ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 4, October 2015

Distributed Intrusion Detection System Using Mobile Agent

Supriya Khobragade, Puja Padiya
Dept. of Computer Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, India

Abstract- The goal of Distributed Intrusion Detection System is to analyze events on the network and identify attacks. The increasing number of network security related incidents makes it necessary for organizations to actively protect their sensitive data with the installation of intrusion detection systems (IDS). There is a difficulty to find intrusion in an distributed network segment from inside as well as from outside network. Intrusion detection system studies very huge amount of data in a network. Intrusion detection system also check that load additional significant is not placed in the system and also not placed in network of monitoring. The Centralized intrusion detection system having certain drawbacks which later on comes with the idea of mobile agent. There is no central point of failure because there is no central station in an agent based Intrusion detection system. Agents can detect malicious activity. After finding malicious activity in a network, predefined actions were taken by agent against it. The system having superior performance than central sniffing Intrusion detection system. The system saves network resources while other distributed Intrusion detection system creates bottleneck in the system by activating too many sniffers in network. Usage of distributed model based on Mobile agent platform is one of the major motivation. This paper presents some architectural approaches of an Distributed Intrusion Detection System using Mobile Agent and survey of Distributed Intrusion Detection System using Mobile agents.

Index Terms- **Distributed Intrusion Detection System, Mobile Agent, Security.**

I. INTRODUCTION

In today's world, the network security is a big task so there is a increasing importance of network security which now a days shifting security concern to network itself and not to the host based network. Security services must be enlarge into network-based. Distributed approaches deals with heterogeneous open platform. Distributed approaches support scalable solution. Intrusion detection technology is the process of analyzing network activity that can lead to a adjustment of security policy.

Intrusion Detection System must evaluate and coordinate a large volume of data collected from different critical network access points. This task depends on an Intrusion Detection System to be able to characterize distributed patterns. The Intrusion Detection System architectures commonly used in commercial and research systems have a number of problems that limit their configurability, scalability or efficiency. The most common shortcoming in the existing architectures is that they are built around a single monolithic entity that does most of the data collection and processing.

In this paper, we review our architecture for a distributed Intrusion Detection System based on multiple independent entities working collectively. We call these entities Autonomous Agents. This approach solves some of the problems previously mentioned. We present the motivation and description of the approach, partial results obtained from an early prototype, a discussion of design and implementation issues, and directions for future work. Depending on the distributed architecture, the recommended approaches, implementing different Intrusion Detection System, accommodate the concepts of distributed agent and mobile computing. Agents are described as entities that analyze and take predefined actions against malicious activity. Using certain kind of algorithm we can find malicious activity on a private network. Agent shares the critical alert knowledge to the host to recognize the attack. It could be applied as software running on servers and host or as separate hardware devices segments. Mobile agent paradigm enlarge the agent by involving the concept of mobile computing. Mobile Agent Environment develops an proper execution environment for Mobile Agent that gives the basic services involving creation, transportation and execution.

The report is structured as follows: Literature survey is described in section II. The different architectures working and their approaches are discussed in section III. The analysis and the different architectural behaviors with their merits and demerits are discussed in section IV. The report is finally summarized in section V as the report's conclusion.

II. RELATED WORK

In this section, we will go through few papers related to Mobile agent based IDS.

In [1] proposed a framework in which Intrusion Detection Systems performs an important part in acquiring survivability of information system and protecting their safety from attacks. Centralized IDS is a single point of failure because it consumes a lot of network resources. So Mobile agent platforms is used to conquered deficiencies of centralized IDS, efficiently conduct the system and dynamically accommodate to network changes and event rules. Intrusion Detection System using Mobile agent shows superior performance than centralized IDS and is able to report intrusion instantly.

In this paper we provide general definition of Intrusion detection system architecture, requirements and limitations. We also present analysis of different IDS.

In [3] proposed a framework focus on one critical issue in security management that is intrusion detection. The concepts of intrusion detection introduced, overviews detection methodologies and approaches for IDSs. We study the technologies of agent and multi-agent system and present benefits of using it to address shortcoming of classical IDS. Although our research is still at the beginning, we aim to develop new intelligent generation of IDS, which are proactive and based on agent and multi-agent technologies.

In [4] proposed framework presents an implementation of a new MA-IDS (Mobile Agent based on Intrusion Detection System) model, established on misuse approach. Through its ease to detect simulated attacks, It shows that the use of mobile agents has practical advantages for intrusion detection. Based on a set of simulated intrusions, they established a comparative experimental study of four IDS, showing that most of current IDS are generally centralized and suffer from significant limitations when used in high-speed networks, especially when they face distributed attacks. This leads us to use distributed model using mobile agents paradigm. We believe that agent will help collecting efficient and useful information for IDS.

In this chapter, security issues of the system and previously applied techniques of intrusion detection and mobile agents are discussed with the merits and demerits. Next chapter introduces advanced techniques applied to secure data from attacks in intrusion detection that overcomes the drawbacks of the previously described methods, using mobile agent.

III. DISTRIBUTED INTRUSION DETECTION SYSTEM USING MOBILE AGENT

This section describes little architecture of IDS using mobile agent.

A. Architecture of Mobile Agent based IDS

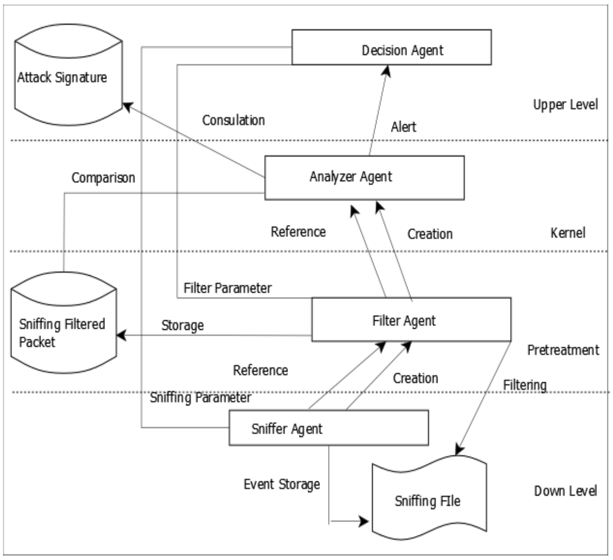

Fig. 1. Architecture of Mobile Agent Based IDS [4]

The Distributed structure of IDS having four levels which are down level, the Pretreatment, the Kernel level and the upper level as shown in figure 1. The levels contain four entities which having capacity to move from one station to another station. Those entities cooperate with each other, communicate with each other and also collaborative. That entities are discussed below.

1) ***The Sniffer agent:*** The sniffer agent grouped in a network. Sniffer agent is distributed all over network. The sniffer agent protects the network. It gathers all the events present in the host to which it is related. Agent stores the gathered data in a sniffing file. Sniffer agent is a moving agent which transfer from one location to the another. Agent replicates itself to lighten the network load. All the events in the network which are obtain in real time is gathered in down level. Sniffers are what is commonly called sensor.

2) ***The Filter Agent:*** Filter agent takes data from sniffing files having modified data which is detected and analyzed by the sniffer agent. All the data is filtered by the Filter agent and collected data passed to the pre-treatment phase. Every level in the architecture requires observation. Filter agent combine all the data which is collected from the sniffer agent. The filter agent will treat these crude events by achieving the following task:

a. Distinguish the various fields of the events collected in crude such as destination address and the protocol.

b. Sort the events by the category of packet (TCP, IP) concerned by a specific kind of intrusion.

3) ***The Analyzer Agent:*** Analyzer agent take action on the data which is carried out by filter agent. All the captured data from sniffer agent and filter agent is analyzed by analyzer agent. If Filtered packets are alike with attack signature then the agent gives alert to the Decision agent.

4) ***The Decision Agent:*** All the data in the network are processed in analyzer agent and then decision agent take decision if alert is generated in analyzer agent.

B. New Generation IDS

Our concept is to create an intrusion detection system that in some aspects mimics what happens in a real war. Instead of remaining on defensive and waiting for the enemies, it is more interesting to go on the offensive, as the saying goes: who stays in the defensive does not make war, he endures it.

Our intrusion detection system will be built on this general philosophy. The objective is to develop new generation of IDS that are more intelligent, more autonomous and proactive. So, the idea is collecting information about attackers and this allows anticipating and predicting intrusions before they occur.

This approach consists of using intelligent and mobile agents, able to communicate and adapt to the current environment and attackers behavior. Also, we envisage using the honeypot to attract and lure attackers while observing their behavior and save their attack methods in order to study, understand and anticipate them. We will benefit from the honeypots installed in network of our partners/collaborators. These honeypots are involved in monitoring the activities of attackers through the collection of their traces. Therefore we have the maximum information about attacker's behavior and so, we can protect ourselves beforehand.

1) ***Architecture of New Generation IDS:*** New generation IDS is more Intelligent, more Autonomous and Proactive which collects information about attackers using Honeypot technique and Anticipating and predicting intrusions before they occur in a network. It uses Intelligent and Mobile agent that adapt changes automatically.

2) ***Honeypot:*** Honeypot is defined as a computer system connected to a network, deliberately vulnerable for the purpose of luring attackers and studying their behavior. It is a great environment to observe malicious traffic. The use of a honeypot has the following objectives:

- Monitoring
- Capturing data
- Analyzing data captured

3) ***Advantages of New Generation IDS:*** The advantages of new generation IDS are as follows:

1. *Load-balance*- Mobile agents can spread the workload of the IDS over a number of machines.
2. *Reduce Network Load*- All the agent work together in a network and distribute the network load. So it reduces the work load of network by transferring data from one agent to another agent.
3. *Dynamic Adaptation*- As a result of dynamic behavior of the mobile agents and their ability to react to changes, the system can be reconfigured at run-time.
4. *Flexibility and Fault-tolerance*- Agents can operate independently of each other. So individual piece can be removed, modified and improved while the system continues to function. Also that implies the system can continue to work even when one agent is destroyed in an attack. This makes the IDS fault tolerant.
5. *Scalability*- Increase in the network load can be managed by the agent.

C. Autonomous Agents for Distributed Intrusion Detection System [AAFDID]

Implementation of the architecture is used to overcome the disadvantage of centralized system. It implements host based hierarchical design. The system consists of three layers. Each layer calls methods of the layer below.

At the Base level, agents gather all information about the data. Agent looks for suspicious packets in the network. Agent passes gathered data to transceiver in the upper layer. Transceivers are like agent manager. Transceiver control agents on the host and arrange it. Transceivers channel information. Transceiver takes only useful data from gathered data and forward it to monitor.

At the uppermost level, each monitor gathers data from one or more transceivers. Then it compares their inputs. Every host has one transceiver. Monitor gathers data from various hosts.

Monitors can be arrange hierarchically in which root monitor present at the top most level providing user interface that controls the IDS. Delivery of audit information is carried out for the intercommunication of agents in a network through the audit router which carries database of current agent and their interests. In this architecture, agents are used to gather data. Also agents are used to pre-process information which plays an important role in detecting intrusions in the system.

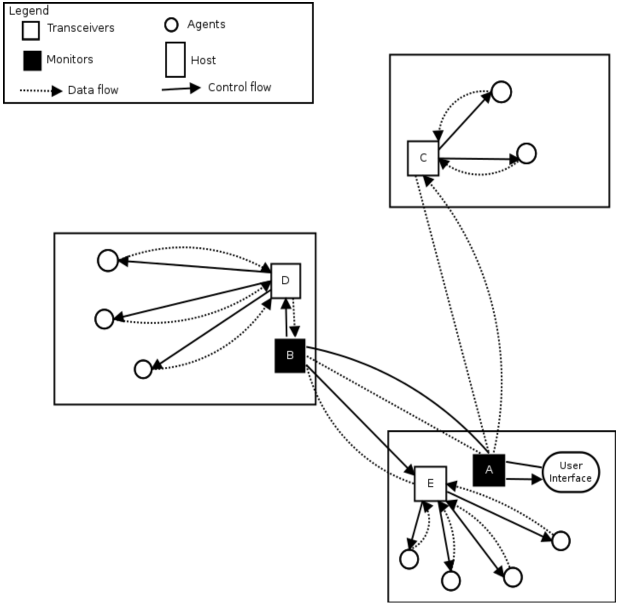

Fig. 2. AAFDID System [1]

Transceiver and Monitor make the system scalable. The biggest problem occurs in this architecture is the delay in the detection of the intrusion caused by the layers between agents and the monitor. Monitors are the single point of failure.

D. Intrusion Detection Agent System [IDA]

IDA is an implementation of the mobile agent approach in intrusion detection. By the analysis of the system designer, attackers obtain unprivileged access to remote machines using some common steps as discussed below:

Scanning of machines and ports done in first step then attacker try to use vulnerability of common services in second step. Actual access to the system obtain in mark stage. Finally after mark stage attacker tries to hide their actions by erasing logs.

The task of IDA is to find intrusions which are left after the scanning of system by the intruder in mark stage. The MLSI, which stands for Mark Left by Suspected. IDA has very simple structure that includes central manager present on every network segment that collects information from sensors and then analyze it. IDA has sensors that monitor network traffic according to MLSIs. There are multiple kind of agents in the network.

The task of Information Gathering Agent (IDA) is to analyze logs throughout. Tracing Agent traces the source of the attack. It works in coordination with IDA. The disadvantage of IDA is centralized management. As the manager can deal with only a certain number of sensors and agents in a network, the problem of scalability occurs.

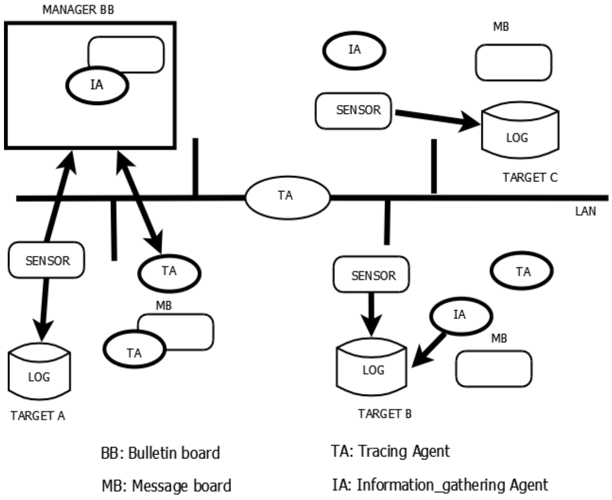

Fig. 3. Structure of IDA [1]

E. Intelligent Mobile Agents for Intrusion Detection System [IMA-IDS]

Intelligent Mobile Agents for Intrusion Detection System:

The architecture of IMA-IDS is defined in terms of four agents.

Collector agent: Agent collects all the data together, duplicate the data and spread all over the network.

Correlator agent: It collects critical information and sends it to the appropriate analyzer agent without passing through the manager agent. Each correlator agent uses a set of rules that clearly specifies the crucial events, contexts and analyzer agents concerned by an urgent reporting event mechanism.

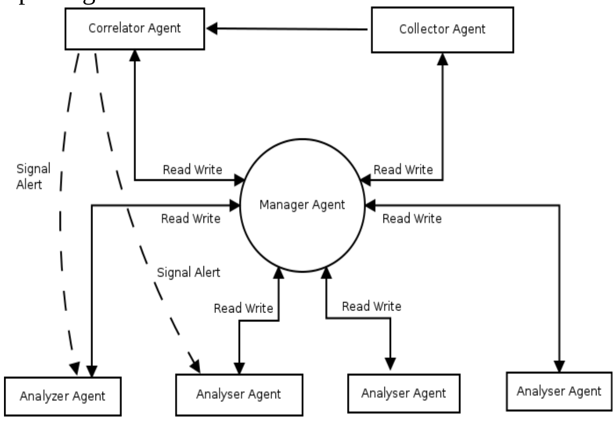

Fig. 4. IMA-IDS Architecture [1]

Analyzer agent: It performs several kind of analysis such as classical signature detection, anomaly detection and a new security protocol analysis based on abstract interpretation.

Manager agent: This agent manages the gathered information and forward it to analyzer agent.

All the collector agents report their results to the manager agent, which transmits them to the analyzer agents. The analyzer agent performs a higher-level analysis and correlation (Anomaly and Policy detection). The analyzer agents report their results to the manager, and they generate alarms if they detect any anomaly.

In order to communicate, agents are able to know all information about the other agents created and running in the network (their locations, their number, and their identifier) by sending a request to the manager agent. The manager agent uses the following two agents:

Registry Agent: being present on all hosts running agents, it maintains information about the agents running in the host.

IDS-Host Agent: it keeps track of all created and running agents. For communication agents subscribe to one or more multicast message list and implement handlers for communication messages.

F. Micael

Micael is agent based approach. In this architecture decision making, distributed, autonomous agents plays very important part in finding intrusions. Micael architecture consists of the following elements.

Sentinels are static agent. All the hosts in the network carries sentinel. Sentinels are unaware about different attacks. They are against distributed attacks (DoS etc.)

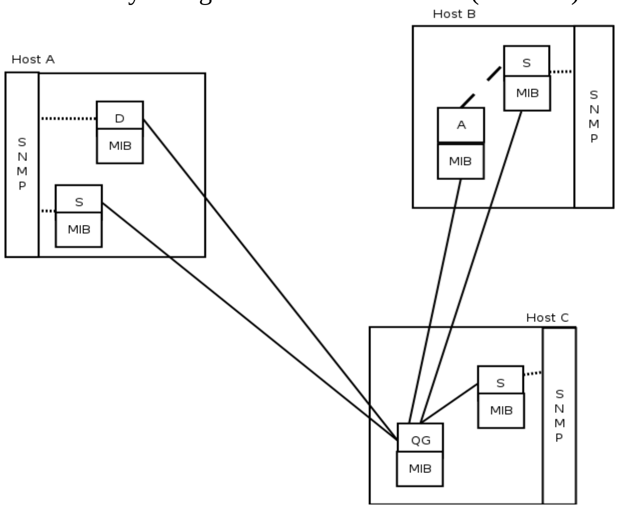

Fig. 5. Micael System [1]

Detachments are mobile agent. It plays a part in finding intrusion. While travelling in a network if agent finds any attack then it goes to the corresponding host in the network and starts to analyze all the log files. If possibility of that attack is confirmed then it takes action for preserving information.

Headquarters are centralized agent. It gathers information from sentinels. It create a new detachment if there is a need to create it. In an example scenario, the intrusion is detected as it follows.

First sentinels look into data for a suspicious activity. If they find any activity then they request for a detachment from the headquarters. The detachment is created by headquarters and sent to the host. After reaching to the host, detachment analyzes information more in detail. Any attack is detected then it takes action. After that information is forward to headquarter.

Micael is a successful implementation of the agent based approach with several advantages. Agents are not only used to collect data but they can also react to the incidents. In addition the whole system is written in Java. So it is very portable. It can run on any platform supporting Java.

G. Intelligent Agents for Distributed Intrusion Detection System [IA-DIDS]

The Specialized Local Agent performs several kinds of attack analysis such as signature detection, anomaly detection and performed global analysis, for detecting distributed attacks. Suspicious network activities are captured by Snort sensor and log files are generated.

Filter Agent is agent responsible for filtering specialized security events from the log files based on event rules. Intrusion Event Rule is a set of requirements that will trigger an alert. The Analyzer Agent checks for the event in the database and analyze it. Interpreter agent select some local events which Analyzer Agent also look for. These patterns are retrieved from Events DB. Analyzer Agent has the pattern-matching task to confirm the occurrence of the given events in Event DB. Then, it reports a search results to the Interpreter Agent using its Specialized Local Agent.

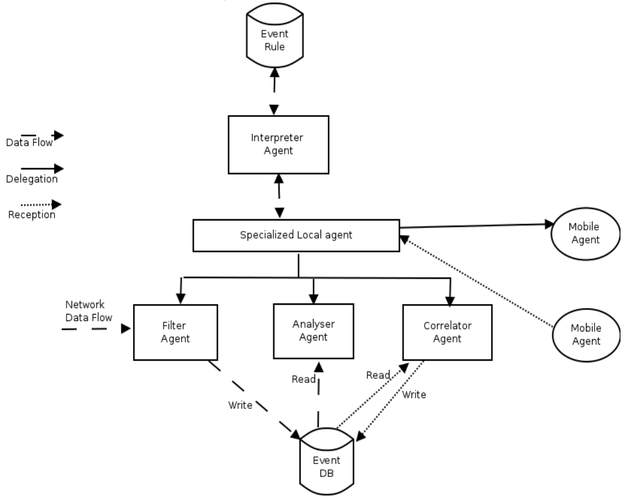

Fig. 6. Multi-Agents Architecture [1]

H. Preemptive DIDS

Preemptive DIDS is a network-based system. In Preemptive DIDS, all the agents are strategically placed around a network. Packets are diverted to various types of agents. If agent detects any intrusion in a network then the detected packets are blocked before they reach to their destination. The policy mechanism verdicts for blockage. The Gateway Agent, The Controller Agent, The Detection Agent, The Policy Agent, and The Home Agent are the five types of agents in this architecture. A Gateway agent is a bridge between the internal network and the external network. It is responsible for capturing packets from the external network. After capturing data, it forward data to one of the controller agents in the internal network for the intrusion detection.

On the below description about the packets, Agent will decide to forward packets to which Controller agent

(1) The workload of the host computer, where the controller agent resides.

(2) The session, which the packet belongs to.

(3) The cluster, which the controller agent is involved.

A controller agent locate in the internal network of a computer. It receives packets either from the home agents (outgoing/ internal traffic) or the gateway agents (incoming traffic). It forward the obtained packets to the Detection agent for the intrusion detection. A Detection agent is responsible for the actual intrusion detection job. Each controller agent controls a number of detection agents. Agent gets updated whenever new intrusion occur or invented. The detection agent gets the packet from the controller agent. The detection agent also obtain the data from the leader controller agents in the cluster. After finding intrusion in a packet it generates alarm. A home agent receives packets from controller agent. If controller agent need packets then the home agent send data to the controller agent. If any intrusion occurs in a packet, then it gets help from policy agent to take action on them.

A policy agent is an agent responsible for what action a home agent or a gateway agent should take when an dropping the packet, letting the packet pass through but informing the SSO, or just logging the event down without informing the SSO, etc. Long time ago, Preemptive IDS has blame that it only report about the intrusion and not stop intrusion whenever occur in a network. But now if any intrusion occurs in a network, and policy agent gives decision for blockage then that suspected packets can be removed from the process before reaching to the destination host.

In this chapter, the mobile agent based intrusion detection system describes various architectural approach, their working using mobile agent and their merits and demerits. The main purpose of the mobile agent based IDS is to detect intrusion in system and provide security to the information with the help of mobile agents.

IV. COMPARATIVE ANALYSIS

We have discussed little architecture of Mobile Agent Based IDS in the previous chapter. Methods in table 4.1

shows differences due to different architecture and their working strategies to complete the task and to secure information, which is provided to the network or networks. Each technique uses different approaches for data security and for intrusion detection. Each technique consists of their advantages and drawbacks as well.

All the demerits of the Centralized IDS network that is, consume lot of network resource are overcome in the architectures discussed above and the new intelligent technologies where invented which is a big help in intrusion detection for securing the data through the use of mobile agent in the IDS. The comparison below shows all the architectural approaches and their respective features.

Architecture	Approach	Advantages	Disadvantages
Autonomous Agents For Intrusion Detection (AAFID)	Host based Mobile agent approach	• Collected and Pre-processed information used to detect intrusions in the system. • Make the system scalable which permits detection of distributed attacks.	• Delay in the detection of the intrusion caused by the layers between agents and the monitor. • Monitors are the single point of failure.
Intrusion Detection Agent System (IDA).	Mobile agent approach.	• Detect intrusions by scanning marks left by the intruder. • Simple structure.	• Limited Scalability • Centralized data collection.
Intelligent Mobile Agents for Intrusion Detection System (IMA-IDS).	Host Based Mobile agent approach.	• All the collector agents report their results to the manager agent. • Generate alarms if they detect any anomaly.	Centralized data collection.
Micael.	Mobile Agent approach.	• Agents are not used only collect data. • Agents can also react to incidents. • It is very portable.	Run on any platform supporting JAVA only.
Intelligent Agents for Distributed Intrusion Detection System (IA-DIDS).	Host based and Network based Mobile agent approach.	The agent can be executed autonomously over a set of network hosts.	No
Preemptive DIDS.	Network based Mobile agent approach.	If an intrusion is found and the agent verdicts for blockage, those suspected packets can be discarded before reaching the process in the destination host.	No

Among all above discussed architectures, Preemptive distributed intrusion detection system is the good architecture for detecting the intrusion while transferring data in a network because when agent detects intrusion in a network it blocks the packets or data and remove it from the network.

V. CONCLUSION

Distributed Intrusion Detection Systems (IDS) having very important role in obtaining survivability of information system. Also it preserves their safety from attacks. This system overcomes the drawbacks of centralized IDS as it requires a lots of network resources. Single point of failure occur in Centralized IDS. Distributed IDS efficiently manage the system. It dynamically adapt to network changes and event rules. Distributed IDS using mobile agent shows superior performance than centralized IDS. Distributed IDS is able to report intrusion instantly.

In this paper, we focus on one critical issue in security management that is intrusion detection. We introduced concepts of intrusion detection and we overview detection methodologies and approaches for IDS. Also limitations of classical IDS are illustrated. Although our research is still at the beginning, we aim to develop new intelligent generation of IDS.

REFERENCES

[1] Patil, Nita, et al. "Analysis of distributed intrusion detection systems using mobile agents." Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on. IEEE, 2008.

[2] Eid, Mohamad. "A new mobile agent-based Intrusion detection system using distributed sensors." proceeding of FEASC (2004).

[3] Benmoussa, Hajar, et al. "Towards a new intelligent generation of intrusion detection system." Security Days (JNS4), Proceedings of the 4th Edition of National. IEEE, 2014.

[4] Barika, F. A., N. El Kadhi, and K. Ghedira. "MA-IDS: Mobile agents for intrusion detection system." Advance Computing Conference, 2009. IACC 2009. IEEE International. IEEE, 2009.

[5] Djemaa, B., and K. Okba. "Intrusion detection system: Hybrid approach based mobile agent." Education and e-Learning Innovations (ICEELI), 2012 International Conference on. IEEE, 2012.

[6] Albag, Hakan. "Network and Agent Based Intrusion

Detection Systems." TU Munich Dep. of Computer Science, Istanbul Technical. University (2001).

[7] Balasubramaniyan, Jai Sundar, et al. architecture for intrusion detection using autonomous agents." Computer Security Applications Conference, 1998. Proceedings. 14th Annual. IEEE, 1998.

[8] Chaware, Sandeep. "Banking security using honeypot." Int J Netw Secur Appl 5.1(2011): 31-38.

[9] Jansen, Wayne A. "Intrusion detection with mobile agents." Computer Communications 25.15 (2002): 1392-1401.

[10] T. Djotio Ndi, C. Tangha and G. Bertrand Fopak. "MAMNID: A Load Balance Network Diagnosis Model Based on Mobile Agents," Journal of Information Security, Vol.3 No.4, 2012, pp.281-294.

[11] El Mourabit, Y. O. U. S. E. F., Ahmed Toumanari, And Hicham Zougagh. "A Mobile Agent Approach for IDS in Mobile Ad Hoc Network." International Journal of Computer Science Issues (IJCSI) 11.1 (2014).

AUTHOR BIOGRAPHY

Supriya Khobragade M.E IInd year (Computer Engineering) student of R.A.I.T College of Engg. Nerul, Navi Mumbai.