Designing a Network Based Intrusion Detection System using MIB with the aid of SNMP Agents

Nisha A Rai
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangalore-575007

Pavan Kumar V
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangalore-575007

***Abstract*— In emerging technology of Internet, security issues are becoming more challenging. The Internet has become an important source for information, entertainment, and a major means of communication at home and at work. With connectivity to the Internet, however, comes certain security threat. Unauthorized access, modifiers, denial of service, or complete control of machines by malicious users are all examples of security threats encountered on the Internet. So, there is need for an approach which will efficiently detect intrusion in wired network. Efficiency can be achieved by implementing distributive, co-operative based IDS. The proposed system deals with network based intrusion detection were there will be one central computer called the manager node helping in the detection of intrusion. Intrusion detection takes place using anomaly based and signature based. If intrusion is detected, sender and other nodes will be alerted and thus it works in a co-operative way.**

***Keywords*— SNMP, threat, Unauthorised access**

I. INTRODUCTION

Security is one of the most important aspects in day today life. Since computer has become part of our life and number of users who use computers are increased it is very necessary to provide security in this field. Attack is an assault on system security that derives from an intelligent threat [1]. With increased number of the users, the network of computers is increased and it is vulnerable to number of attacks. Attacks can be mainly classified as Active attacks and Passive attacks. In an active attack, the attacker tries to bypass or break in to secured systems. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly-encrypted traffic, and turing authentification information such as passwords. [3]. Thus it is very necessary for protecting ones computer from unauthorities due to which data in a computer will be misused by the intruder or it may be corrupted.

The purpose of an Intrusion Detection System(IDS) is to constantly perform monitoring of the computer network and also possible in detecting any intrusions that have been penetrated and hence alerting the concerned person after the intrusion have been detected and recorded[2]. The proposed system deals on network based intrusion detection system based on the concept of simple network management protocol (SNMP) using Management Information Base (MIB) with the aid of SNMP agents in a co-operative way. SNMP monitors the network information which will be stored in the Management Information Base (MIB). Using this information intrusion will be detected and an alarm in form of message will be sent to concerned node and the neighbouring nodes.

II. RELATED WORK

Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking sources. Purvag Patel, Chet Langin, Feng Yu, and Shahram Rahimi proposed that network Intrusion Detection Math (ID Math) consisting of two components: (1) a way of specifying intrusion detection types in a manner which is more suitable for an analytical environment; and (2) a computational model which describes methodology for preparing intrusion detection data stepwise from network packets to data structures in a way which is appropriate for sophisticated analytical methods such as statistics, data mining, and computational intelligence[11]. Krishnun Sansurooah proposed a work on Intrusion Detection System techniques by detecting anomalies in the mobile ad-hoc network including inconsistencies in the routing tables and activities on other layers [3]. While in the proposed project it is detecting anomalies in network packets by using information from Management information table. Ashvini Vyavhare, Varsharani Bhosale, Mrunal Sawant, Fazila Girkar proposed an intrusion detection system where there is IDS agent in each system which detects the intrusion locally. This local IDS agent comprises of Local Intrusion Detection System (LIDS), Simple Network Management Protocol (SNMP) agent, mobile agent and Management Information Base (MIB) [1].

Eugene C. Ezin and Herv´e Akakpo Djihountry have proposed an intrusion detection system implemented in Java. This system has been tested by simulating three types of attack: land attack, flooding attack and death ping attack. It detected all three attacks correctly. The proposed network intrusion detection system is extensible and portable and much other functionality can be implemented [4]. However in the proposed system other type of attacks will also be implemented. Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita large number of network anomaly detection methods and systems [3]. J. Arokia Renjit1 and K. L. Shunmuganathan proposed an effective intrusion detection system in which local agent collects data from its own system

and it classifies anomaly behaviors using SVM classifier. Each local agent is capable of removing the host system from the network on successful detection of attacks. The mobile agent gathers information from the local agent before it allows the system to send data[5]. Where as in the proposed system information about data sent by the system is obtained by fetching it from the MIB. Using this information the intermediate node, where the intrusion detection takes place can determine the change in the traffic behavior and thus detect intrusion if any anomaly is observed.

Yongguang Zhang, Wenke Leeand Yi-An Huang together proposed a system to examine the vulnerabilities of wireless networks and argue to include intrusion detection in the security architecture for mobile computing environment [7]. Oleg Kachirski and Ratan Guha have proposed a distributed modular IDS system designed for ad hoc wireless networks.The architecture aimed to minimize the costs of network monitoring and maintaining a monolithic IDS system, also providing a degree of protection against the intruder [9].

R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai proposed, an anomaly detection system comprising of detection modules for detecting anomalies in each layer. The system works in a cooperative and distributive way; it considers the anomaly detection result from the neighbour node(s) and sends the current working node's result to its neighbour node(s) [10].

III. DESIGN METHODOLOGY

SNMP consists of three key components: managed devices, agents, and network-management systems (NMSs). A managed device is a node that has an SNMP agent and resides on a managed network. It may be routers and access servers, switches and bridges, hubs, computers, or printers. An SNMP manager, also known as an SNMP management system, is any computer that sends queries about network information to a managed computer consisting of an SNMP agent. An SNMP agent is any computer or other network device that monitors and responds to requests from SNMP managers

MIB (Management Information Base) is a collection of information organized hierarchically. When an SNMP manager requests information from an SNMP agent, the agent retrieves the current value of the requested information from the Management Information Base (MIB). The MIB defines the managed objects that an SNMP manager monitors (or sometimes configures) on an SNMP agent. Each system in a network (workstation, server, router, bridge, and so forth) maintains a database i.e MIB that reflects the status of the managed resources on that system. These resources may be the version of the software running on that particular device, the IP address assigned to a port or interface, total file size sent, timestamp of sent or relieved file, agent address etc. The MIB does not contain static information, instead it is an object-oriented and dynamic database which provides a logical collection of managed object definitions. The MIB defines the data type of each managed object and describes it. At the programmatic level, the definition of each MIB object that an SNMP agent manages includes the following elements:

- The object name and object identifier (also known as an OID).
- Agent ID or identifier address for SNMP agent.
- The object's data-type definition (such as counter, string, or address).
- The objects are assigned with index that are of complex data types. The index specifies the key field for the table —i.e., the field that can be used for the row identification (eg. Message id, sender id etc)
- The access level to the object (such as read or read/write) that is allowed.
- Restrictions for size.
- Timestamp i. e, sending time of file or message and the last modified time

Every MIB variable in SNMP is referenced with a unique object identifier, which identifies the location of a given managed object within the MIB namespace. In the proposed system, the system design will be as figure shown below

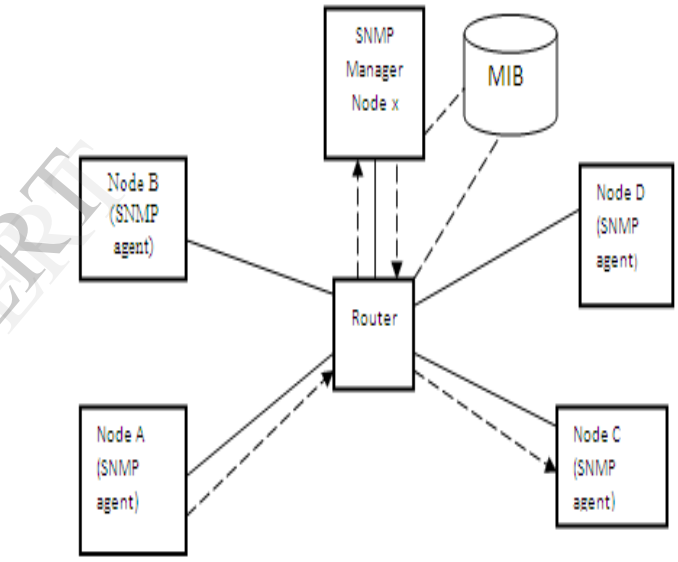

Fig 1.System Design

Wired connection
Packet flow

Node X is the manager device consisting SNMP manager.

Node A,B,C,D are managed devices consisting of SNMP agents .There is one centralized database called MIB consisting of all information about all the nodes managed by manager node x. Node A sends message to Node C which will be sent to through the router first to the Node X(denoted by dotted lines in Fig 1). Intrusion detection takes place in the node that contains SNMP manager (Node X) which uses the information from the MIB for traffic information. Intrusion can be detected at Node X using anomaly based detection or signature based detection .The type of intrusion detection is selected by the sender while sending data to the receiver. All these information will be stored in the MIB.

In case of anomaly based detection, timestamp (sending time of the data) and data size will be used creating

profile for the normal traffic. This can be considered as the Reference data. At the intermediate node (manager node x) this profile (reference data) is matched with the configuration data (i.e. data size and timestamp (last modified time) of the sent data at the manager node). If the normal traffic is disturbed or the reference data does not match with the configuration data then it means that data was intruded or modified. The reference data and configuration data are fetched from the MIB. Thus the data can be discarded if any malicious packet is arrived at node x (Manager Node) and alert will be sent to sender along with other neighboring nodes using mobile agent. When the sender receives the alert he can resend the data.

In the case of signature based intrusion detection, agentId is used as the signature which is unique for each node. This agentId is encrypted and is appended along with the data while the sender sends it to the receiver. At the manager node this signature is decrypted and will be checked and compared with the sender node agentid using MIB. If the signature is not present in the data then it means that data is modified or intruded. The data will be blocked as in anomaly based detection, and alert will be sent to resend the data.

IV. RESULT AND ANALYSIS

Intrusion detection system [1] consists of IDS agent in each system which detects the intrusion locally. This local IDS agent comprises of Local Intrusion Detection System (LIDS), Simple Network Management Protocol (SNMP) agent, mobile agent and Management Information Base (MIB). However this methods needs the contribution of each nodes for intrusion detection.

Signature detection [3] involves searching network traffic for a series of malicious bytes or packet sequences. The main advantage of this technique is that signatures are very easy to develop and understand. Limitations of these signature engines are that they only detect attacks whose signatures are previously stored in database; a signature must be created for every attack; and novel attacks cannot be detected

Network Anomaly detection methods [2] describes about one of the network anomaly detection methods.

All these types are combined and altered to have a better replacement of an Intrusion detection technique by overcoming the disadvantages where there a centralized intrusion detection system which detects intrusion before data is received and blocks the data if it is modified by intruder. Sender is given the option for selecting the type of security he needs by being more user-friendly. All Attack on data is detected prior to the receiver. Sender along with other neighboring nodes will be notified about the intrusion.

V. CONCLUSION

Since SNMP manages the traffic flow in a network it is expected to achieve security in a wired network with intrusion detection system using MIBs from SNMP with the aid of SNMP agents. With this centralized intrusion detection system the load on the receiver side can be minimized having intrusion detected beforehand

REFERENCES

[1] Ashvini Vyavhare, Varsharani Bhosale, Mrunal Sawant, Fazila Girkar ”Co-operative Wireless Intrusion Detection System Using MIBs From SNMP” International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[2] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita “Network Anomaly Detection :Methods, Systems and Tools” IEEE communications surveys & tutorials, vol. 16, no. 1, first quarter, 2014

[3] Krishnun Sansurooah, Edith Cowan University ”Intrusion Detection System (IDS) Techniques and Responses for Mobile Wireless networks ”published in the Proceedings of 5th Australian Information Security Management Conference, December 4th 2007

[4] Eug`ene C. Ezin , Herv´e Akakpo Djihountry, " Java-Based Intrusion Detection System in a Wired Network" International Journal of Computer Science and Information Security, Vol. 9, No. 11, November 2011

[5] 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

[6] Abdulrahman Hijazi, Nidal Nasser, "Using Mobile Agents for Intrusion Detection in Wireless AdHoc Networks".

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

[8] Fariba Haddadi, Dr. Mehdi A. Sarram, “Wireless Intrusion Detection System Using a LightweightAgent".

[9] Oleg Kachirski, Ratan Guha, “Effective Intrusion Detection Using Multiple Sensors in Wireless AdHoc Networks”

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

[11] Purvag Patel, Chet Langin, Feng Yu, and Shahram Rahimi “Network Intrusion Detection Types and Computation”2012

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

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