IDS) Techniques and Responses for Mobile Wireless Networks”.

[3] Abdulrahman Hijazi, Nidal Nasser, "Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks".

[4] Yongguang Zhang,Wenke Lee, Yi-An Huang, Intrusion Detection Techniques for Mobile Wireless Networks, Page Numbers (3-4), Year (2003).

[5] Fariba Haddadi,Dr. Mehdi A. Sarram, “Wireless Intrusion Detection System Using a Lightweight Agent".

[6] Allam Appa Rao, P.Srinivas, B. Chakravarthy, K.Marx, and P. Kiran, "A Java Based Network Intrusion Detection System (IDS)".

[7] Oleg Kachirski, Ratan Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks”

[8] R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai, “Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks".

[9] http://tools.ietf.org/html/rfc2248 Accessed 15th Nov. 2011

[10] http://lyberty.com/encyc/articles/snmp.html Accessed 30th Nov. 2011

[11] http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch01_04.htm Accessed 30th Nov. 2011

[12] http://tools.ietf.org/html/rfc1351 Accessed 17th Nov. 2011

[13] http://www.opennet.ru/base/cisco/monitor.txt.htm Accessed 30th Nov. 2011

Acknowledgment

We owe a great thanks to the people who helped and supported us while writing this survey paper. Our deepest thanks to **Prof. V. K. Khatavkar**, the guide of the project for guiding and correcting us with attention and care. He has taken efforts to go through the project work and make necessary correction as and when needed.

We would also thank our institute and faculty members without whom this would have been a distant reality.