Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Literature Review on Agent Based Intrusion Detection System

Abhijit Dwivedi* Department of CSE REC, Bhopal (M.P), India

Y. K. Rana Department of CSE REC, Bhopal (M.P), India

B. P. Patel Department of CSE REC, Bhopal (M.P), India

Abstract*—Attacks or intrusions must be blocked or stopped at their entry points before they spread. The intrusion detection system plays a crucial role to enforce the policies for pattern matching decided for the network. A Mobile agent (MA) is a concern to of a computer software and information which is capable to move around one system to another separately and carry on its execution on the target system. Mobile agent based intrusion detection system is a proficient way to the intrusion detection in the dispersed environment. This paper contains a review of the intrusion detection system based on mobile agent. It includes the performance increased that happen through mobile agent on intrusion detection system and analysis the presented mobile agent based intrusion detection system focusing on every of the categories of the categorization techniques used and the shortcomings of the present IDS design and implementations.

Keywords— Decryption, Encryption, Internet, Intrusion detection,Network security.

I. INTRODUCTION

Computer security is the process of detection and prevention of unauthorized access of computer system. Prevention measures help to avoidthose users whose authenticity is suspected and not justified, and they are treated as “Intruders”. Such users are being stopped by accessing entire part of computer system. Detection helps us to determine whether someone had made attempt to unauthorized access of system or not, if they got success, then what they may have done [1]. It uses computer for everything, from banking to shopping and communicating with others through chat programs or email [2]. It probably do not want strangers to read email, to use computer to attack or intrude other systems, to send forged messages or email from one’s computer, or examining personal information stored on one’s computer (such as financial statements). Intruders (also known as attackers) may not care about one’s identity [3]. Often they want to gain control over accessing rights of computer so that they try to use for launching attacks on other systems. If intruders own the control over one’s computer gives, it enables ability to hide their actual location as they introduce theintrusion , often against very high-profile computer systems like government or financial systems [4]. For instance, even if a computer is connected viaInternet only for playing games or sending emails, that computer may be taken as a target. Intruders having possibility to watch all actions performed inside the computer, or cause damage to one’s computer by changing their data or by crashing their system [5]. Unfortunately, intruders always discovers new vulnerabilities (functionally called as "holes") to exploit computer or system software. When loop holes (backdoors) are obtained, computer vendors generally find patches to represent the obtained problems. Although, it`s up to the user, to obtain and install file patches, perform the configuration of the software for operating in more secure manner [6-7]. Also, there are such software applications which have predefined usual settings that allow accessing rights to other users for accessing computer unless it changes the settings to be more secure. For examples, including chat programs that let outsiders to execute commands on one’s computer which provides facility to enable someone to introduce destructive programs that run when clicked by user.It probably wouldn't let a stranger to look through important documents [1,2,4,21]. In the same way, it may want to keep the tasks confidential to perform on computer, whether it is tracking our documents or performing other applications. Also users should have some assurance that the information entered into computer remains intact and is available when it is required. With the possibility of intentional misuse of our computer by intruders via the Internet there could be generated security policy voilation [8]. There are some more risks which could befaced even if users weren't connected to the Internet like hard disk failures, theft, power outages, etc. The bad news caused by this problem is that it possibly unable to plan for all possible risks. The good news is also exist here is that it can take some usualsteps to reduce the chance to be affected by the most common threats.Some of those steps help to face with both the intentional and accidental risks. Before we get to know what we can do to protect our computer or home network, let us take a descriptive glance at some of these associated risks with security. Here some very common methods given which are used by intruders to gain control of computers also briefly described below [9-11].

Trojan horse
Back door
Denial of service
Being an intermediate for other attack
Unprotected Windows sharing
Roaming code (ActiveX and JavaScript)
Spoofing

Email-borne viruses
Chat clients
Packet sniffing

Coordinating attack: It is a well-organized and can be executed offensively by which the differentelements of a command are entered where their powers can be utilized for achieving the greatest advantages.

A. Intrusion Detection System (IDS)

IDS Detects malicious activity in computer systems and Conducts forensic analysis once attack is over.Monitors network resources to detect intrusions and attacks that were not stopped by preventative techniques (firewalls, packet-filtering routers, proxy servers) [10].Expands available options to manage risk from threats and vulnerabilities. Fig. 1 is showing the conventional architecture of an IDS.

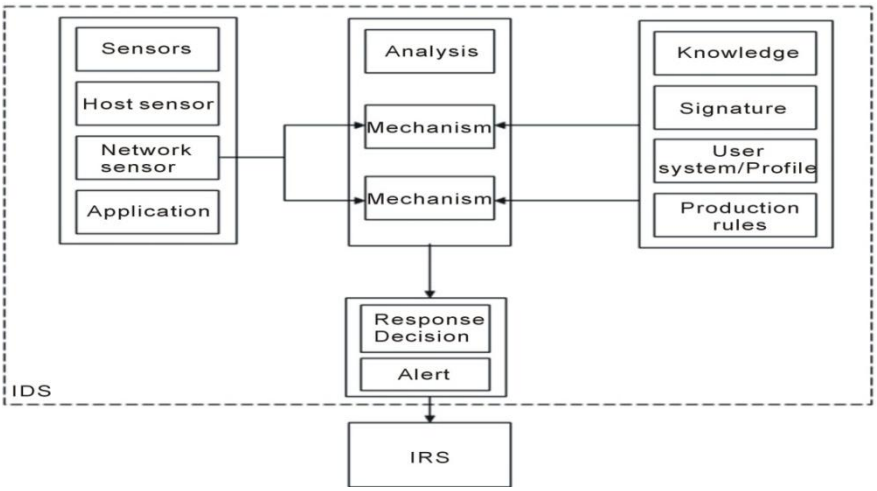

Fig. 1 Conventional IDS architecture

Types of IDS-there are various types of IDS which is following:

1) *Network Intrusion Detection Systems (NIDS):*NIDS is a type of system that usually consists of a network sensor with a Network Interface Card (NIC) which is used to inspect all incoming and outgoing network traffic and identifies suspicious activities which attempt to break the security of the system.The IDS is placed along the boundary of a network segment that monitors all network traffic on that segment [9-10].
NIDS Architecture: NIDS architecture (Fig. 2) has following strength.
Ownership cost: It is lower because IDS is shared.
Packet Analysis: Can look at all network traffic.
Evidence Removal: Packets are captured in a separate machine.
Real-Time Detection and Response: Can detect (and block) DDoS attacks.
Operating System Independence.

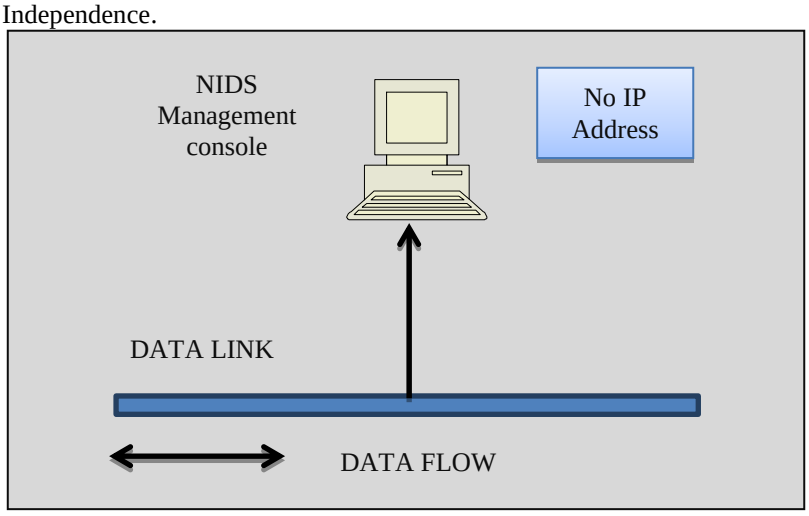

Fig. 2 NIDS architecture

2) *Host Intrusion Detection Systems (HIDS):* A HIDS is an software applications (agents) installed on a computer system which is to be monitored and analyzed for the network packets on its networking interface. An agent monitors the operating system and maintains data within log files also alert by triggering alarms. A HIDS is designed for only monitor the individual workstations which are equipped with an agent. It is unable to monitor the entire network [12-13]. Therefore HIDS systems are used for monitoring any attempts of attack occurred on critical servers. HIDS has following strength.

Verifies success or failure of attack by reviewing HIDS log entries.
It looks after use and specific activities of system; used for forensic analysis.
Monitor network encrypted traffic.
Near real-time detection and response.
Log based analysis, having good design mitigates much of the delay.
Focus on key system components.

3) *Active/passive IDS:* IDS can also categorized by active IDS and passive IDS, where usually used and known Intrusion Detection and Prevention System (IDPS) is active Intrusion Detection Systems. It is designed such that it automatically blocks suspected attacks without any interference by an operator. In response to an attack IDPS has the advantage of providing real-time correction action. A passive IDS is a system that is configured to only monitor and analyze activities of network traffic and to generate alert for an operator to potential findings of attacks. Therefore passive IDS cannot perform any protection or correction functions on its own [5, 14].
4) *Signature Based IDS:*A knowledge-based (or Signature-based) IDS references a database of previous profile or signature of attacks and known system vulnerabilities. Here `Signature` means "the recorded evidences of intrusions". Always intrusions leave their behavior sign as a fingerprint behind in terms of:
Data packet's nature
To run an application, number of failed attempts
Failed logins
File access

The above fingerprints are called signatures. These are used for identification and prevention from the same attacks which possibly occur in the future. On the basis of these signatures Knowledge-based IDS identify attempts of intrusion. The demerits of Signature-based Intrusion Detection Systems (IDS) are that:
Signature database must be regularly updated and maintained.
New or unique attack may not be detected [13,15].

5) *Anomaly Based IDS:* a Behavior-based (or Anomaly-based) ID references a learned pattern of normal system activities to identify any attempt for active intrusion. The inferences from these patterns become a reason for triggering of an alarm [13, 15]. The demerits of Anomaly Based IDS are that:
Higher false alarm rate
Usage pattern are not static(i.e. they often change) to implement Anomaly based IDS.

B. IDS Terminologies

The security terms which are related to intrusion detection and prevention techniques:

1) *Vulnerability:*Vulnerability is considered as a weakness that allows an attacker to reduce the security of a particular system in a network. It is also considered as an "attack surface".
2) *Exploit:*An exploit is a piece of software or mechanism which takes advantage of bug or vulnerabilities that exist in the system in order to cause unintended behavior of the system. For example, if poor passwords are used in network for authentication then a password-cracking might be the exploit on such vulnerability [12].
3) *Signature:*A signature is a pattern sets which are used by IDS to identify an unwanted packet. A signature is usually created to watch network traffic for a particular attack or vulnerability [13].
4) *Alarm:* An alarm is considered as a signal generated by IDS in response of occurrence of an attack.
5) *Detection rate:* Detection rate refers as number of alarms generated after intrusion detection to the total number of attacks occurred.
6) *False Alarms*:These are events of IDS. There are two types of false alarms i.e. false positive and false negative [13].
7) *False Positive:*A false positive is an attack alarm that is triggered incorrectly (means traffic that does not constitute an actual attack).
8) *False Negative*:A false negative is a term which means no alarm is triggered if any attack occurs. This is one of the worst type of false alarm [15].
9) *True Alarms*:There are two types of true alarms triggered in IDS i.e. true positive and true negative [12].
10) *True Positive:*A true positive is a type of alarm that is triggered when the IDS device had recognized and responded to an attack [13].
11) *True Negative:*This means that attack had occurred but IDS had not triggered an alarm [13].

C. Incidental and Accidental Intrusion

No IDS is perfect and unerring. Each network is different. Traffic that is deemed harmful on a network may be regarded perfectly normal on another network. Therefore, no matter which technique the IDS uses, it is the task of the administrator to configure and tune the system so that it serves its purpose for that network [16]. Only with active maintenance can the number of false positives and false negatives be brought to an acceptable level. Any brand new IDS deployed on a network is bound to have a tuning period that could amount to several weeks. During that time it is the administrator's task to tune the system, modify the default settings, and disable irrelevant fingerprints, and so on [17]. Moreover, since new vulnerabilities are discovered almost daily, the administrators are required to stay vigilant, for example, by monitoring various mail groups and security Web sites. One of the useful skills a network security administrator is bound to need is the ability to analyze traffic recordings in hexadecimal notation (packet dumps). True, the IDSs, and packet sniffers can in most cases identify and interpret a packet correctly, but they are not infallible [17]. A

suitably crafted or otherwise malformed packet may not be correctly decoded by the IDS, or the sniffer. In that kind of situation a skilled network security analyst can step in and check from the hexadecimal dumps what is at fault [16]. The human factor comes into play also when analyzing and correlating log data from various sources such as firewalls, sensors and syslog. It is crucial to be able to determine whether the analyzed traffic is stimulus or response in order not to draw wrong and hasty conclusions. At first glance, for example, it might seem that a number of hosts from your network are initiating connections to some external network [7]. But what if someone has actually send traffic to your machines with a spoofed source IP address, and in fact, our machines are just sending responses to that spoofed source? In that case traffic that at first could have been categorized as stimulus, in fact, turns out to be responsive traffic. The main asset an administrator has in this type of cases is experience [3,8 and 18].

This paper presents review on Agent Based [1-19] IDS for detecting attack using agent based detection technique and protocol acknowledgment for intrusion detection system. The rest of the paper is structured as follows. Section II discuses mobile agent based IDS. Section III discuss the related work on Intrusion detection system, Section IV presents about open source IDS tools "SNORT". Section V presents the risk analysis during intrusion detection. Section VI conclude and discuss the future directions of this work.

D. Mobile Agent Based IDS

In order to improve the efficiency and effectiveness of the system, mobile agents [4-7, 14-19] are used, which not directly improves the detection techniques, to reshape the way detection techniques are applied. Having agents which visit database and extracts results is an ideal way to transfer the computation to the data [7]. Having mobile agent is a sustaining approach which focuses on specific type of vulnerability, such as coordinating attacks that occur from multiple sources over long periods of time. Another area of concern is to minimize the ability of an attacker to provoke IDS through differences between the IDS protocol stack of target and the protocol model. All these comes true due to capability of agents replication to themselves and resident also over more than one platforms [8, 9, 18, 20]. To reduce the potential for dropping packets, while maximizing the potential for generating a quick response towards a detected intrusion or attack it is required to migrate out from network-based IDS to multiple host-based detection agents functioning simultaneously also. The presence of resident components at the host provides clear text visualization for the IDS. During these situations host adopts network level encryption by the use of Internet Protocol Security (IPsec) [20]. Hence MAs are capable for facilitating the implementation of robust attack, resistant IDS architectures also. MAs are capable of moving from one location to another after sensing danger or suspicious activity [9]. The greatest potential for mobile agents that resides in the contrast of response to an intrusion rather than its detection. By which they can start their execution over entire network anywhere. Mas are capable of handling attacks in a more optimal way than conventional IDS. Mobile agents enhance an IDS's ability of tracking an attacker by the attacked network, for responding to target, source, and for collecting all the evidences related with the attack from the host and network components. It also separates the source and target [8]. There are elements to describe some pros of applying mobile agents for responding to an intrusion: ·

1) *Tracking an Attacker*: Before attacking a system, attackers often enters into the chain of many hosts also may apply their source address spoofing. For searching the attacker, the IDS must trace back along the chain and locate the actual host who is launching the spoofed packets. In order to perform such a trace, the IDS monitor every segment of network and analyze each and every host [5].
2) *Responding at the Target Host:* IDSautomatically respond at the target host *when* an attack is traced. A quick response can prevent the attacker from establishing a better grip on penetrated host and using it for future attacks on network. It can also minimize the effort needed to recover damage done by the attacker.
3) *Responding at the Source:* IDS can restrict the action of attacker by responding at the victim host. It is unlikely that an IDS would have sufficient access to victim host in order to take corrective action without using mobile agent. IDS requires an agent platform to be active on the victim. Mobile agents is a very effective part of the IDS armory [1,14].
4) *Evidence Gathering:* It is said to be impractical to collect automatically evidence of an attack from many different sources. The problem is that how to run the right software at the right place on the right time. Mobile agents offer the ability to run anything, anywhere, at any time. Mobile agents can also control network capabilities by dynamic reconfiguration of the auditing capabilities of host from highly suspicious network locations [1, 14].
5) *Isolating the Source and Target:* Since actions to respond automatically at the victim host and source may fail which ultimately create a need of response at the network level to limit actions of attacker. Three general strategies exist:

   Block the communications of victim host.
   Block the communications of attacker.
   Block communications between the victim host and the attacker.

II. RELATED WORK

Numerous research works are going on these days in IDS for better improvement in the performance of host system as well as networks and its components. The already accomplished research work in the contrast of Mobile Agent based Intrusion Detection Systems (MA-IDSs) have central conceptualization oriented over its feature constraints like design architecture, technique used to develop , strength and weakness also. All these aspects are going to be explored in this paper. Intrusion is an undesirable act which leads to losses of different magnitude in different forms. Intrusion detection (ID) is a part and parcel tool to detect the unauthorized and suspicious activities of intruders that can compromise the

security aspects (i.e. Confidentiality, Availability, Integrity, and Authentication) of data or information as well. In [19] IDS with the integration of Mobile Agents is presented to look after the anomalies found and respond back by taking appropriate measures using agents.

A. Wireless/Mobile ad-hoc network

The collection of wireless mobile hosts forms a dynamic network infrastructure. There are two approaches:

- On the basis of access control[5]
- On the basis of anomaly detection technique for mobile agents [1].

The first approach [5] discusses problems related to latest wireless Ad-hoc network`s infrastructures. These are characterized by the lack of infrastructure. The characterization characteristic creates difficulty to implement generic administrative approaches to short out and enlist the problems to detect intrusions. Using Destination Sequenced Distance Vector Routing Protocol (DSDV), the wireless Ad-hoc communication described in [8]. It is conceptualized by Bellman-Ford routing algorithm. Since DSDV maintains a routing table with attributes such as reachable destination, next hop and neighbouring clusters to communicate. The concern problem associated with the Ad-hoc network is access control. Hence, there is couple of proposed authentication mechanism [5] as: RSA-1024 explained in [21] and AES-128 also includes it. Clustering is an alternative technique to the mobile agent. There are some key responsibilities in this mechanism like-load balancing, fault tolerance and security. It decrease network load, reduce overhead, increase packet delivery from source to destination, overcome network latency, are discussed which make improved use of resources by using mobile agents. It is done by choosing some parameters for analysing the behaviour of routing protocols and finding some comparative evaluations of it with other derived routing protocol for Ad-hoc network. To improve network bandwidth utilization DSDV must very perform very well. The second approach [1] focuses on the anomaly detection technique guaranteed security of mobile adhoc network. In [21] a study illustrates the solution of intrusion detection system in adhoc network. The modern approach is described below –

1) *Mobile agent approach:* In this approach Mobile agent do the following:
   It monitors the neighbouring nodes.
   It collects the information from neighbouring home agent.
   It determines the co-relation among the observed anomalous pattern.
   After analysing co-relation it sends the data. This approach provides security to current node, neighbouring node and network.
2) *Home agent:* It is an important agent for the network, which collects the information from other nodes. It performs its function over application layer to network layer where used to monitors its own system continuously based on the Bayesian classification approach and also develop mobile computing application.

B. Distributed Architecture

There are various approaches to the distributed architecture-

1) *Intrusion Detection based on SNORT:* The snort is open application software. It functions as detector for finding the malicious activity on distributed intrusion detection system (DIDS). It overcomes latency, reduces network load and adapts dynamic environments also [14]. It consists of the following objective:
   It introduced A new mechanism for obtaining extra data about user action from client machine or control module in server applications.
   It reduces the congestion from the distributed intrusion detection system.
   It compares to sensor distributed network [17] and find out many resources problem.
   For analysis here mobile agent collects data and sends them to the main station.
2) *Anomaly Approach*:Since anomaly detection is very important so to find anomaly in the distributed network, there are following approaches introduced:-

Anomaly approach: It detects anomaly by applying comparisons between current activity pattern and predefined patterns. Here any deviation results as anomaly. Hence it is advantageous for finding unknown attacks also. The current Intrusion Detection Problems in anomaly approach includes-

No. of alarms higher that are caused by unusual authorized activities.

It includes some undetected attacks but may occur over an extended time span.

It includes all the abrupt changes in the network deviating from predetermined threshold so that anomaly can be considered as intrusive.

Misuse approach: In this approach signature based intrusions can be detected.

The above discussed approaches can be implemented through mobile agents. These models are called as Mobile Agents for Intrusion Detection System (MAFIDS). MAFIDSs are described in detail in [14]. It is having four level approach like:

Level-1: It is the Down level

Level-2: It is the Pretreatment level

Level-3: It is the Kernel

Level-4: It is the upper level.

MAFIDS is a Distributed Agent Architecture approach. It includes four mobile agents as following:-

Sniffer Agent (SA): It provides a real-time look of the network conversation and its protocols. The agent is cloned and explored over entire network.

Filter Agent (FA): Since Intrusions may spread over all levels of the distributed network, so this agent provides filtering from various sources by analyzing of data by monitoring, aggregating, sorting and merging events.

Analyzer Agent (AA): As its name it functions as analyzer. This agent is used to analyze the events collected from the previous two agents. It finds the alarm condition in the network.

Decision Agent (DA): This agent is used to transmit decision to the administration level.

C. Multilevel Anomalies Detection approach

Anomalies detection system (ADS) is of the type of existing architecture. It implements the "Plug-in", so ADS having requirements of signatures' database. Due to movable behavior of ADS, in computer system it suffers a heavy outgoing flow. The ADS architecture is centralized one and it correlates in single level after taking incoming events. It stuck with the huge surcharge of the alerts, hence master machine may falls into some breakdown. Distributed multilevel approach can be categorized into two ways:

1) *Synchronous detection:* Synchronous anomalies detections method consists of a set of sensors in the system [7, 16-17]. These sensors composed with a host ADS, a network ADS and an integrity checker. The anomalies detector generates it's outcome in such a concentrator module which is divided in two parts. It is a collection of database of alert and normalization. Finally all alerts will go for correlation. It is composed of two parts one is aggregation and another synthesis for enhance anomalies detection.
2) *Asynchronous detection:* Asynchronous anomalies detection can be categorized as below.
   Local asynchronous anomalies detection.
   Distributed asynchronous anomalies detection.

As studies exploit the distributed anomaly approach of correlation levels performed in way that first of all initial step is to filter anomalies associated with all hosts which will become the input for distributed detection`s architecture of the second level. This model is used to minimize the false positive rate (FP) and network load for empowerment of network security. This architecture recognizes and unhide the unknown anomalies with delayed period of synchronous and asynchronous detection by the help of mobile agent.

Functional steps of multilevel ADS:

Step-1- ADS architecture`s administrator supply a mobile agent (MA) to first host.

Step-2- The MA integrated by (Sniffer Agent-1)SA1 with suspected detected results and sends to second host.

Step-3-The result of previous step-2 migrated by SA2 and passed to next host.

Step-4- Step-1 to step-3 processes will repeat until MA will return back to administrator [9].

D. Immune Mobile Agent

The Immune Mobile Agent is a mechanism organized with two concepts. One of them is dynamic clonal selection algorithm and another collaborative signal mechanism. In this mechanism an Immune mobile agent is used. Since Mobile agent behavior possibly forwarded to local host, hence two reductions caused one is reduction of network load and another reduction in capability of improvement of real time. Here Immune mobile agents roam over the network to monitor and detect any attack.

The architecture of Immune mobile agent composed with some agents like:

Central control agent (C-agent)
Detection agent (D-agent)
Memory agent (M-agent)
Response agent (K-agent)

Here D-agent and M-agent roam on the network and K-agent only activated if any attack has been found. C-agent perform managing, coordinating on network and control roaming agents. Where M-agent is a set of memory detectors in the secondary response in immune system. M-agent activates if any suspected pattern has been detected in the system otherwise D-agent perform detection over entire time. Mainly collect agent collects data [4-5, 14].

E. Peer to Peer Intrusion Detection System

In this type of IDS, suspicious activities are verified by sending the detection request to other hosts of the system. To avoid single point failure this system is used. There are six types of agents introduced in this model. Agent are-

1) *Monitor Agent:* It performs the monitoring activities like detecting some suspected activities.
2) *Analysis Agent:* It integrates and analyzes the information from monitor agent. In the case of multi host attack, manager agents reply
3) *Executive Agent:* It performs restoring corrupted files, preventing network connections etc.
4) *Manager Agent :* are static agents Each manager agent has a RAR
5) *Retrieval Agent:* It is a dynamic agent. Here Time to Life (TTL) is generated by initiator. It also gives information about the number of rest nodes.
6) *Result Agent:*It is a dynamic agent. These are used to send the required information back to the manager agent (initiator), which perform the decision making for broadcasting in the case of multi host attack.

Working Process- In Peer to Peer intrusion detection system first of all Monitor agent performs analysis over the network and obtained suspicious activity is reported back to the Analysis agent. It is the responsibility of Analysis agent to decide

the nature of attack, whether it is attack or intrusion and accordingly executive agents are informed to take action against the intrusion or attacks.

F. Central coordinator approach

It is very efficient approach for detecting unintended behavior and activities. Since architecture for IDS of the type mobile agent detects the complex attack to the networks. As it implies the some load on entire network and thus detects the suspicious activity also. There are different intrusion detection methods and architectures exists for finding suspicious activity of the host, in the distributed intrusion detection based on mobile agent(DIDMA) its architecture is designed as per host entry , here trigger is used, which is an specific event. It will be received by Victim Host List (VHL). On the basis of type of trigger; events will be dispatched to visit all victim using the victim path. Since there exists dependency on a central node due to central node model so few shortcomings can also be existed by single point of failure. Here network is being configured within different phases. For each phase there is a manager and alternative manager designed, and the key component is placed over host manager in subnet which can be executed automatically or manually as well [1, 3, 11, and 21].

Here different MA-IDS can be reviewed collectively from given TABLE I.

Table i: quick view of reviewed ma-IDSS

Architecture	Approach	Technique	Strength
Adhoc based	Destination Sequence Distance Vector Routing(DSDV)	Authentication mechanism(RSA 1024, AES 128) Clustering of mobile agent	Low routing, less overhead
Adhoc based	Anomaly detection using MA	Bayesian classification	High rate of anomaly, Reduced false alarm
Distributed based	Anomaly detection	Event correlation engine, Agent synergy	Reduced false alarm rate, ID is greater than SNORT
Hybrid and Distributed based	Distributed multilevel(synchronous and distributed correlation) approach	SynFlooding	Least result of false positive rate, false negative rate, semantic detection
Distributed	Immune based	Dynamic clonal selection algorithm and collaborative signal mechanism	Reduced false positive rate, Increased detection rate
Distributed	SNORT based	Message exchange between server and SNORT	SNORT performance is good
Distributed	Peer to peer IDS	Retrieval agent generation, retrieval agent dispatch	Efficient migration strategies, MADIDF is better than MASHD
Distributed	Central coordination peer to peer IDS	Agent based	Less load on entire network, detection more complex, distributed attack

G. Issues

Until now IDS have poor perfection. There are so many shortcomings associated with IDSs. During development of these IDSs many shortcomings continuously addressing through the improvement and refinement of existing techniques, but some of them are inherent in the way IDSs are constructed. There are the most common shortcomings given below:

1) *Lack of Efficiency:* To evaluate the activities in real time IDSs are needed. It is very hard need to meet when faced with a very large number of events as is typical in today's networks. hence, HIDSs usually slower down a system where as NIDSs drop network packets for those there is no sufficient time to process.
2) *High Number of False Positives:* Most IDSs detect attacks throughout an enterprise by analyzing information from a single host, a single application, or a single network interface, at many locations throughout the network. False alarms are high and attack recognition is not perfect. Lowering thresholds to reduce false alarms raises the number of attacks that get through undetected as false negatives. Improving the ability of an ID to detect attacks accurately is the primary problem facing IDS manufactures today.
3) *Burdensome Maintenance:* There are some requirements specific knowledge as well as substantial efforts to configure and maintain the IDSs usually. Here some examples like, misuse detection where usually for their

implementation expert system shells that encode and match signatures using rule sets are used. Upgrading these rule sets involves details peculiar to the expert system and its language for expressing rules sets, and it may only permit an indirect specification of the sequential interrelationships between events. These considerations are also applied to the addition of a statistical metric, typically used to find unusual deviations in nature.

4) *Limited Flexibility:*If an Intrusion detection system has been developed for a typically specific environment then it may hard to use in other environments whether it consists of same kind of concern as well as policies. The mechanism used for detection may also face hardships to adapt to different patterns of usage. The tailoring detection method specifically to the system with some if and buts replacing those over time with improved detection techniques are also problematic with many IDS implementations. Often the IDS needs to be completely restarted in order to make changes and additions take effect.

III. IDS TOOLS

A. SNORT

It is an open source of the type network intrusion detection and prevention system.It can perform two functions over IP networks:

Real-time traffic analysis
Packet logging on.
Initially it was called as a "lightweight" intrusion detection technology.

SNORT has some specific features like:

It is having rich IPS technology that can be concluded byits over 4 million downloads and nearly 400,000 registered users.
It is the most widely deployed intrusion prevention technology in the world.
It contains rules to describe traffic
It has a detection engine that utilizes a modular plug-in architecture

SNORT has three primary uses:

A straight packet sniffer like tcp dump
A packet logger (useful for network traffic debugging, etc)

A full-blown network intrusion prevention system [11].

SNORT components are –

1) *Data Flow Capture:* It captures the data packets from the network, monitors it and sends the data to the IDS for detecting suspicious activity.
2) *Intrusion Detection Agent:* It plays a vital role in IDS, which seems to function as a central node and data pre-processor. It is used to check the system has either normal or abnormal behavior according to their set of rules. It informs the administrator, if any error occurs.
3) *Mobile Agent Environment*: It is used to create agent, interpret, execute, transfer and terminate the agents.
4) *Data Analysis:* This Analysis is a training procedure which is used for transferring the data to mobile agent and also collects worthy information from them and analyzes them.
5) *Sensors (Sniffing):* It is used for network analysis, performance analysis and monitoring. It uninterruptedly sends the data to the network until stop sniffing instructions received [21].

IV. RISK ANALYSIS

*Possible Risks for Services:*TABLE II. is showing the possible intrusions and affected services.

Table 2: intrusions and description [21]

Intrusion	Protocol	Description (Risks for Services)
Land	TCP SYN	Source and destination IP addresses are the same causing the response to loop.
SYN Flooding	TCP	Sending large numbers of TCP connection initiation requests to the target. The target system must consume resources to keep track of these partially open connections.
Teardrop	TCP fragments	Sends overlapping IP fragments.
Smurf	ICMP	ICMP ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.
Ping of Death	ICMP	ICMP packets greater than 65536 bytes can shut down a system.
Open/Close	TCP/UDP	The open/close attack opens and closes connections at a high rate to any port serviced by an external service through internet service demon (inetd). The number of connections allowed is hard coded inside inetd.

ICMP Unreachable	ICMP	The attacker sends ICMP unreachable packets from a spoofed address to a host. This causes all legitimate TCP connections on the host to be torn down to the spoofed address. This causes the TCP session to retry and as more "ICMP unreachable" messages are sent, a DoS condition occurs.
ICMP Redirect	ICMP	ICMP redirects can cause data overload to the system being targeted.

V. CONCLUSION AND FUTURE WORK

This paper reviewed a number of presented mobile agent based intrusion detection system (MAIDS) and projected different types of presented MAIDS architecture. It presented behaviour to sense the intrusion, the mode of information collection, the method of IDS used in the variety of scenarios and the security of the presented systems is also discussed. This paper focused on the various type of intrusion detection system (IDS) techniques like Misuse detection, Anomaly detection,. Here mentioned various architecture of Hierarchical, Network, and Hybrid like Distributed system and Centralized system. Immune mobile agent is based on Distributed IDS improves dynamic clonal section algorithm and collaborative signal mechanism to increase detection rate and reduce false positive rate. The intend of applying such types of intrusions is to accentuate and refer to other IDS [7]. At last it included the strength and drawback of existing MA-IDS. The existing IDS approach can be improved by providing additional security in mobile agents. In future work there is necessitate to examine the novel concept of activities to build this agent additional intelligent to increase the genuine performance and follow any latest type of attack which is the major objective to use the network IDS.

REFERENCES

[1] Wang Yu, Cheng, Xiaohui and Wang Sheng ,"Anomaly Network Detection Model Based on Mobile Agent", *IEEE,Third International Conference on Measuring Technology and Mechatronics Automation*, 2011.

[2] Jaydip Sen "An Agent-Based Intrusion Detection System for Local Area Networks" published in *International Journal of Communication Networks and Information Security (IJCNIS)* Vol. 2, No. 2, August 2010 PP 128-140

[3] Mr. Suryawanshi G.R, Prof. Vanjale S.B "Mobile Agent for Distributed Intrusion detection System in Distributed System" Publication in" *International Journal of Artificial Intelligence and Computational Research (IJAICR.)* ", Jan-June 2010 .ISSN-0975-3974. PP 1-8.

[4] Shiv Shakti Srivastava, Nitin Gupta, Saurabh Chaturvedi, Saugata Ghosh "A Survey on Mobile Agent based Intrusion Detection System" published inInternational Symposium on Devices MEMS, *Intelligent Systems & Communication (ISDMISC) 2011 Proceedings published by International Journal of Computer Applications® (IJCA)*PP 19-24.

[5] Pranita Jain, Sandeep Raghuwanshi And Pateria Rk "New Mobile Agent-Based Intrusion Detection Systems For Distributed Networks" *International Journal Of Wireless Communication* Volume 1, Issue 1, 2011, Pp-01-04 [Online], Available: Http://Www.Bioinfo.In/Contents.Php?Id=109

[6] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" *Computational Intelligence and Communication Networks (CICN)*, 2012 Fourth International Conference on 3-5 Nov. 2012 Page(s): 695 - 699

[7] Zhang Ran "A Model of Collaborative Intrusion Detection System Based on Multi-agents" *IEEE International Conference on Computer Science & Service System (CSSS)*, 2012 , Page(s): 789 - 792

[8] Martin Rehak, Michal Pechoucek, Pavel Celeda, Jiri Novotny, Pavel Minarik "CAMNEP: Agent-Based Network Intrusion Detection System" published in *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems (AA-MAS 2008)- Industry and Applications Track*, Berger, Burg,Nishiyama(eds.),May,12-16 2008, Estoril, Portugal, pp.133-136 Available: www.ifaamas.org/ Proceedings/.../pdf/.../ AAMAS08_IndTrack_34.pdf

[9] Xiantai Gou ; Weidong Jin "Multi-agent system for security auditing and worm containment in metropolitan area networks" *Autonomous Decentralized Systems*, 2005. ISADS 2005. Proceedings 4-8 April 2005 Page(s):201 - 207 Print ISBN:0-7803-8963-8.

[10] D.J. Ragsdale, C.A. Carver, J.W. Humphries, U.W. Pooh, Adaptation techniques for intrusion detection and intrusion response systems, Proceedings of the *IEEE International Conference on Systems, Man and Cybernetics, 2000*, pages 2344-2349, http://www.itoc.usma.edu/ragsdale/pubs/adapt.pdf.

[11] C. Krügel, T. Toth, Applying Mobile Agent Technology to Intrusion Detection, ICSE Workshop on Software Engineering and Mobility, Toronto May 2001[online], Available: http://www.elet.polimi.it/Users/DEI/Sections/Compeng/GianPietro.Picco/ICSE01mobility/papers/krugel.pdf.

[12] E. Lundin, E. Jonsson, Survey of research in the intrusion detection area, Technical report 02-04, Department of Computer Engineering, Chalmers University of Technology, Göteborg January 2002, Available: http://www.ce.chalmers.se/staff/emilie/papers/Lundin_survey02.pdf.

[13] Stonesoft Corp. Stonesoft Corp "Intrusion Detection and Analysis for Active Response - Version 1.2" Available: https://www.stonesoft.com/opencms/ export/system/galleries/download/product_docs/archive/SG_IPS_12_SMC_32_RG.pdf

[14] Trushna Tushar Khose Patil, C.O.Banchhor "A survey on Mobile Agent Based Intrusion Detection System" published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 9, November 2012 PP 773-777

[15] www.laas.fr/METROSEC/Security_and_DoS.pdf

[16] 1A. KARTIT, 2A.SAIDI, 3F.BEZZAZI, 4M. EL MARRAKI, 5A. RADI " A New Approach To Intrusion Detection System" *Journal of Theoretical and Applied Information Technology* 29th February 2012. Vol. 36 No.2, Avilable: http://www.jatit.org/volumes/Vol36No2/16Vol36No2.pdf

[17] P.Rama Subramanian and J. Wilfred Robinson2 "Alert Over the Attacks of Data Packet and Detect the Intruders" *International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*, 2012

[18] Jianping Zeng and Donghui Guo "Agent-based Intrusion Detection for Network-based Application" *International Journal of Network Security*, Vol.8, No.3, PP.201-210, May 2009

[19] Ionita, L. "An agent-based approach for building an intrusion detection system" *Networking in Education and Research, 2013 RoEduNet International Conference* 12th Edition 26-28 Sept. 2013 Page(s):1 - 6 ISSN :2068-1038 Print ISBN:978-1-4799-2599-5

[20] Renuka Prasad.B, Dr.Annamma Abraham, Chandan. C, Prabhanjan.A, AjayBilotia "Information Extraction for Offline Traffic Anomaly Detection in NIDS" *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.9, September 2008 309 Manuscript received September 5, 2008. PP 309-315.

[21] Kamaruzaman Maskat, Mohd Afizi Mohd Shukran, Mohammad Adib Khairuddin & Mohd Rizal Mohd Isa "Mobile Agents in Intrusion Detection System: Review and Analysis" Modern Applied Science Vol. 5, No. 6; December 2011 ISSN 1913-1844 E-ISSN 1913-1852 pp 218-231

