IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

An Investigation of Multi-Agent System Model for Intrusion Detection/Prevention

Georgi Tsochev[1]

Faculty of Computer Systems and Technology, Technical University of Sofia, Sofia 1000, Bulgaria[1]

Abstract: Following ENISA's findings on the two main trends in Cyber Defence development over the past few years - adopting the philosophy and methods of Military Intelligence and introducing Artificial Intelligence into technologies for counteraction of cyber attacks was made research on the application of intelligent methods for increasing the security in computer networks. Penetration is defined as a set of actions to compromise the integrity, confidentiality, and availability of resources. This paper introduces a model for Intrusion detection/prevention system based on multi-agent systems. Results of simulation are presented and a comparison is made of the performance of the system compared to others.

Keywords: multi-agent systems, security, intrusion detection system, intrusion prevention system.

I. INTRODUCTION

At present, the networks are an essential component in our everyday life. Central to the entire discipline are the networks, which are crucial for delivering many services for people and businesses: web applications, IP communications, e-commerce and others [1]. The advent of the internet is a major concern and alongside with it is the security. Network security has become more important to personal computer users, organizations, and the military [2].
Security is crucial to networks and applications. While the network security is a critical requirement for the development of networks is a major disadvantage methods of protection that can be easily implemented [3]. There are many types of attacks and corresponding methods of protection.

TABLE I ATTACK METHOS AND SECURITY TECHNOLOGY [3]

Computer Security attributes	Attack Methods	Technology for internet Security
Confidentiality	Eavesdropping, Hacking, Phishing, DoS, IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec, SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, Hacking, Phishing, DoS, IP Spoofing	IDS, Firewall, Anti-Malware, Software, IPSec, SSL
Privacy	Email bombing, Spamming, Hacking, DoS, Cookies	IDS, Firewall, Anti-Malware, Software, IPSec, SSL
Availability	DoS, Email bombing, Spamming, System Boot Record Infectors	IDS, Firewall, Anti-Malware, Software, IPSec, SSL

An attack could be considered to be comprised of three phases, preparation, execution and post-attack. In the preparation phase, the attacker gathers information needed to loach the attack. The actual attack occurs in the execution phase. In the post-attack phase, the desired effects (including side effects) of the attack are observable [4].
With the pace of cyber-attacks, the human factor is not sufficient for timely analysis and action under attack . Human resources and lack of expertise were the main weakness of the organizations. The fact is that the intelligent agents carry out most network attacks, such as computer viruses and worms (Fig. 1). So fighting them can become smart semi-autonomous or fully autonomous agents that can detect, evaluate and respond with appropriate action for protection. [5]
These intelligent methods will need to be able to manage the whole process in response to an attack, i.e. to analyse and determine what type of attack happens, what is intended and what is the appropriate countermeasures, and not least how to prioritize and secondary prevention of attacks. It was in those difficult situations we need innovative approaches by applying methods of artificial intelligence.

Thus intrusion detection can be defined as technology to observe computer activities to prevent at preparation phase of the network attack. Intrusion detection is the process of identifying and responding to malicious activity targeted at computer and networking sources [6].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

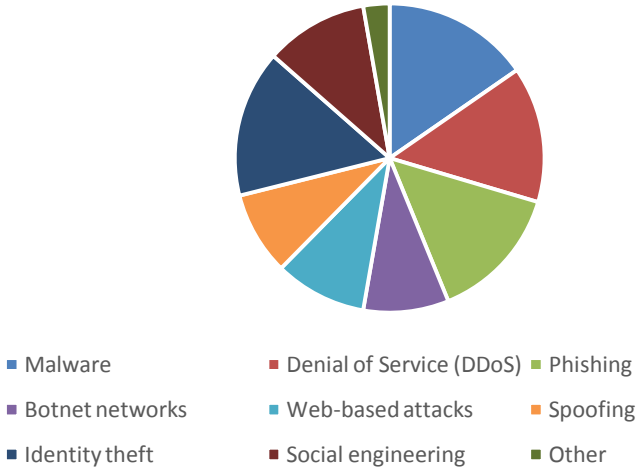

Fig. 1. Percentage of different attacks in 2015

II. METHODS OF ARTIFICIAL INTELLIGENCE IN NETWORK AND INFORMATION SECURITY

As mentioned in the introduction to this article, world practice has already noted a significant number of various "Artificial Intelligence" applications in computer security. Without trying for a comprehensive classification, we could divide these methods into two main directions:
A. Conditionally named "distributed" or "network" methods:
A1. Multi-Agent Systems of Intelligent Agents;
A2. Neural Networks;
A3. Artificial Immune Systems and Genetic Algorithms, etc;
B. Conveniently named "compact" methods:
B1. Machine Learning Systems, including associative methods, inductive logic programming, Bayes classification, etc.
B2. Pattern recognition algorithms;
B3. Expert Systems;
B4. Fuzzy logic, etc.
Having into account this variety of methods, it is of particular importance that adequate criteria are selected for the assessment and selection of a specific application for each specific solution.

III.RELATED WORKS

In line with the progress of multi agent-based systems, multiple intelligent intrusion detection systems apply them. Figure 2 shows that the results of proper detection using multi agent-based systems are constantly increasing as the percentage of false alarms drastically decreases. Undoubtedly, multi agent-based approaches can potentially reach increased flexibility, making them even more popular in the near future.

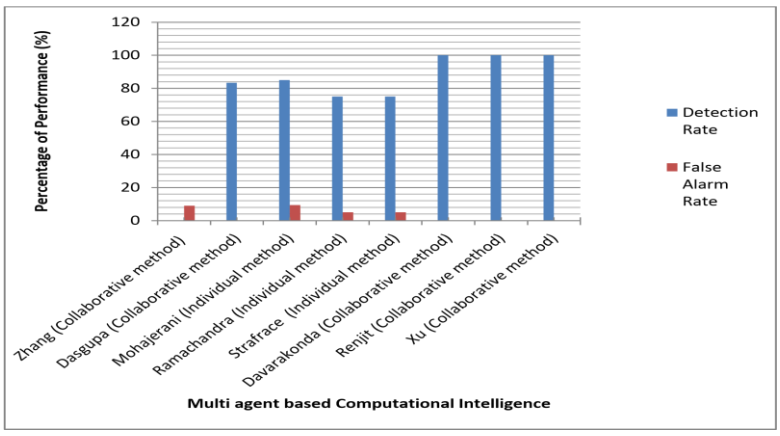

Fig. 2. Applications with multi-agent systems

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

IV. PROPOSED MODEL

The proposed model consists of two major multi-agent frameworks – host based monitoring system and network gateway monitoring system (partly based on rules). The two frameworks operate at different layers. The proposed system work is divided into five layers – network layer, system hardware, transport layer, data layer and system software.

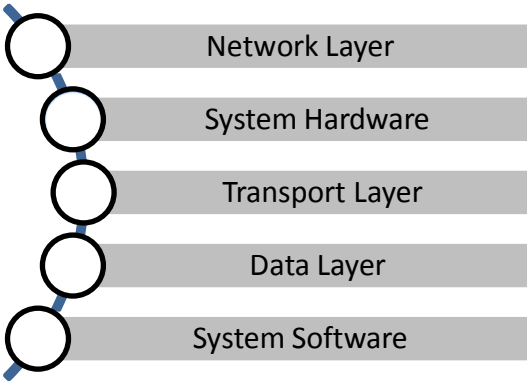

Fig. 3. Operating layers of the Proposed System

A. Host based monitoring system

The host based monitoring system (HBMS) is multi-agent framework installed on each host in the protected network. It works and monitors the Data Layer of the TCP/IP stack model and system software. The HBMS first task is to monitor the operating system resources and user activities, which can be target of potential attack of hackers. If there is a detected problem, an agent contacts the server if it is normal or not. Then the necessary actions are taken.

HBMS is similar to HP from NGMS, but two more features have been added - server help and alarm. If a question cannot be solved (for example, it is not possible to determine with accuracy whether a new process is a malicious code or not), a query is sent to the server. Sending the necessary information is done by the Host Advisory Agent User Mode Analysis and Detection Agent. The second additional function serves to alert other hosts to the network segment, to a problem that has occurred, and to the actions that have been taken.

Figure 4 shows the design of HBMS and the interactions of the agents.

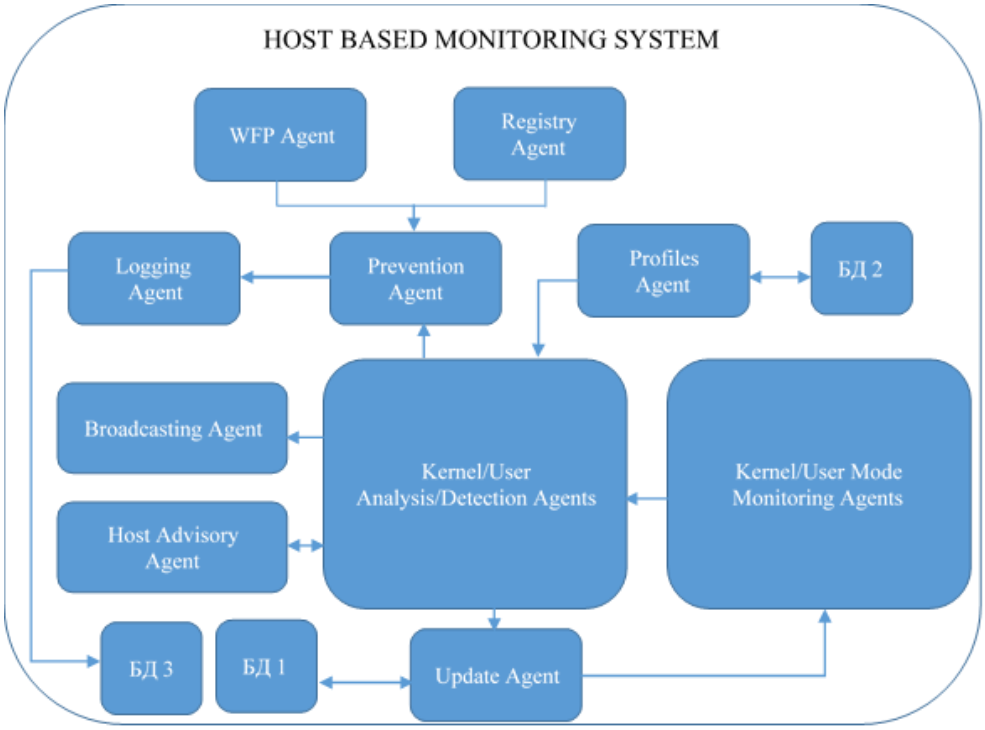

Fig. 4. Design of HBMS and agent interactions

DOI10.17148/IJARCCE.2017.6901

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

B. Network Gateway Monitoring System

The network gateway monitoring system (NGMS) is at the entry point of the internet traffic. At the server also is installed a host based monitoring system to monitor the server activity, because it can be a target of hacker. Besides that, NGMS operates at Network and Transport layer. The NGMS is a multi-agent framework which main function is detecting and preventing TCP/IP attack. It is focused on packets header.

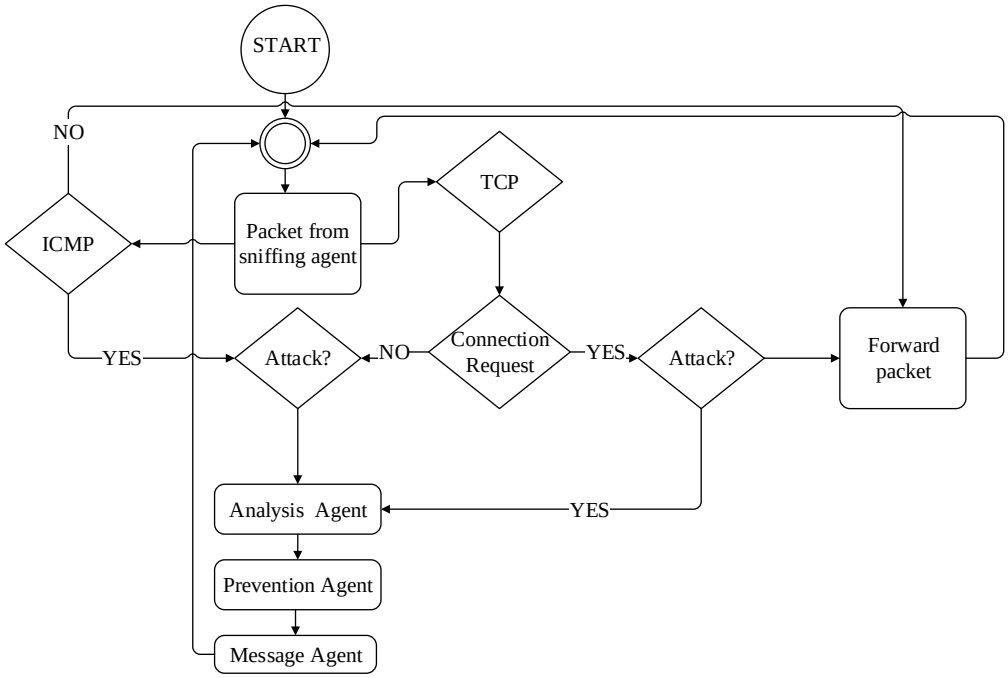

Fig. 5. NGMS flowchart

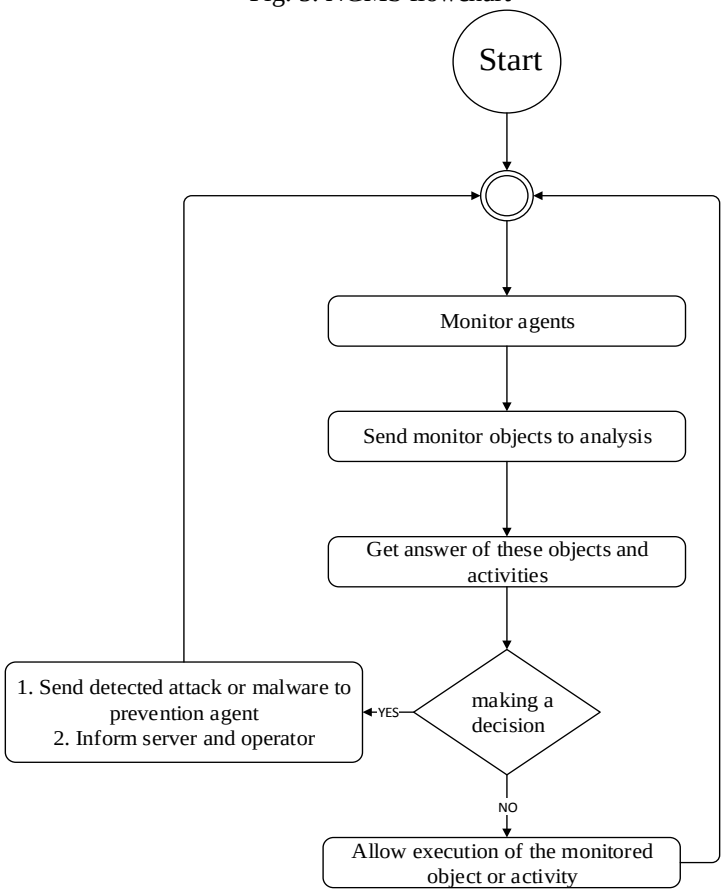

Fig. 6. HBMS flowchart

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

V. RESULTS

So far, simulations have been made with the host based network monitoring system. For attack system is used Kali [7], which is Linux distribution for penetration testing and security auditing.
The performance of the prototype has been tested in a network of 80 workstations, with each workstation having Intel core i5-4570 Processor, 3.20 GHz, 6MB cache, 4 cores/4 threads, 4 GB DDR3 RAM with 1333 MHz and Windows 7/XP. The data rate of the Ethernet was 1 Gbps between the hosts and the switch and 10 Gbps between the swetches. The variety number of active users were from 5 to 80 and the average load of the workstations was recorded. To test the workstation utilization by the agents, some attack ware simulated directly on them.
Based on the studies made on existing multi-agent-based methods of artificial intelligence, a mean percentage of their success was determined by applying each of the attacks listed in Table II. Figure 7 shows a comparative analysis of the success of the different methods.

TABLE II STATISTICS OF DETECTED INFILTRATIONS AND SYSTEM ATTACKS

Attack type	Software	Received packets	Found attacks	Time (sec)	Percent
Network Scan	Angry IP, HPING2, Ping Sweeps	3000	600	20.25	97%
Port Scan	Nmap, NetScan Tools Pro, IPScanner	3300	700	22.3	95%
Enumeration	SuperScan 4, enum, PsGetSid	2000	500	10	95%
Smurf Attack	Land and Latierra	500	400	15.5	97%
SYN Flooding	NemeSys	2000	2000	25.4	96%
Ping Flooding	Crazy Pinger	2000	400	25	96%
Session Hijacking	RST Hijacking Tools, Remote TCP Session Reset Utility	900	900	30	96.5%

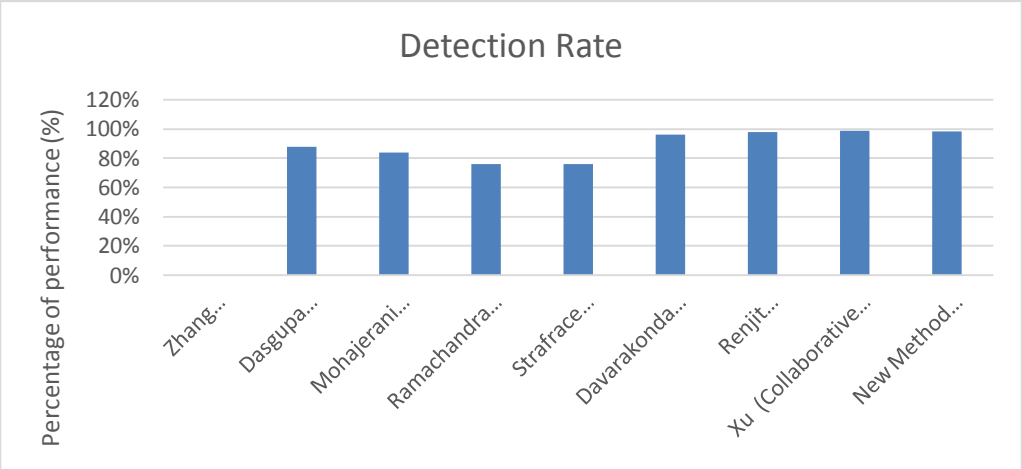

Fig. 7. Detection rate comparison

VI. CONCLUSION

Before creating a network security system, security experts need to define the security policy and the methods and technologies for the development of the system. These features allow to develop a system that is able to achieve its objectives with a high degree of efficiency and compatibility.

The proposed system speeds up the detection of attacks and malicious code that are targeted to the security system with high accuracy and real-time. The NP component manages to characterize the normal behavior of the TCP \ IP protocol and to detect the simplest attacks aimed at affecting the header of the packets. The HP component has proven its high

malware protection capability that affects Windows operating systems, whether the malicious code is in the kernel or focused on user activity.
The proposed system has some benefits like protection against attacks and malwares, eliminate false alarms, real-time detection, early attack detection, simple building, login and reporting.

ACKNOWLEDGEMENT

This research is funded in relation to the execution of a project BG05M2OP001-2.009-0033 "Stimulating modern scientific research through the creation of a scientifically innovative environment for the promotion of young researchers from the new generation at the Technical University of Sofia and the National Railway Infrastructure Company in the field of engineering and technical development". The project is implemented with the financial support of the Operational Programme “Science and Education for Smart Growth 2014 - 2020”, co-financed by the European Union through the European Social Fund and the European Regional Development Fund.

REFERENCES

[1] R. Graziani and A. Johnson, Routing protocols and concepts, Indianapolis: Cisco Press, 2008.
[2] "Network Security: History, Importance, and Future," [Online]. Available: http://www.alphawireless.co.za/the-history-importance-and-future-of-network-security/.
[3] O. Adeyinka, "Internet Attack Methods and Internet Security Technology," in AICMS'08, 2008.
[4] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P Anderson Co, Fort Washington, Pennsylvania, 1980.
[5] B. Rebecca, "An Introduction to Intrusion Detection & Assessment," ICSA Inc, 1998.
[6] P. Saini and S. Godara, "Modelling Intrusion Detection System using Hidden," International Journal of Advanced Research in Computer Science and Software Engineering, pp. 542-547, 2014.
[7] "https://www.kali.org/," [Online]. Available: https://www.kali.org/.

BIOGRAPHY

Mag. Eng. G. Tsochev is a Ph.D. student at the Technical University of Sofia and has experience as system and network administrator. His fields of research are network and information security, intelligent angents.