Impact Factor: 9.9 ISSN-L: 2544-980X

THE NEED AND IMPORTANCE OF USING ANTIVIRAL DEFENSE SYSTEMS BASED ON ARTIFICIAL IMMUNE SYSTEMS

Umarov Shukhratjon Azizjonovich[1], Umarova Munojatkhon Ibragimovna[2], Kayumova Mohinur Abduvahob kizi[3]

[1]Associate Professor of the Department of "Software Engineering and Cybersecurity" Fergana State Technical University, sh.umarov81@mail.ru

[2]Secondary school No. 2 with in-depth study of individual subjects, Fergana city

[3]10th grade student of the 6th general secondary school in the city of Fergana

Abstract: This article describes the use of artificial immune systems in creating anti-virus protection systems, the architecture and model of this system. Systems based on the idea of creating a "honeypot" - a small network for detecting and eliminating network viruses are analyzed in detail and comparative tables are given. Theoretical data and experiments show that such systems can be more effective when integrated into IDS/IPS, especially when used in conjunction with an artificial immune system.

Keywords: information security, artificial immune system, antivirus patch generator, Cybersecurity, network virus, virus signature, machine learning, cyberattack.

Introduction

In recent years, along with the rapid development of information technologies, cyberattacks and virus epidemics have become widespread. Experts say that over the past ten to fifteen years, the number of computer virus attacks aimed at both corporate networks and individual users has increased sharply. Various types of viruses are known (computer worms, macro viruses, polymorphic viruses, rootkits, Trojans, etc.). According to statistics, on average, a new malicious program appears every 15 seconds. A whole industry of creating and distributing malicious programs through attacks from botnets (Criminal-to-criminal, C2C) has emerged. Despite the enormous efforts of competing antivirus companies, computer viruses cost hundreds of millions of dollars every year. The explanatory dictionary of computer science gives the following definition of a virus [1]: computer viruses are a class of programs that are capable of self-replication and self-modification in a working computing environment and cause undesirable behavior for the user. These actions can be expressed in disrupting the operation of programs, displaying extraneous messages or images on the screen, damaging records, files, disks, slowing down the computer, etc.

Most modern antivirus packages use signature analysis methods to combat viruses. At the same time, some developers, trying to increase the efficiency of their products, release several updates of signature databases every hour. However, frequent signature updates and constant scanning of computers by antivirus systems for malicious code lead to a decrease in the performance of protected information systems, since antiviruses use large resources of RAM and processor time.

Materials and methods

Traditional antivirus and IDS (Intrusion Detection System) tools are often designed to react after an attack and are not sufficiently effective against real-time threats [2]. In recent years, heuristic methods have been increasingly used to develop mechanisms for detecting new and unknown computer

Impact Factor: 9.9 ISSN-L: 2544-980X

viruses. Thus, the Bloodhound Heuristic technology used in the Norton Antivirus package (Symantec) studies the structure of files, program logic, instructions, file information and other attributes, after which it determines the likelihood of infection based on heuristic rules. "Clean" files pass through this filter without hindrance, while suspicious files are delayed. Using this technology allows you to automatically detect and neutralize up to 95% of all viruses [3].

Artificial immunity models based on the principles of the human immune system are an important innovative solution to solving such problems. One of the promising areas in the field of creating anti-virus protection systems that can detect new and unknown viruses and effectively eliminate them is the use of artificial immune system technologies [4, 5]. Such systems have the ability to detect attacks early, analyze them, self-adapt and distribute protection throughout the network. Thus, IBM presented a working model of the Immune System for Cyberspace (KIT) at the Virus Bulletin '97 conference in San Francisco, USA. Anti-virus protection algorithms protected by a number of patents and implemented as part of this system were used (Fig. 1).

According to this structure, the immune system for cyberspace should provide the following functions:

- detection of an unknown virus on the user's computer;¬

- isolation of the virus and its transmission to the central computer;

- automatic analysis of the virus and generation of instructions for its detection and removal from any machine connected to the network;

- delivery of the order to the user's computer, integration into its anti-virus databases and launch the program for detecting and deleting all copies of the virus;

- distribution of anti-virus programs on the user's local network.

The well-known American RAND Corporation, commissioned by the Department of Defense, conducted research in the field of selecting technologies capable of providing the necessary level of information security for the national information infrastructure of the United States. Technologies for creating artificial immunity systems were selected as the most promising technologies for creating new generation information security systems.

Impact Factor: 9.9 ISSN-L: 2544-980X

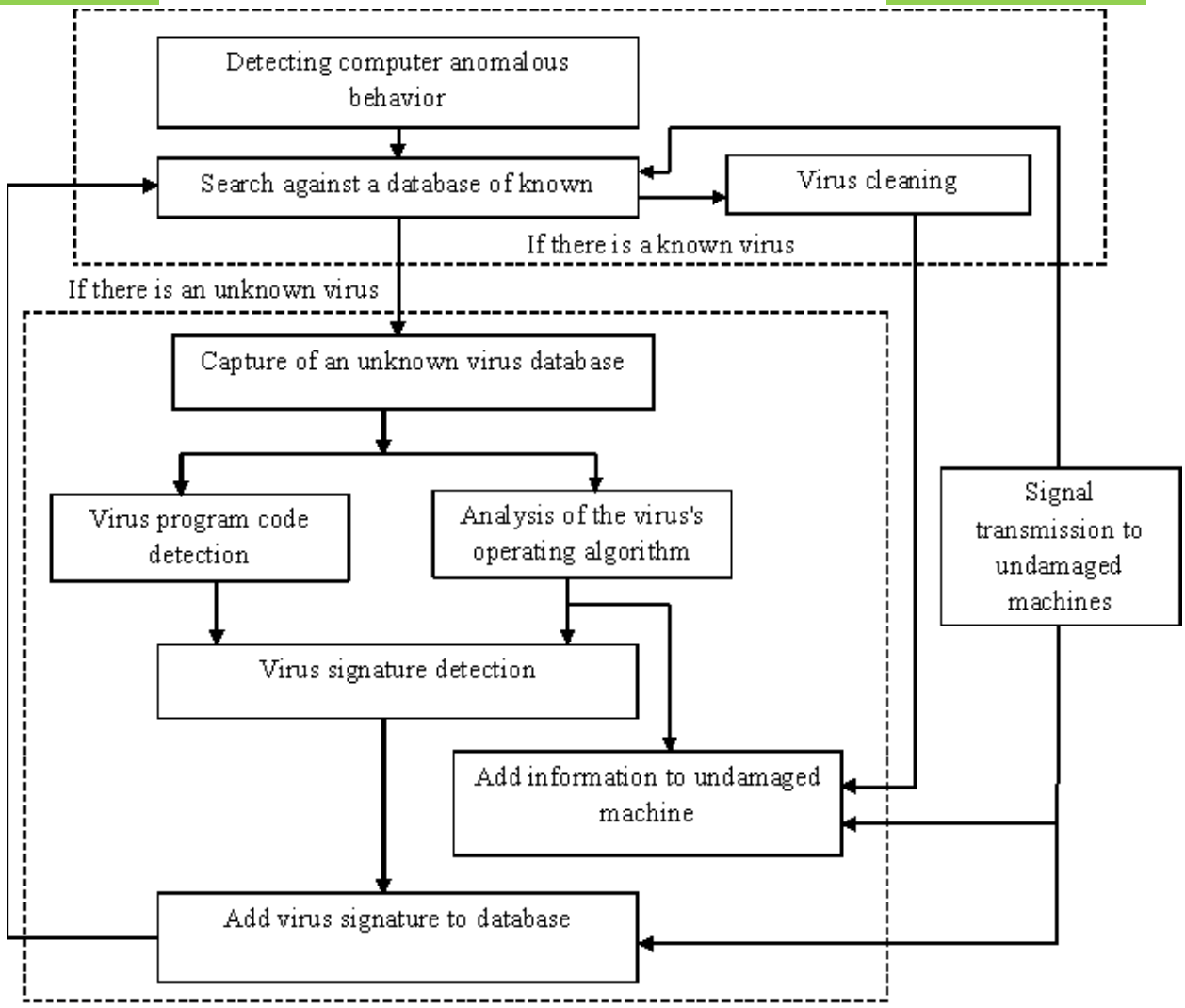

Figure 1. Structural diagram of the immune system for cyberspace

Discussion and results

In the State of Israel, an immune system for computers has been developed that can successfully combat virus epidemics on the Internet. The system is based on the idea of creating a small network of "honeypot" computers on the Internet. The main goal of this method is to detect and analyze viruses or malicious programs early and protect the entire network from them. The system is based on the concept of "computer immunity", which is to introduce the ability to recognize and respond to threats at the computer network level. Specially vulnerable or weakened computers (honeypots) connected to the Internet are created. These computers attract viruses, malicious programs and cyberattacks from the environment. This system automatically analyzes viruses on the computers that are attracted to it and distributes protective equipment throughout the network. The "honeypots" must be interconnected by separate secure channels. If an attack is detected on one of the "honeypots", the others are immediately notified and begin to act as centers for distributing neutralization code (Fig. 2).

The model consists of the following 4 main parts:

- Honeypot network - virtual computers that attract attacks;
- Analysis module - threat detection using artificial intelligence and IDS tools;
- Antivirus patch generator - generation of protection codes;
- Real network computers - protected user equipment

Impact Factor: 9.9
ISSN-L: 2544-980X

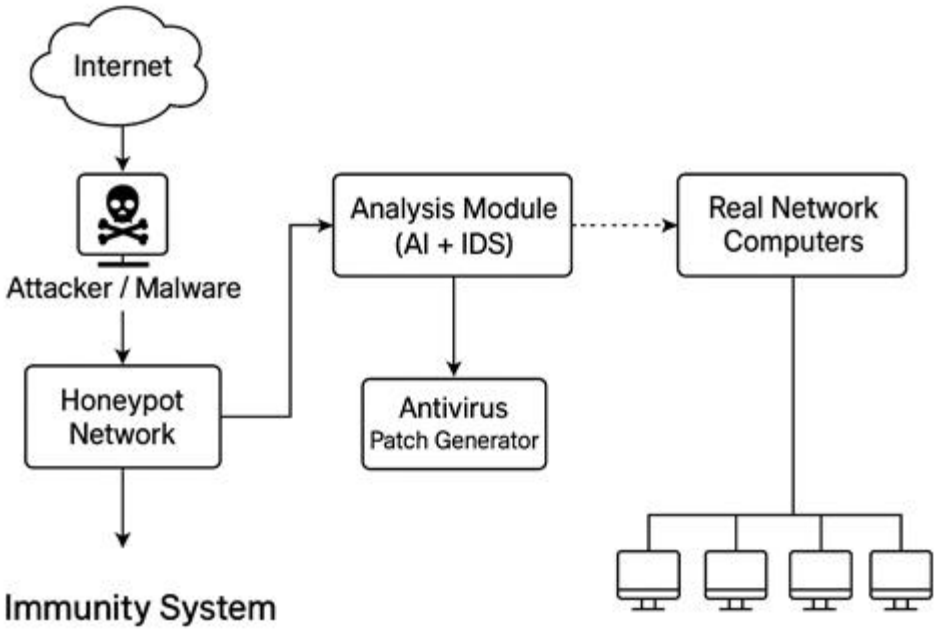

Figure 2. Honeypot-based artificial immune system model

When an attacker sends a virus or malware to a honeypot network over the Internet, this information is passed to the analysis module. It classifies the virus, automatically creates an antivirus patch, and distributes it to real network computers.

Application of the SEIR model to model virus spread in the immune system:

$$\frac{dH}{dt} = -\beta HZ ,$$

$$\frac{dY}{dt} = \beta HZ - \sigma Y ,$$

$$\frac{dZ}{dt} = \sigma Y - \gamma Z ,$$

$$\frac{dI}{dt} = \gamma Z ,$$

bu yerda H - “tuzoq” himoyasiz kompyuterlar, Y - virus bilan aloqada bo‘lgan, lekin zararlanmagan kompyuterlar, Z - zararlangan kompyuterlar, I -immunitet hosil qilgan kompyuterlar. β - virusning tarqalish koeffitsienti, σ - virusning inkubatsiya koeffitsienti, γ - tiklanish koeffitsienti.

where H - "trap" are unprotected computers, Y - computers that have come into contact with the virus but are not infected, Z - infected computers, I - computers that have developed immunity. β - the virus propagation coefficient, σ - the virus incubation coefficient, γ - the recovery coefficient.

The larger the network, the more effective this scheme will be. For example, if there are 50 thousand nodes (computers) in the network and only 0.4% of them are "trapped", then, as the developers note, viruses will have time to capture no more than 5% of the network and then be stopped by the immune system. For a network of 20 million nodes with the same proportion of "trapped", the infection rate will be only 0.001%.

Impact Factor: 9.9 ISSN-L: 2544-980X

Similarly, the Digital Immune System (DIS) - created by Symantec, implements an automatic analysis and distribution mechanism against computer viruses, that is, a special client computer that receives an attack sends the virus to the Symantec center, where the virus is analyzed, its signature is determined, and an updated antivirus is automatically sent to clients. IBM Immune System for Cybersecurity (Watson-based) - developed by IBM, the "cyber-immune system" works using artificial intelligence Watson, that is, it analyzes the attack based on machine learning and responds appropriately to the situation (Table 1).

Table 1

Comparison of artificial immune system-based antiviral defense systems

№	System name	Technology	Analysis method	Automatic patch deployment	Immunity
1	**Symantec DIS**	Client-server, signature analysis	Analysis + automatic	Yes	High
2	**IBM Watson Immune System**	Immune System Artificial intelligence (Watson), machine learning	Artificial intelligence	Yes	Very high
3	**FireEye DTI**	Artificial intelligence, real-time threat intelligence	Automatic analysis	Yes	High
4	**Honeynet Project**	Honeypot simulation	Scientific analysis	No	Average
5	**Cisco Talos**	Threat Analysis	Automatic analysis	Yes	High

Conclusion

The results of theoretical studies and computational experiments show that artificial immune systems can solve data compression, clustering and protection, change detection, search for the optimality of complex functions, etc. more effectively than intelligent systems built on the basis of fuzzy logic and neural networks, which indicates their wide application in various immune systems and promising areas of science. Modeling has shown that it is advisable to integrate the above system into cyberattack detection and response systems (IDS/IPS). In particular, systems based on the idea of creating a "honeypot" small network will be more effective when used in conjunction with an artificial immune system.

References

1. Akbarov D. E. Cryptographic methods of ensuring information security and their application // Uzbekistan Markasi. – 2009. – T. 432.
2. Крыжановский, А. В. (2008). Применение искусственных нейронных сетей в системах обнаружения атак. Доклады Томского государственного университета систем управления и радиоэлектроники, (2-1 (18)), 104-105.
3. Васильева К. В., Лаврова Д. С. Обнаружение аномалий в киберфизических системах с использованием графовых нейронных сетей //Проблемы информационной безопасности. Компьютерные системы. – 2021. – №. 1. – С. 117-130.
4. Мухториддинов, М., Акбаров, Н., & Умаров, Ш. (2023). Machine learning for network security and anomaly detection. In Conference on Digital Innovation:" Modern Problems and Solutions.

Impact Factor: 9.9 ISSN-L: 2544-980X

5. Хайруллин, Э. Р., Вульфин, А. М., Васильев, В. И., & Мандовен, С. А. (2025). Нейросетевая система обнаружения сетевых атак. Системная инженерия и информационные технологии, 7(1 (20)), 105-112.
6. Umarov, S. A. (2024). Axborot xavfsizligining intellektual tizimlarini qurish asoslari. Buxoro davlat universiteti ilmiy axboroti, (2), 9-16.
7. Wang S. et al. Machine learning in network anomaly detection: A survey //IEEe Access. – 2021. – T. 9. – C. 152379-152396.
8. Umarov, S. A., & Abduqodirov, A. (2024). AXBOROT XAVFSIZLIGI TIZIMLARINI INTELLEKTUALLASHTIRISH MASALALARI. Al-Farg'oniy avlodlari, (1), 4-10. doi: 10.5281/zenodo.10866967
9. Bhuyan, M. K., Kamruzzaman, M., Nilima, S. I., Khatoon, R., & Mohammad, N. (2024). Convolutional Neural Networks Based Detection System for Cyber-Attacks in Industrial Control Systems. Journal of Computer Science and Technology Studies, 6(3), 86-96.
10. Qodirov, F., & Xolmurodova, A. (2025). TARMOQ XAVFSIZLIGINI TA'MINLASHDA SUN'IY INTELLEKT IMKONIYATLARI. Наука и инновация, 3(7), 61-65.
11. Sadirova, X. X. (2025). IDS ORQALI TARMOQDA BO 'LADIGAN HUJUMLARNI AQINLASH USULLARI VA TAHLILI. Miasto Przyszłości, 56, 298-302.
12. Azizovich, U. B., & Ravshanjon o'g, J. R. A. (2024). IOTDA SUN'IY INTELLEKT ULANISH VA SAMARADORLIKNI OSHIRISH. JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH, 1(3), 378-386.