The Architecture of Mobile Agent Based Distributed Intrusion Detection System (MABDIDS)

Okan Can, Ozgur Koray Sahingoz, Emin Kugu

***Abstract*——An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. In a network-based intrusion detection system, the individual packets flow through a network are analyzed. In a host-based system, the IDS examines at the activity on each individual computer or host. IDS techniques are divided into two categories including misuse detection and anomaly detection. In recent years, mobile agent based systems are emerged as an attractive paradigm and they are defined as agents that can migrate among different hosts. According to their creation purpose, they can execute their tasks autonomously in distributed environments by communicating with other mobile and static agents. In this paper, we described an architecture for intrusion detection by combining both IDS mechanisms of both network and host based IDS. The proposed approach can monitor the system by using mobile agents which are the lowest-level element to collect and analyze intrusion data. By using this technology it is aimed to overcome the speed-bottleneck of IDS by reducing network load.**

***Index Terms*—security, intrusion detection, mobile agent, cyber-attack.**

I. Introduction

TOday the Internet continues to grow day by day and it connects hundreds of millions of computing devices all around the World, which run on different type hardware and software platforms to provide a lot of services. On the other hand, this interconnectivity among these devices also enables security deficiencies and, as a result, malicious users can easily attack to networked systems and misuse resources. While these attacks are increasing, there is a growing need to develop a secure network systems. In network security concept, firewalls are the most preferred tool. However, *Intrusion Detection Systems (IDSs)* differ from firewalls and they mainly focus on intrusions/attacks that originate from within the system. If an IDS evaluates a suspected intrusions once, it can directly signal an alarm.

According to Symantec's Internet Threat Report in 2013 [1], *there is a 42% increase in targeted attacks, 31% of all targeted attacks aimed at businesses with less than 250 employees, one waterhole attack infected 500 organizations in a single day, 14 zero-day vulnerabilities, 32% of all mobile threats steal information, a single threat infected 600,000 Macs in 2012, spam volume continued to decrease, with 69% of all email being spam, the number of phishing sites spoofing social networking sites increased 125% , web-based attacks increased 30%, 5,291 new vulnerabilities discovered.* Every year the number of these attacks increases incredibly and have an important role for the Worlds economic, social, political, military system.

Mainly, IDSs are usually classified in two categories: host-based and network-based. Host-based IDSs decide whether an intrusion exist or not according to information obtained from a single host (i.e. system calls, log files, CPU utilization, etc.). On the other hand, network-based IDSs collect data by monitoring the network in which hosts are connected. Although, they are suitable for catching distributed attacks, they cannot analyze encrypted data.

At the same time, IDS can be divided into two classes in terms of their data analysis and processing units: anomaly based IDS and signature based IDS. In the former one, IDS reacts to anomalous behavior according to previously defined or stored definitions from the history of the monitored system. However, in the later one, an IDS contains a preloaded database of known attack signatures and to detect an attack it compares the stored ones with the intrusion signatures.

In recent years, mobile agent technology has been emerged as an exciting concept in distributed computing platform. Because of it autonomous decision making capability, mobility feature from one host to another, and it social ability to communicate with other static/mobile agents enables to use them as a good solution opportunity to lots of distributed problems.

In this paper, it is aimed to implement an IDS architecture by using a mobile agent structure to execute them on a distributed systems in scalable and efficient way. Proposed system can detect the attacks not only by network based IDS technique, but also by host based IDS technique. System also uses both anomaly detection techniques and signature detection techniques to decrease false positive and false negative rates. Therefore, this approach can be called as a hybrid IDS approach.

Because of the distributed structure of mobile agents proposed system can continue intrusion detection when a problem occurs in a host. As a result, the network load can also be reduced because active codes go to data instead of moving data to code. As a last point, it is possible to run this system in a heterogeneous platforms, and it can react dynamically to environmental changes.

The rest of the paper is organized as follows: The necessary background information was given in Section 2. Then, the proposed architecture and system components

Manuscript received March 14, 2014 revised April 10, 2014

O. Can, Department of Computer Engineering, Turkish Air Force Academy, Istanbul, Turkey, ocan@hho.edu.tr

O.K. Sahingoz, Department of Computer Engineering, Turkish Air Force Academy, Istanbul, Turkey, sahingoz@hho.edu.tr

E. Kugu, Department of Computer Engineering, Turkish Air Force Academy, Istanbul, Turkey, e.kugu@hho.edu.tr

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

are detailed in Section 3. In Section 4, the recent related works are detailed. Finally, Conclusions and Future works are presented.

II. Basic Issues

In this sections, the following issues, such as cyber-attacks, intrusion detection systems and mobile agent technologies have been studied to make an introduction to main concepts of the proposed structure.

A. Cyber Attacks

Cyber-attacks are attempts which try to by-pass computer security mechanisms. Information security is one of the most important parts of cyber security issues. Any intrusion to the system has a negative impact on the confidentiality, integrity, or availability of that information [2]. The most important risk of todays internet world is the attack which done over network and these attacks divided into four basic categories [3]:

Port Scanning: Scanning a specific port continuously (ipsweep) or scanning all ports to find services which are on any server (portsweep)[4].

Denial of Service (DoS): Denial of Service (DoS) attack utilize weakness of TCP/IP protocols. It aims to make out of service the server. Attacker sends requests and s/he try to server cant answer these requests.

Remote to Local (R2L): This attack is making an unauthorized logging to the system as a guest or another user. A Trojan attack (sshtrajan) which works on Unix operating system can be given as an example.

User to Root (U2R): In this type of attack, an attacker gets the password information of an authorized user, and he can log on like authorized user to system limitlessly [5].

B. Intrusion Detection Systems

First intrusion detection system (IDS) was developed by Dorothy Denning at SRI International. After that, a lot of intrusion detection systems have been proposed, and numerous studies created various IDSs. IDS are one of the most important systems to make efficient system security. Due to traditional firewall cannot provide a certain security for intrusions that growing in our time Intrusion Detection Systems are very necessary. Intrusion Detection (ID) is an active and important research area of network security.

The goal of Intrusion Detection can be sorted like this:

- Attack detecting
- Attack preventing
- Evidence collecting
- Situational awareness
- Enforcement of connection policies.

IDSs main goal is to detect the attacks which can happen from inside or outside. The more detecting the attacks successfully, the more decreasing the attackers motivation. When architecture of IDS is examined (as depicted in Figure 1), it is seen that IDSs components like this:

- Sensor: It is responsible for collecting data from the monitored system.
- Detector (Analyze Engine): It processes the data collected from sensors to identify intrusive activities.
- Knowledge Base: contains information collected by the sensors, but in a preprocessed format (e.g. knowledge base of attacks and their signatures, filtered data, data profiles, etc.). This information is usually provided by network and security experts.
- Response Component: It initiates actions when an intrusion is detected. These responses can either be automated (active) or involve human interaction (inactive).

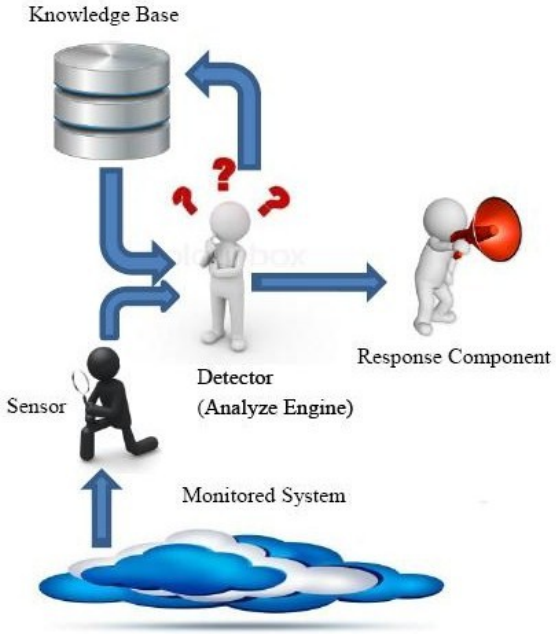

Fig. 1. Public (Classically Known) Intrusion Detection System Structure.

Intrusion detection systems can be divided into two parts according to monitor the system: *Network Based Intrusion Detection System (NIDS)* and *Host Based Intrusion Detection System (HIDS)*. Selecting NIDS or HIDS can chance according to circumstances (organizational structure, user profile, accessible resources, the overall risk of an organization have, system structure). HIDS is on a specific computer and monitors the intrusions that can be on this machine. NIDS is on a distributed network and monitors network traffic to detect intrusions that can be on this network. NIDS sensors can be on anywhere of network. These days combining both of NIDS and HIDS is a current trend. This approach is named as Hybrid system. There are two basic approach to detect intrusions. These approaches can be divided into two techniques too. Techniques are named as ”**anomaly detection**” and ”**misuse detection**”.

Anomaly detection is an approach examining normal behaviors. It thinks ”anomalies are not normal”. This technique uses normal behavior to match and identify anomalies. Anomaly detection analyzes profiles of user, network connections and servers acting normally. This technique is successful to detect new attacks but sometimes can give false alert.

Misuse detection depends on the signature of known attacks. System has a knowledge base including attack signatures and weak points of the system. Misuse detection technique uses pattern of known attacks and their signatures to match and identify the attacks. Misuse detection is so

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

efficient for known attacks but has some weakness for new and not known attacks. Misuse detection use keystroke monitoring based approaches, genetic algorithm, data mining, expert system and pattern matching.

C. Agent Based Systems

Agents are computer system/softwares that have the capability for changing environment by inputs getting from the same environment autonomously [6]. The most significant peculiarity of agent systems is having their own autonomy. Agents are goal based and show social and sensible behaviors and also have learning capability. All of the agents in multi-agent systems have control of its own thread. Besides, control is distributed in multi-agent systems.

The system that is formed with many autonomic agents, we called multi-agent system. In this system, agents have different goals. To succeeded, agents have to coordinate, cooperate and communicate with each other [7]. In addition, agents are agreed on common rules before to achieve coordination and cooperation. Thus, the effective communication model is exposed.

In multi-agent system, if the agents that are developed from different platforms exist, we have to decide on a common language to obtain communication between these varied platform formed agents. We call this common language, The Agent Communication Language and generally, FIPA-ACL is the well-known language in agent communication languages.

Mobile agents are also communicative agents that migrate from one node to another autonomously and continue its work for completing the task in heterogeneous network system [8].

III. PROPOSED MOBILE AGENT BASED SYSTEM

It is aimed that planned system has two principles. MABDIDS is planned as a system that can analyze both network traffics and host traffics so that it has sensors both on the host and the network. Because of the system is planned mobile agent based, it is considered that the system doesnt have any network traffic density and is efficient, flexible and scalable. Due to system has both host sensors and network sensors, it has NIDS and HIDS properties. It also uses both of detection techniques (Anomaly Detection and Misuse Detection). So that the system can detect known attacks and new attacks which not known and change the routines of the system.

A. JADE Platform

The implementation platform is selected on JADE (Java Agent Development Framework). This framework is fully implemented in JAVA language, and it has two important advantages to use. The first one is JADE try to make easier the agent system development in compliance with the FIPA specifications. The second one is it supports heterogeneous computers due to all computers must have Java Runtime Environment. JADE serves some additional benefits to developers and it contains following components:

- *a runtime* environment where in agents can be alive and must be active,
- *a library* used for creating agent,
- *a GUI* that allows to make easier creating, managing, killing the agent.

The execution environment of JADE agent system is called as *container* and the set of these containers is called as an *agent platform*. The platform must have a working *main container* and other containers register via main container to the platform. In the proposed architecture, these containers are designed as depicted in Figure 2. All hosts are connected to MABDIDS management system (Main Container), and they are named as container1, container2, container3,..., containerN (N = Number of Nodes).

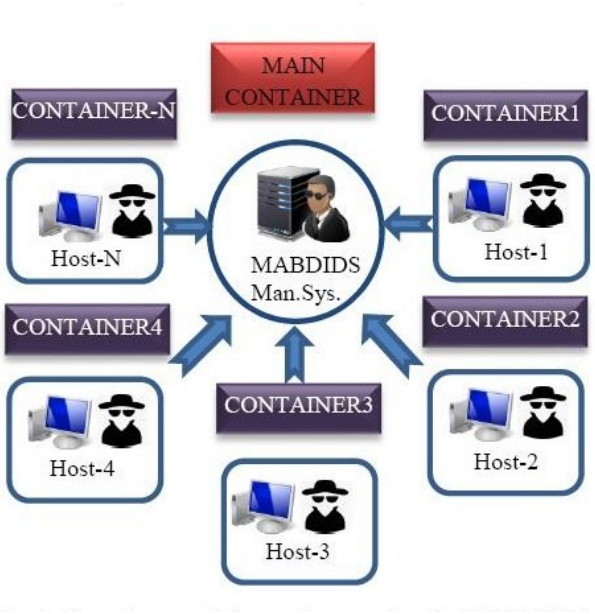

Fig. 2. Containers and Agent Connections in MABDIDS.

B. MABDIDS Architecture

The system has four main components as depicted in Figure 3.

1) MABDIDS management system: MABDIDS Management system manages all communication and interaction between agents. It mainly responsible for the coordination of all activities in the systems. It also has the administrative roles overall static and mobile agents in the system.

2) Sensor Agent: Sensor agent collects data from critical points of the network and sensors by using data sniffing programs. Sensor agent controls log files, accessing to kernel and system files and collect data for mobile analysis agent. These programs can be shown as data sniffers which are SNORT, dSniff, NetworkMiner.

3) Mobile Analysis Agent: Mobile analysis agent is created by MABDIDS management system. It moves with a route which is given by MABDIDS management system. This route says to mobile analysis agent that how it moves and which sensor agents are visited. It decides whether there is any intrusion or not by use the data which collected by sensor agent. If it decides, there is any intrusion then warns the response agent by an ACL message. It can be followed that how mobile analysis agent work in Figure 3.

4) Response Agent: A response agent produces a warning when mobile analysis agent decide to there is an intrusion. Response agent is created on the main container (MABDIDS Management System) and is responsible for managing system, generating an alarm. It waits for messages come from

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

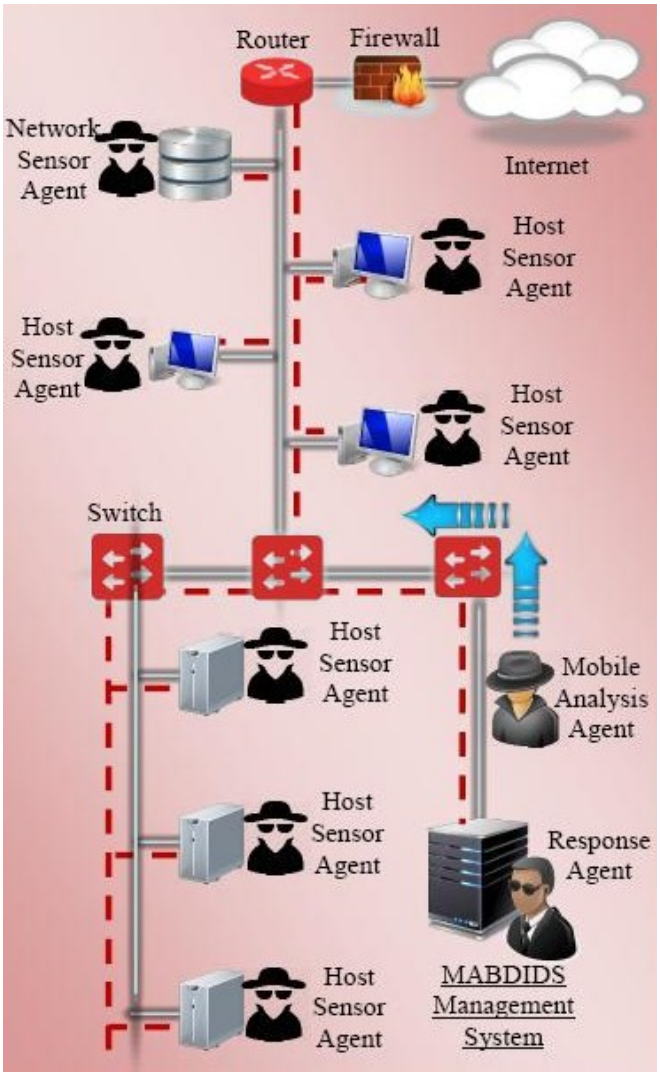

Fig. 3. Proposed Mobile Agent Based Distributed Intrusion Detection System Architecture.

mobile analysis agent about intrusion. If an intrusion message comes from mobile analysis agent, it generates an alarm message to system administrator. Response agent has two behavior. These behaviors are communication behavior and alarm generator behavior.

C. Agents and their Coordination

This system has many agents, and we have described our agents as three types (sensor agent, mobile analysis agent, response agent) previously. Sensor agents run on hosts (computers e.g.) and network component. We plan to use network component for NIDS, and we placed it on a critical point over LAN. Sensor agents are divided into two parts and named as Network Sensor Agent and Host Sensor Agent. Both of them make same works, but they are named according to machine they placed for having situational awareness. Sensor agents have two behaviors. These behaviors are data collecting and communication.

Mobile analysis agent is created on main container and visits all containers (computers, network components) by a route. Mobile analysis agent has three behaviors. These are moving behavior, communication behavior and analyze the behavior.

Mobile Analysis Agent matches the raw data which get from sensor agent with attack signatures. These known attack signatures are in knowledge bases. All of the hosts have a knowledge base. This matching provides misuse detection for user. After that even if mobile analysis agent cant match data with known attack signature, it uses data for anomaly detection and work for hardly whether any abnormal data there is or not. If mobile analysis agent finds any abnormal data, it flag data as an intrusion and after update knowledge base, warns response agent. Transactions over hosts and network are shown in Figure 4.

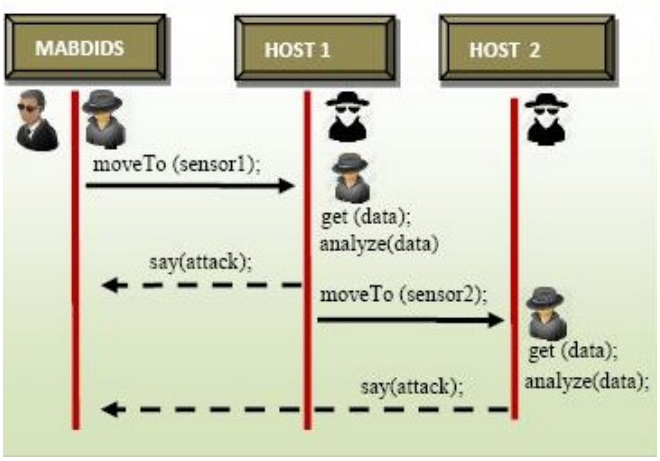

Fig. 4. Message Traffic And Communication Architecture of System Agents.

Agents of MABDIDS have several tasks and in order to perform tasks they must work cooperatively, so they exchange messages. Response agent needs to learn whether there is an intrusion or not the message comes from analysis agent, so communication between agents is very important. The principal characteristic of MABDIDS is the individual agents communicate and interact. This is performed through the message passing and to understand each other, it is very important to be agreement about format and semantics of this messages. JADE adopts FIPA ACL standards so that JADE agents can interact with other agents which is written by different program language. The Foundation for Intelligent Physical Agents (FIPA) is a non-profit associations and based on speech acts (messages are actions or communicative acts.). A sample FIPA-ACL message is shown in Figure 5.

```
( inform
   :sender mobile_analysis_agent29
   :receiver response agent12
   :content (intrusion type:TYPE27  detected on:HOST21
info:NULL)
   :language SL
   :ontology IDS
)
```

Fig. 5. A FIPA-ACL Message to Response Agent.

D. Intrusion Detection Algorithm

Proposed architecture controls both Signature base intrusions and Anomaly based intrusions. These intrusions are catched according to algorithms in Figure 6.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

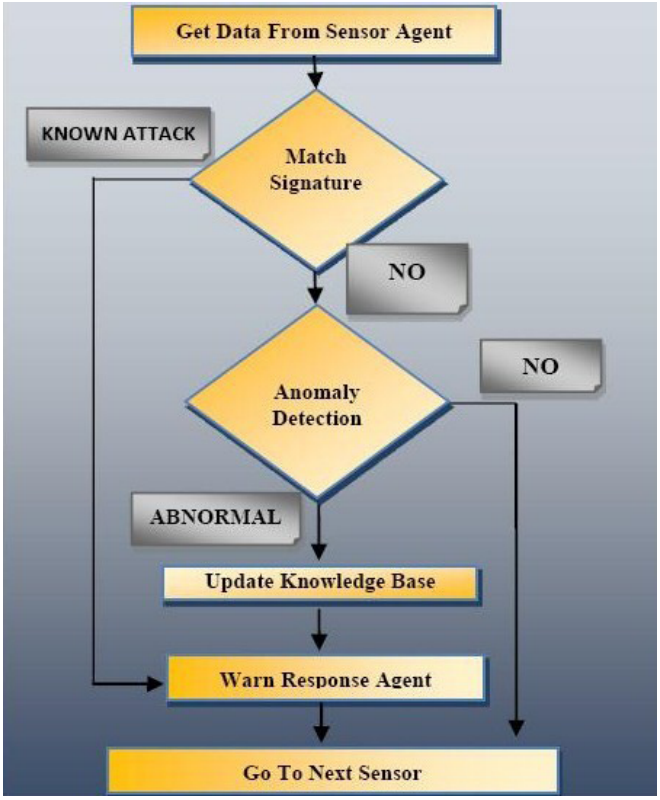

Fig. 6. The Working Algorithm of Mobile Analyze Agent on Any Sensor.

In the first phase the signature of the detection is controlled from the knowledgebase/signature base of the system. If it is not matched, the anomaly of the suspected message/event is controlled.

E. Advantages of Proposed System

It is predicted that users have a lot of benefits by implementing the system with mobile agents. Most of these advantages are listed in [9]:

Reducing Network Load: Through developing Intrusion Detection Systems, the most important problem we confront with is the high data transmission density in the network. All of the servers in the network, forward the gathering data to centralize area for analyzing. In this case, bandwidth problem occurs in the network. Mobile agents cope with this problem. As through this approach data is not sent to agent, agent migrates to data to solve the overload data in the network.

Overcoming Network Latency: Mobile agents migrate from one server to another and continue their work in target server. Therefore, agents can achieve to establish communication faster than communicate with centralized coordinator according to hierarchical IDS approach.

Asynchronous Execution and Autonomy: Mobile agents can complete their tasks in case of their platforms loses the connection of the network. Mobile agents support centralized controller to IDSs and even if the communication line of the controller is out of service, IDS can continue running by means of mobile agents. So, this situation provides fault tolerance mechanism to the system.

Dynamic Adaption: Mobile agents can be moved, migrated, cloned and killed. They can be moved to another site and can work at other site dynamically. This dynamic adoption helps users for scalability too.

Behavior: Mobile agents have parallel behavior working paralleled, and this parallel behavior shows a multithread architecture. Users organize agents by this parallel behavior.

Scalability: Mobile agents can achieve their goals in network by their migration behaviors. This behavior makes the system more scalable.

According to the above attributes, we will argue, in this section, the use of mobile agent to improve the characteristics of the IDS, overcome the limitations described previously and to evaluate their applicability to design an automated intrusion detection:

IV. RELATED WORKS

Mobile agent approach brings a new dimensions to IDSs. There are some proposed IDS systems with agent usage in the literature. Although their common point is the agent structure that they use, they also differ in the roles of agents in a multi-agent solution platform.

In [10], the authors tried to reach a performance enhanced IDS by applying an Artificial Neural Network to make a decision over the agent based intrusion detection systems. Their proposed system presents a distributed structure consisting four interconnected phases. Namely down, pretreatment, kernel and upper levels. All of these four levels have special agent types. These agents can move from one node to another while they are communicating with each other and having collaborative works. Sniffer agent category is for down level; Filter agent category is for pretreatment level; Analyzer agent category is for kernel level and Decision agent category is for upper level.

The data required by the ANN is collected by agents communicating with each other all over the IDS. The ANN is trained by supervised learning method feed with event parameters and attacks as the input and the desired output sets. The authors chose a Multilayer Perception structure as the ANN within the IDS.

The number of neuron in the input layer of the ANN is decided by the amount of events collected and sent by the sniffer and filter agents. They placed about 20 neurons in the input layer. The hidden layer is very important for decision making in an ANN. For their work, they put three hidden layers having 5-10-15 neurons respectively as the best solution for IDS. The output layer has 20 neurons each one representing different attacks. The mission of the output layer is to catch the possible attacks to the system. The results of the simulation conducted using JavaNNS show the reduction of false positive alarms and increase on the attack detection performance supported by the information on the status of the system.

Zhisong et al. developed an IDS structure especially for the large-scale complex networks in which the collaborative works are done by the mobile agents [11]. The distributed IDS based on mobile agents consists of several agent types implemented in JADE. Management agent checks the condition of all agents living on the system, and it works as an interface between the management and the network. Daemon agent controls the life cycle of the internal agents and guides the agents to the targeted networks. Crawler agent travels all over the network and collect important information about the processes to sense an intrusion. Sensor agent investigates the system logs and creates its own intrusion detection database.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Info Collection agent collects information from the databases about the target node. Learning agent tries to figure out the user behavior using data mining techniques. Integrated learning agent synthesise all kinds of data from different types of agents to make a judgment if there is an intrusion. Tracking agent tracks the intrusion back to find the source of it. The authors advocate that their proposed system lighten the network load reduce the false negative and positive alarms.

In [12], the authors designed a new architecture consisting seven components. Their proposed model is a mix of classification and outlier detection methods. In addition to that, they propose an intelligent agent based attribute selection method to increase the accuracy of the detection compared with the other algorithms such as support vector machine. The proposed IDS is especially for the MANETs and the experiments conducted by the authors show that the system catch the attacks with the accuracy of 99.77%, 99.70%, and 79.72% for the attack types DoS, Probe and other attacks respectively

V. CONCLUSION

In this paper, it is aimed to design a Mobile Agent Based Distributed Intrusion Detection System (MABDIDS) by combining both network based intrusion detection and host based intrusion detection techniques. System can also detect intrusions not only by using signature based approach, but also anomaly based approach. By using these techniques and approaches, it is intended to increase the speed up the detection process, especially in the new type of attacks, and to decrease to decrease false positive and false negative detection rates.

The proposed system also uses mobile agent based structure for detecting intrusion. This results a distributed detection architecture and makes IDS system more robust. System is designed as a multi-agent concept and contains both mobile and static agent and these agent can communicate each other over a large network. This mechanism increase the adaptability and scalability of the system decreases network load and enables asynchronous execution environment.

REFERENCES

[1] Symantecs 2013 internet security threat report. *Available:http://www.symantec.com/publications/threatreport.jsp*, 18, 2013.

[2] S. Sonawane, G. Prasad, and S. Pardeshi. A survey on intrusion detection techniques. *World Journal of Science and Technology*, 2(3), 2012.

[3] M.H. Sazli and H. Tanrikulu. Saldiri tespit sistemlerinde yapay sinir aglarinin kullanilmasi. *XII. Turkiyede Internet Konferansi 8-10 Kasim 2007 Bildiriler Kitabi*, pages 217–225, 2007.

[4] O.K. Sahingoz and U. Oktay. Attack types and intrusion detection systems. *6th International Information Security Cryptology Conference*, 2013.

[5] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan. A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1):42–57, 2013.

[6] Michael Wooldridge. *An introduction to multiagent systems*. John Wiley & Sons, 2009.

[7] O.K. Sahingoz and A.C. Sonmez. Agent-based fault tolerant distributed event system. *Computing and Informatics*, 26(5):489–506, 2012.

[8] O.K. Sahingoz and N. Erdogan. A two-leveled mobile agent system for e-commerce with constraint-based filtering. In *Computational Science - ICCS 2004*, volume 3036 of *Lecture Notes in Computer Science*, pages 437–440. Springer Berlin Heidelberg, 2004.

[9] P. Jain, S. Raghuwanshi, and R.K. Pateria. New mobile agent-based intrusion detection systems for distributed networks. *International Journal of Wireless Communication*, 1(1), 2011.

[10] N. El Kadhi, K. Hadjar, and N. El Zant. A mobile agents and artificial neural networks for intrusion detection. *Journal of Software (1796217X)*, 7(1), 2012.

[11] Zhisong. Hou; Zhou. Yu; Wei. Zheng; Xiangang. Zuo. "Research on Distributed Intrusion Detection System Based on Mobile Agent" *Journal of Computers*. Aug2012, Vol. 7 Issue 8, p1919-1926, 2012

[12] S. Ganapathy, P. Yogesh, and A. Kannan. Intelligent agent-based intrusion detection system using enhanced multiclass svm. *Computational intelligence and neuroscience*, 2012:9, 2012.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)