Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers

Vladimir Golovko, Myroslav Komar, Anatoly Sachenko

Abstract – **It's proposed to use artificial immune systems and neural networks to detect attacks on computer systems. The principles of attack detection system design based on artificial immune network are described, and the architecture of attack detection system is presented.**

Keywords - **Intrusion Detection Systems, Computer Network Security, Neural Networks, Artificial Immune Systems, Immune Detectors.**

I. INTRODUCTION

Currently, there is a continuous increase in the number of attacks and abuses in the sphere of high technologies. Therefore, the security of computer systems is gaining more and more attention [1].

The main task of the Intrusion Detection Systems (IDS) is to protect computer networks from attack in real time. Today are being developed many different technologies to protect computer networks, which are based on the application of neural networks, on the technologies for data extraction (data mining), statistical analysis, etc. The main disadvantage of existing systems is their inability to detect new or unknown attacks, which are characterized by the absence of records about them in the system. Modern intrusion detection systems are also poorly suited to work in real time, which reduces their efficiency in the protection systems.

In this work the use of immune system and neural networks technology to detect attacks on computers is considered. The immune system can be trained to recognize a variety of bacteria and viruses, to store information on detected infections and effectively protect the body from external influences [2]. Therefore, the ability of such systems for learning and generalization of the results give possibility to create on their basis the intelligence information protection systems that can detect unknown computer attacks.

II. THE STRUCTURE OF NEURAL NETWORK ARTIFICIAL IMMUNE SYSTEM TO DETECT ATTACKS

Propose artificial immune system consists of a population of immune detectors, each of which represents a neural network with n - inputs and two outputs. Output values of the detector are formed as follows:

$$Z_1 = \begin{cases} 1, & if\ \ no\ attack \\ 0, & in\ other\ case \end{cases}$$
$$Z_2 = \begin{cases} 1, & if\ the\ attack \\ 0, & in\ other\ case \end{cases} \qquad (1)$$

A set of clear recordings and attacks constitute a training set for neural network detectors.

Attack detection system, built on the basis of artificial immune systems consists of the following modules:

- module generation detectors;
- learning module immune detectors;
- module selection detectors;
- module destruction detectors;
- module IDS;
- module cloning and mutation detection;
- module formation of immune memory.

After the stage of training and selection, the detectors have the ability to respond to the attack and ignore the clear record that can minimize the number of false reactions. A neural network of counter-proliferation is used as a detector. The selection of the best detector made in accordance with the smallest meaning of the total squared error, which is determined on the test sample. The operation of mutation is based on additional training of clone detectors on the detected attack. As the number of detectors in the system increases the probability of detecting attack, is also increases.

III. CONCLUSION

Approach to use artificial immune systems and neural networks for attacks detection on computer systems is proposed and architecture of proper security system is described.

REFERENCES

1. J. Allen, A. Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, State of Practice of intrusion detection technologies // Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute. 2000.
2. Dasgupta D. Artificial immune systems and their applications / translation from English edited by A.A. Romanyukha. - M.: FIZMATLIT, 2006. - 344 pp.

Vladimir Golovko - Brest State Technical University, Moskovskaya Str., 267, Brest, 224017, BELARUS, E-mail:gva@bstu.by
Myroslav Komar - Ternopil National Economic University, 3 Peremoga Square, Ternopil, 46004, UKRAINE, E-mail: mko@tneu.edu.ua
Anatoly Sachenko - Ternopil National Economic University, 3 Peremoga Square, Ternopil, 46004, UKRAINE, E-mail: as@tneu.edu.ua