SOME SECURITY MODEL BASED ON MULTI AGENT SYSTEMS

Georgi Tsochev
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, Bulgaria
gtsochev@tu-sofia.bg

Roumen Trifonov
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, Bulgaria
r_trifonov@tu-sofia.bg

Radoslav Yoshinov
Laboratory of Telematics
Bulgarian Academy of Sciences
Sofia, Bulgaria
yoshinov@cc.bas.bg

Slavcho Manolov
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, Bulgaria
slav1943@gmail.com

Georgi Popov
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, Bulgaria
popovg@tu-sofia.bg

Galya Pavlova
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, Bulgaria
raicheva@tu-sofia.bg

***Abstract*— Computer security is defined as the protection of computer systems against threats to confidentiality, integrity and availability. Penetration is defined as a set of actions to compromise the integrity, confidentiality, and availability of resources. To monitor the events that occur in computer systems or networks is called intrusion detection system (IDS). This paper introduces a model for IDS based on multi-agent systems and artificial intelligence.**

Keywords— multi-agent systems, artificial intelligence, network and information security, intrusion detection system, intrusion prevention system

I. INTRODUCTION

At present, the computer networks and information systems are an essential component in our everyday life. Central to the entire information and communication infrastructure are the computer networks which are crucial for delivering many services for people and businesses: web applications, IP communications, e-commerce and others information society service [1]. The advent of the Internet is a major concern and alongside with it is the network and information security. Network and information security has become more important to personal computer users, different organizations, and the military also.

Network and information security is crucial to computer networks and software applications. While the network security is a critical the requirement for the development of computer networks is a major disadvantage the methods of protection that can be easily implemented [2], [10]. There are many types of attacks and corresponding methods of protection (Table 1).

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.

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 [3].

The Faculty of Computer Systems and Control at Technical University of Sofia began research on the application of intelligent systems for network and computer security. During the study, was made a survey of the various intrusion detection systems. This paper introduces a model for IDS based on multi-agent systems and artificial intelligence and some of the results achieved by this model.

TABLE I. ATTACK METHODS AND SECURITY TECHNOLOGY [2]

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

II. INTRUSION DETECTION AND PREVENTION SYSTEMS

Intrusion Detection System (abbreviated as IDS) is a security system that detects hostile activity on the network. The key is then to detect and possibly prevent actions that could jeopardize the security of the system, or attempt to break in the work, including the phases of exploration / collection of

data that include, for example, a port scan. One of the key features of intrusion detection systems is their ability to provide a view of the unusual activity and issue alarms notifies administrators and / or block the connection of the suspect.

A. Components

The typical components in an IDPS are sensor or agent, management server, database server and console [4].

Sensors and agents monitor and analyze activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies [9], [11].

A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

A database server is a repository for event information recorded by sensors, agents, management servers. Many IDPSs provide support for database servers.

A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

B. Functions

IDS consist of four major elements – data collection, feature selections, analysis and action.

The data collection is a file in which is recorded the data that should be analyzed. In rule based IDS the analysis is done by checking the data of compare it to a signature or pattern. Another method is anomaly based. The action defines the attack and reaction of the system.

III. 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 (Fig. 1) – network layer, system hardware, transport layer, data layer and system software.

Identify applicable funding agency here. If none, delete this text box.

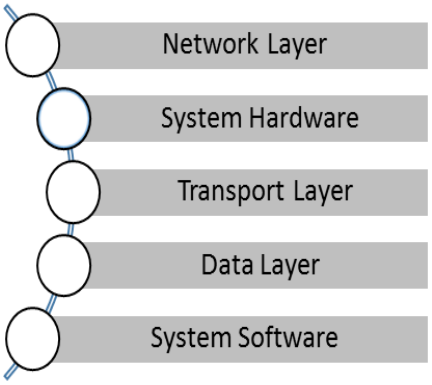

Fig. 1 Operating layers of the Proposed System

The host based monitoring system (HBMS) is multi-agent framework installed on each host in the protected network.

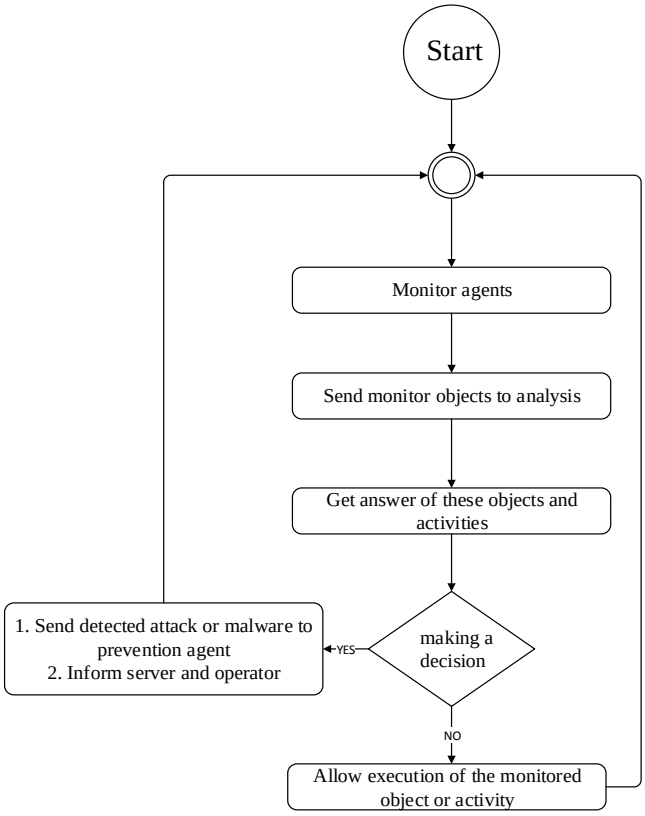

Fig. 2 HBMS flowchart

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. The flowchart of how the packets are being checked is shown in Fig. 2.

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. The process showing of how NGMS is working is shown in Fig. 3.

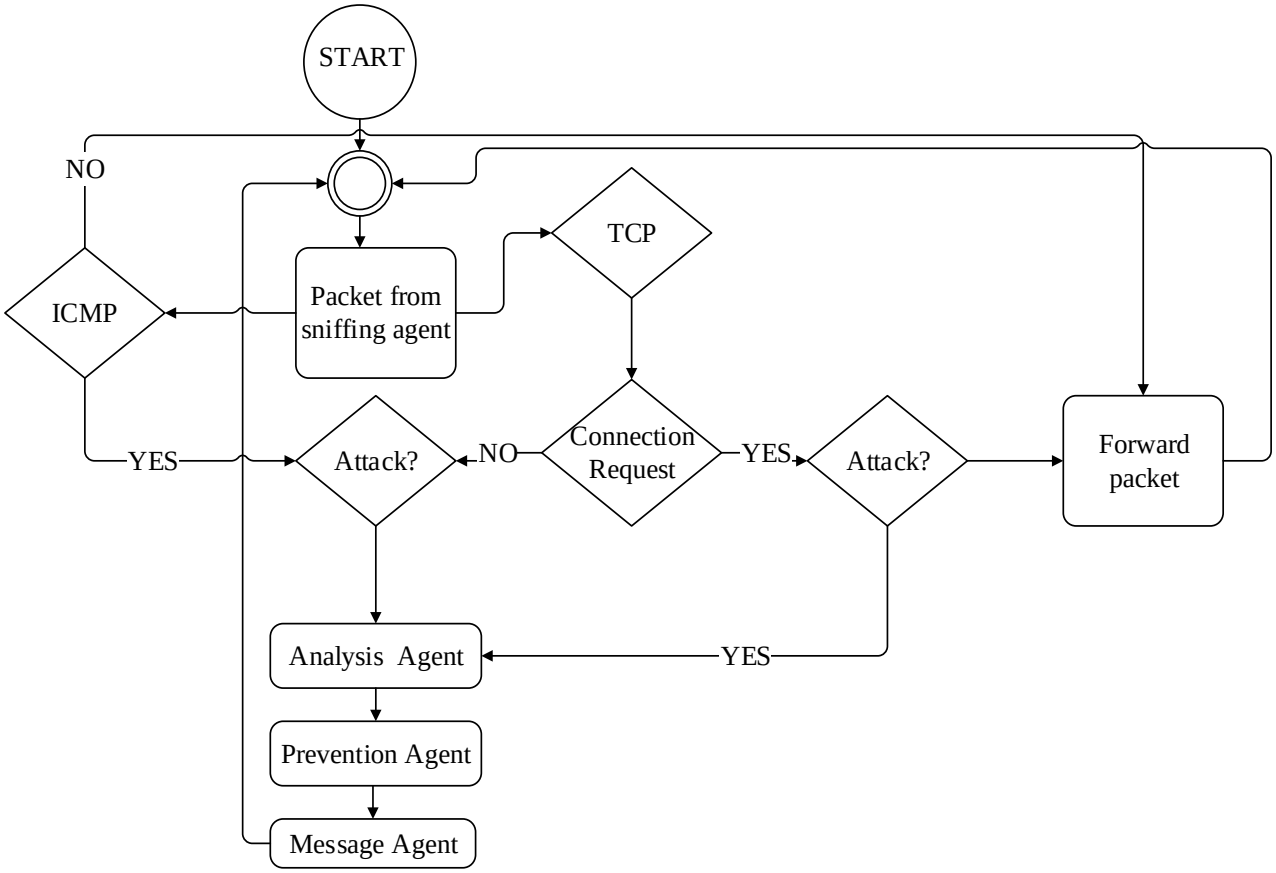

Fig. 3 NGMS flowchart

IV. RESULTS

So far simulations have been made with the host based network monitoring system. For attack system is used Kali [8], which is Linux distribution for penetration testing and security auditing.

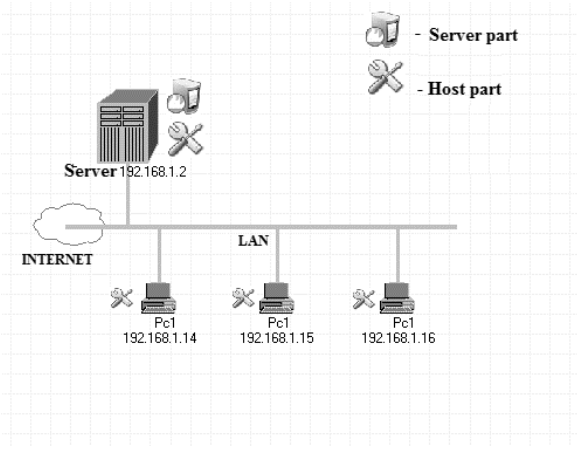

Fig. 4 Network topology used for simulation

The performance of the prototype has been tested in a network of 40 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 100 Mbps. The variety number of active users were from 5 to 40 and the average load of the workstations was recorded. To test the workstation utilization by the agents, some attack ware simulated directly on them. The results of the performed test are shown in Table 2.

TABLE II. RESULTS

Attack type	Detection Rate (%)	False Positive(%)
DoS/DDoS	75.25	22.25
Malicious code	62.85	25.22
Probe/Scanning	68.28	24.87
Normal	75	19.31

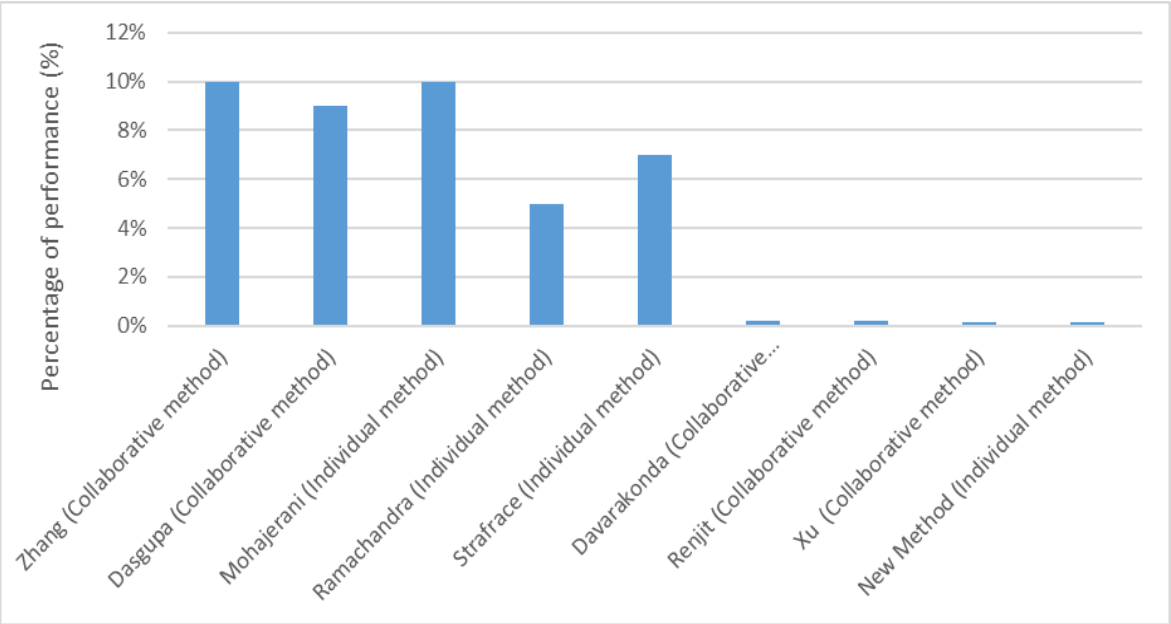

Fig. 5 False alarm rate comparison

The False alarm rate comparison (Fig. 5) is not fully accurate, because so far our system is not fully implemented, compared to the other models. Currently the team is working on a hybrid version of the NGMS, to reinforce the multi agent system with Q-learning algorithm. This will lead to more accurate precision of the false positive alarms.

V. 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 has some benefits like protection against attacks and malwares, eliminate false alarms, real-time detection, early attack detection, simple building, login and reporting.

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.

The next step is to implement the network gateway monitoring system. When this is done will be made a larger class of security attacks. The results will be summarized to show is the complete system better than some of the currently existing schemes.

ACKNOWLEDGMENT *(Heading 5)*

This research is conducted and funded in relation to the execution of a scientific-research project № H07/56 “Increasing the level of network and information security using intelligent methods” under the contract with National Science Fund in Bulgaria.

REFERENCES

[1] Graziani, R., & Johnson, A. (2008). Routing protocols and concepts. Indianapolis, IN 46240 USA: Cisco Press.

[2] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008.AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

[3] J.P.Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.

[4] Mell, P., & Scarfone, K. “Guide to Intrusion Detection and Prevention Systems.” NIST Special Publication 800-94. 2007. NIST. 9 June 2008

[5] “Host- vs. Network-Based Intrusion Detection Systems”, SANS Institute 2000 - 2005

[6] [6] Bace, Rebecca: An Introduction to Intrusion Detection & Assessment. Infidel Inc., prepared for ICSA Inc. Copyright 1998.

[7] Chapter 8 Cisco Network-Based Intrusion Detection—Functionalities and Configuration

[8] https://www.kali.org/

[9] Tsochev G., R. Trifonov, G. Naydenov. Agent communication languages comparison: FIPA-ACL and KQML. 7th International Scientific Conference COMPUTER SCIENCE'2015, 08-10 September 2015, Durres, Albania, ISBN: 978-619-167-177-9

[10] Tsochev G., R. Trifonov, R. Yoshinov, Multi-agent framework for intelligent networks, 29th International Conference on Information

Technologies (InfoTech-2015), 17-18 September 2015 Varna – St. St. Constantine and Elena resort, Bulgaria, ISSN: 1314-1023

[11] Trifonov R., S. Manolov, G. Tsochev, Application of multi-agent systems for network and information protection, 28th International Conference on Information Technologies (InfoTech-2014), 18-19 September 2015 Varna – St. St. Constantine and Elena resort, Bulgaria, ISSN: 1314-1023

[12] Scarfone K., Mell P., GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

[13] http://shodhganga.inflibnet.ac.in/bitstream/10603/34783/12/12_chapter3.pdf