Prototype of security system based on multi-agent architecture

G. Tsochev, R. Trifonov, G. Popov, R. Yoshinov, Sl. Manolov, G. Pavlova

***Abstract*—**The technology of intrusion detection systems in computer networks is quite young and dynamic. Today in this area there is an active formation of the market. Currently, intrusion detection systems (IDS) are becoming increasingly common among companies of various sizes. However, unfortunately, these systems, designed to identify and repel attacks by hackers, can themselves be exposed to unauthorized influences that could disrupt the system's performance, which would prevent it from fulfilling its tasks. The present paper describes some of the results obtained in the Faculty of Computer Systems and Technology at Technical University of Sofia in the implementation of project related to the application of intelligent methods for increasing the security in computer networks. The paper introduces a model for IDS where multi agent systems and artificial intelligence are applicable by the means simple real-time models constructed in laboratory environment.

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

I. Introduction

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). 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]. That’s why according to the vast majority of experts, the qualitative transition to new Cyber Defense tools must involve the widespread use of Artificial Intelligence methods to analyze information exchanged, network flows, sources of threats, and to plan effective impact measures, including proactive ones.

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.

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.

Georgi Tsochev is a Ph.D. student at the Technical University of Sofia
Rumen Trifonov is a lecturer at the Technical University of Sofia. He is a head of department “Information Technologies in Industry.

Georgi Popov is with the Technical University of Sofia

Radoslav Yoshinov is with the Laboratory of Telematics at the Bulgarian Academy of Sciences.

Slavcho Manolov works at the Technical University of Sofia.

Galya Pavlova is with the Technical University of Sofia.

The Faculty of Computer Systems and Technologies 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 AND INTELLIGENT AGENTS

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]. Agents can be defined to be autonomous, problem-solving computational entities capable of effective operation in dynamic and open environments [24]. Agents are often deployed in environments in which they interact, and may be cooperate, with other agents (including both people and software) that have possibly conflicting aims. Such environments are known as multi-agent systems. Agents can be distinguished from objects (in the sense of object oriented software) in that they are autonomous entities capable of exercising choice over their actions and interactions. Agents cannot, therefore, be directly invoked like objects. However, they may be constructed using object technology.

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 consists 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

Multi-agent-based technologies have been used to design and implement the proposed system due to the fact that they are developing rapidly in the field of network applications. Behavior analysis and detection techniques were also used in the analysis and detection modules in the proposed system. Behavioral techniques serve to compare the behavior of objects with a predefined normal profile of behavior. Then they discover deviations from normal and treat it as malicious behavior.

Building a normal profile requires a lot of training to train the system to get a clean "snapshot" of a single object. The proposed system is installed in a clean system that is completely free from all sorts of threats. This means that machines have been prepared that do not have access to the Internet at an early stage so that the proposed system can build the profiles of the sites of protection by taking a real "picture" of the attributes of the site. Once the normal profiles are built, the system is connected to the Internet

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. Layers can be merged according to their intended purpose. The first three network, system hardware, transport are grouped together in the TCP / IP stack area, and transport, data, operating system level software (Operating System). As you can see, the transport level is involved in both groups due to the fact that it has an important dual character.

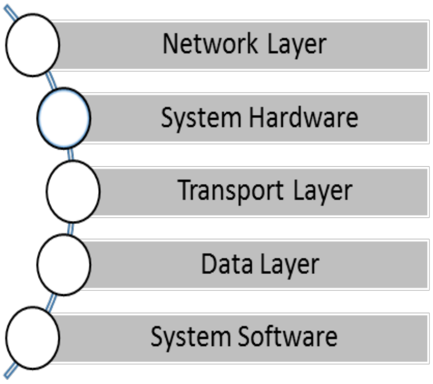


Fig. 1 Operating layers of the Proposed System

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

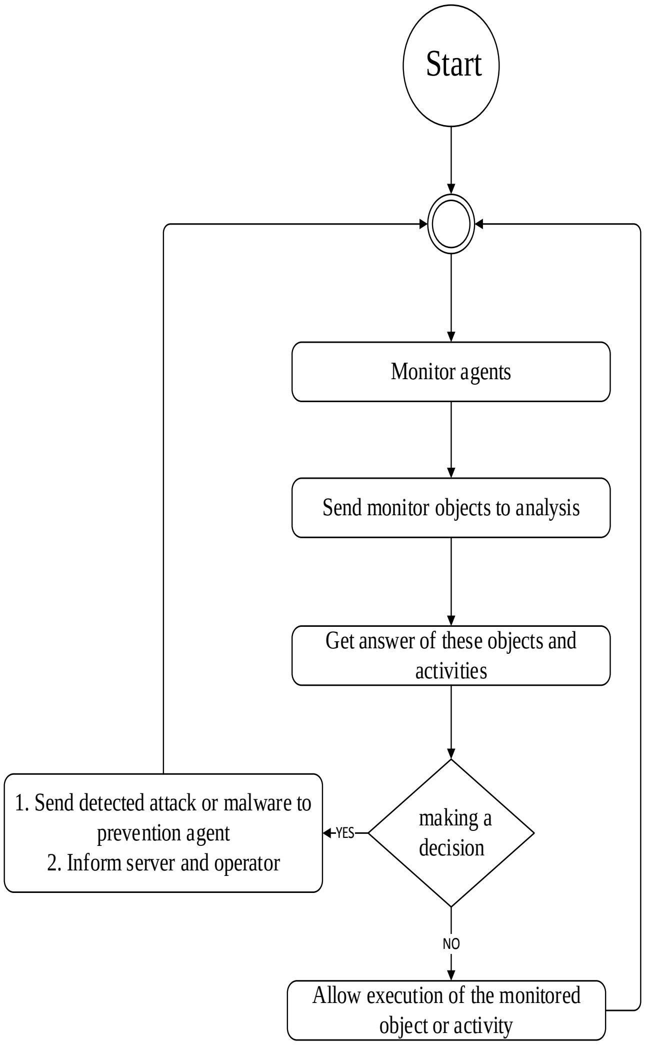

Start
Monitor agents
Send monitor objects to analysis
Get answer of these objects and activities
making a decision
YES
1. Send detected attack or malware to prevention agent
2. Inform server and operator
NO
Allow execution of the monitored object or activity

Fig. 2 HBMS flowchart

It works and monitors the Data Layer of the TCP/IP stack model and system software. As mentioned, many organizations use encryption or similar techniques to conceal the basic information in the body of the package. In this case, the malicious code is hidden and will only be executed when it reaches the corresponding service that encrypted it. In its execution, the machine will be compromised. To prevent this scenario happening, the HBMS is built to monitor the internal processes of the OS or the user's activities. 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. At the end if the attack is new to the system is serves to alert other hosts to the network segment, to a problem that has occurred, and to the actions that have been 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. As already mentioned, NGMS is a multi-agent software framework that consists of two parts - Network Prevention (NP) and Host Prevention

(HP). Its main function is to detect and prevent TCP / IP attacks and malware in the OS kernel or user activities. It works on the network interface that is external to the server. Its work begins with Sniffing Agent Traffic Tracking, which communicates with the TCP / IP Stack Connector (tcpip.sys) kernel driver. Due to the fact that the machine itself has some OSs and different service facilities installed on it, only network monitoring is not enough. 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 focuses on the header of the packets rather than on the information in the package as its inspection is a longer process and will take longer and in many cases will not yield useful results due to the fact that most hackers use clever techniques to hide real data. The NP component focuses on the header of the packets rather than on the information in the package as its inspection is a longer process and will take longer and in many cases will not yield useful results due to the fact that most hackers use clever techniques to hide real data. In addition, most organizations use encryption techniques to hide the data actually transferred over the Internet. The proposed system inspected the header to detect traces of penetration of the first two stages of the life cycle of one or more attacks. The process showing of how NGMS is working is shown in Fig. 3. Some of the protection actions can be one of the following:

•Dropping a bundle
•Blocking
•End the TCP connection
•Record.

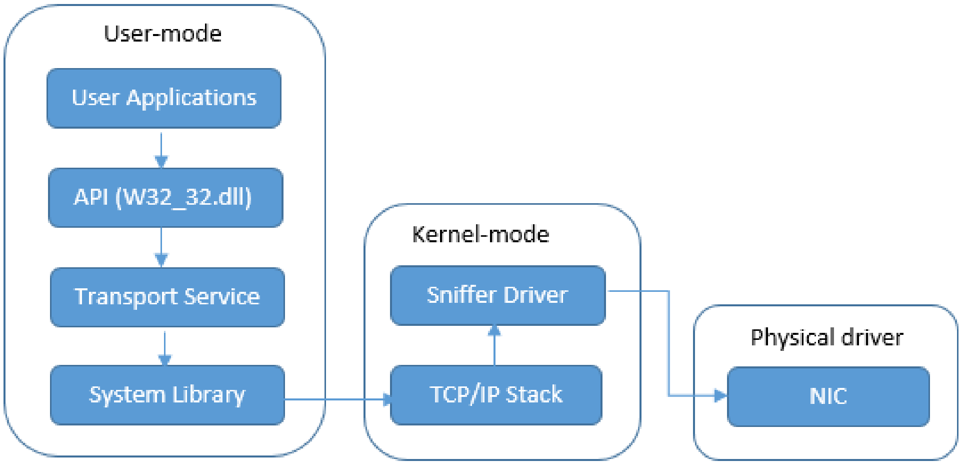


Fig. 3 HBMS component

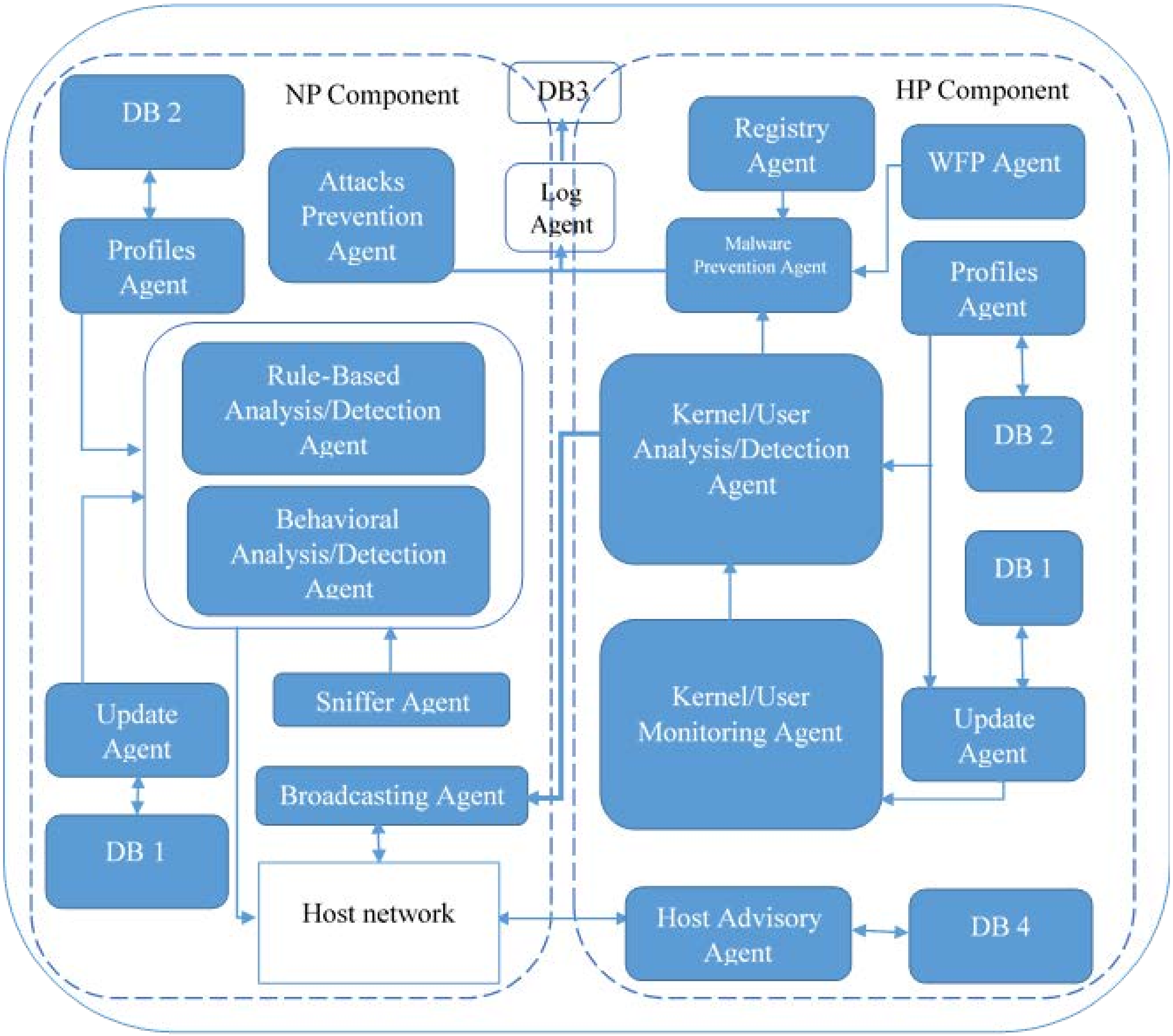


Fig. 2 NGMS flowchart

IV. Results

The goal of the proposed system is to protect network servers, the Internet access point (separate server), and individual hosts against attacks and malware without relying on any database structure with ready-made signatures. The proposed system works in the Microsoft Windows environment and protects the critical operating system objects. It also protects network-level protocols, especially TCP, ICMP, and UDP. The TCP / IP protocol has a number of vulnerabilities and vulnerabilities that are often used by hackers to perform DoS attacks, session hijacking, and more. UDP-enabled services can transfer data without an established connection and send data for multiple computers in one packet. This can affect a network with multiple vulnerabilities. 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.

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

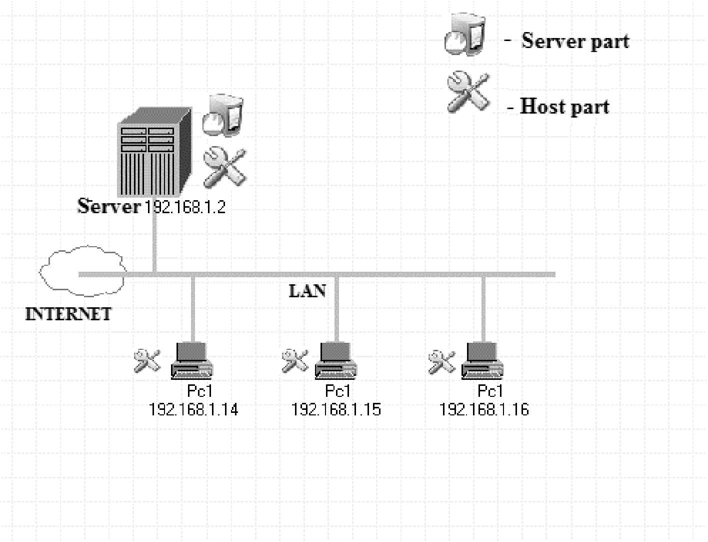
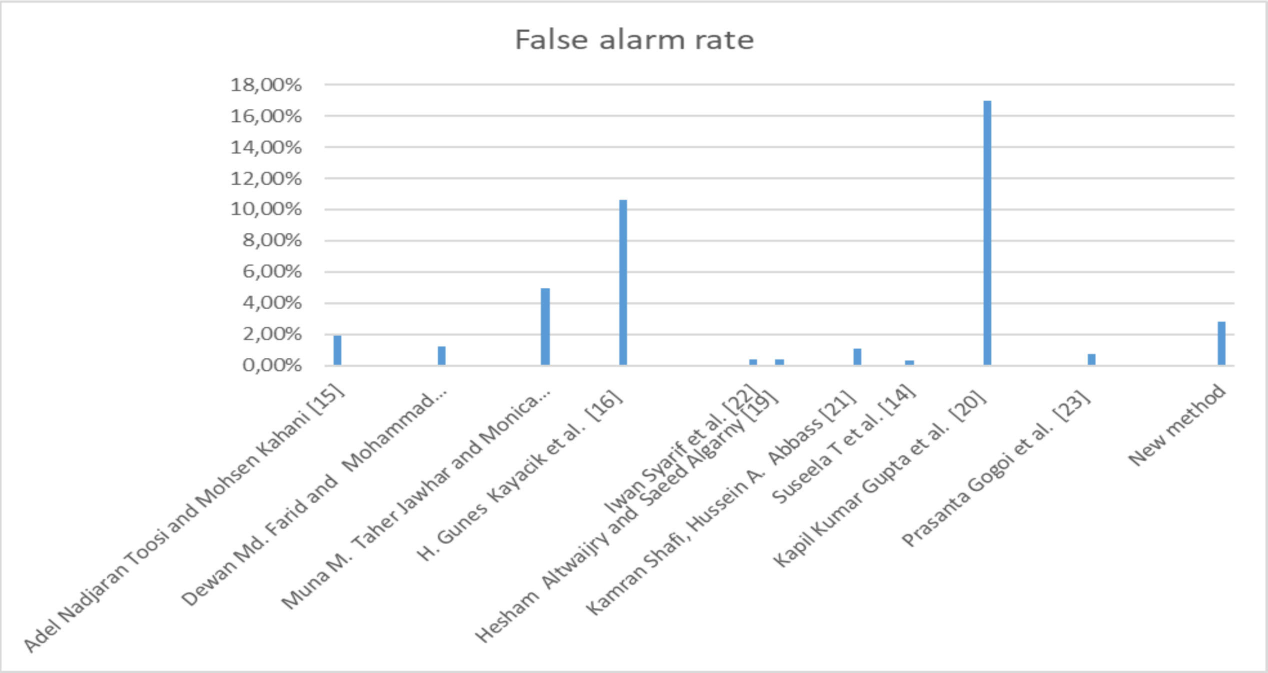


Fig. 3 Network topology used for simulation



V. CONCLUSION

When designing agent systems, it is impossible to foresee all the potential situations an agent may encounter and specify behavior optimally in advance. Agents must therefore learn from, and adapt to, their environment. This task is more complex when the agent is situated in an environment that contains other agents with different (and in many cases unknown) capabilities, goals, and beliefs. Multi-agent learning, (the ability of agents to learn how to communicate, cooperate, and compete) becomes crucial in such domains. Learning is increasingly being seen as a key quality of agents, and research into learning agent technology, such as reinforcement learning and genetic algorithms, is now being carried out across Europe. Applications of learning agent technology have been especially successful in the areas of personalization and information retrieval, and promising results have been achieved in the areas of robotics and telecommunications. 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.

Future work includes building misuse detection components, the decision module, additional machine learning components, and a graphical user interface for the system. The future improvements on this research could be done on implementing the prototype in Mobile Ad Hoc Networks.

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

[14] Suseela T. Sarasamma, Qiuming A. Zhu, and Julie Huff "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Transactions on Systems, Man, And Cybernetics-Part B: Cybernetics, Vol. 35, No. 2, April 2005.

[15] Adel Nadjaran Toosi, Mohsen Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," Computer Communications vol.30, pp.2201–2212, 2007.

[16] H. Gunes Kayacik, A. Nur Zincir-Heywood, Malcolm I. Heywood," A Hierarchical SOM based Intrusion Detection System, "Engineering Applications of Artificial Intelligence,Vol.20,no.4, pp.439-451,June 2007.

[17] Dewan Md. Farid, Mohammad Zahidur Rahman, "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm," Journal of Computers, Vol. 5, No. 1, January 2010.

[18] Muna M. Taher Jawhar and Monica Mehrotra, "Anomaly Intrusion Detection System using Hamming Network Approach," International Journal of Computer Science & Communication,Vol. 1, No. 1, pp. 165-169, January-June 2010.

[19] Hesham Altwaijry, Saeed Algarny," Bayesian based intrusion detection system," Journal of King Saud University, Computer and Information Sciences, 2010.

[20] Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri,"Layered Approach Using Conditional Random Fields for Intrusion Detection,"IEEE Transactions On Dependable And Secure Computing, Vol. 7, No. 1, January-March 2010.

[21] Kamran Shafi, Hussein A. Abbass, "Evaluation of an Adaptive Genetic-Based Signature Extraction System for Network Intrusion Detection, "Pattern Analysis and Applications, November 2011.

[22] Iwan Syarif, Adam Prugel-Bennett, Gary Wills, "Unsupervised clustering approach for network anomaly detection," Fourth International Conference on Networked Digital Technologies, 24 - 26 Apr 2012.

[23] Prasanta Gogoi, Monowar H Bhuyan, D K Bhattacharyya, and J K Kalita,"Packet and Flow Based Network Intrusion Dataset," Contemporary Computing Communications in Computer and Information Science, vol.306, pp.322-334, 2012.

[24] Michael Luck, Peter McBurney, Christ Preist Agent Technology: Next Generation Computing AgentLink II, January 2003

mag. eng. Georgi 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 agents.

Prof. Rumen Trifonov - is a lecturer at the Technical University of Sofia. He is a head of department "Information Technologies in Industry. His fields of research are artificial intelligence, systems and information security, e-government.

Assoc. prof. Georgi Popov - is a lecturer at the Technical University of Sofia. His fields of research is systems security.

Assoc. prof. Radoslav Yoshinov - is Director of Laboratory of Telematics at the Bulgarian Academy of Sciences. Research in the field of telecommunications, computer networks, Modelling and creation of heterogeneous, distributed network education environments for e-learning.

Assoc. prof. Slavcho Manolov - works at the Technical University of Sofia. He has experience and research publications in the field of: Electronic Governance; System Integration and Interoperability; Network and Information Security.

Assist. prof. Galya Pavlova - is a PhD student at the Technical University of Sofia. Her fields of research application of artificial intelligence methods in robotics, machine learning and data mining, information security.