An algorithm based on artificial intelligence for solving information security tasks

Olga Purchina[1], *Anna* Poluyan[1], and *Dmitry* Fugarov[1*]

[1]Don State Technical University, Gagarin square 1, 344000 Rostov-on-Don, Russia

Abstract. In the age of rapidly developing information technologies, when the process of informatization has long touched almost all aspects of human life, it is impossible to imagine a single company that would not use a computer network for its functioning. And also with the development of the software and hardware infrastructure of companies, security requirements are growing. But business development through the introduction of the Internet only increases the number of threats associated with the availability, integrity and confidentiality of information. The development of antivirus software, intrusion detection and prevention systems does not fundamentally change the statistics on the number of attacks on enterprises. The number and variety of attacks on information systems is growing every year, and financial losses from the introduction of computer viruses and unauthorized access to the system are growing proportionally. Artificial intelligence (AI) is present in all areas of our activities. Whether it is a household area or a commercial one. In this regard, the use of AI in the fields of information security is more often observed, which is a promising area of research. The article describes the ways of possible application of artificial intelligence methods in the field of information protection, and also proposes an algorithm for the system of information protection from abnormal requests. The use of an artificial immune algorithm makes it possible to increase the effectiveness of threat detection by comparison with existing analogues. A distinctive feature of these methods is the ability of these systems to solve multidimensional problems of enormous computational complexity in real time.

1 Introduction

Due to the widespread use of the Internet, sufficient attention has been paid to issues related to the preservation of information from unauthorized access [1]. The methods of intrusion into the system are becoming more sophisticated every day. In this regard, great attention is paid to methods of combating various network attacks.

Consider the nature of network threats [2]:

— the degree of influence on the object (passive, active);

— implementation objectives (unauthorized access (NSD) to information for the purpose of changing it or NSD to the system itself);

* Corresponding author: ddf_1@mail.ru

— the condition of the beginning of the implementation of threats (an attack on the implementation of a request or the implementation of a necessary event, an unconditional attack);
— the presence of feedback with the attacked object (with or without feedback);
— location of the attacker (intra-segment or inter-segment);
— number of attackers (distributed or unallocated);
— the ISO standard level (physical, channel, network, transport, session, representative, applied) [3].

To ensure the security of network resources, a range of various specialized systems are used, such as load testing systems, network monitoring systems, management systems tools, as well as intrusion detection systems [4]. Intrusion detection systems can be divided into two types of non-adaptive and adaptive methods. Non-adaptive systems perform their functions well for known types of intrusions, but stagnate when new types of attacks appear [5].

For adaptive methods, algorithms based on bionic methods are introduced into protection systems. Of course, systems based on bionic search are superior to traditional security systems, combining evolutionary methods, genetic algorithms and artificial immune systems.

Intrusion detection systems can be classified according to the following characteristics (Figure 1). Each of them has its advantages and disadvantages [6].

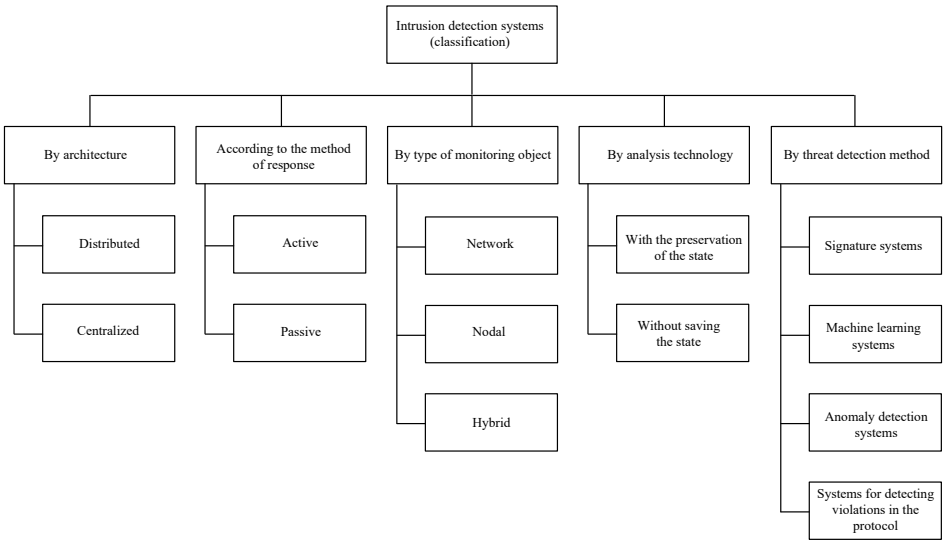

Fig. 1. Classification of intrusion detection systems.

2 The main part

Currently, there is an increased interest in approaches based on modeling of natural processes. A significant number of bioinspired heuristic methods have been developed to solve optimization problems. Artificial immune systems are one of the bio-engineered systems that simulate biological processes and are iterative methods of random search optimization [7].

Artificial immune algorithms are considered as antigens, candidates for solutions, and the qualities of the solution candidates correspond to the similarity between antibodies and

antigens. The process of finding possible solutions is similar to the process of immune cells recognizing antigens and performing an immune response in the immune system [8].

One of the main advantages of using artificial immune systems can be distinguished [9]:

Adaptability, the ability to develop in accordance with changes in the field of knowledge.

Flexible scalability. Due to the presence of a dynamic retraining mechanism, the system is able to generate new knowledge about new threats and automatically implement it into work.

Dynamic retraining. The artificial immune system is equipped with a mechanism that allows you to adjust the knowledge base based on new threats in the operating mode.

The disadvantages include:

— the complexity of learning;
— a sick number of constants that need to be set at the beginning of the algorithm (cloning level, mutation level, etc.);
— non-triviality of mutation and cloning operations;
— formation of the initial population and generation of a new one.

The formation of the initial population under uncertainty conditions is due to the need to ensure coverage of the search space using a minimum amount of resources [10]. A method of forming a new population under conditions of some uncertainties is proposed.

To build effective search procedures, the structure of an algorithm based on an artificial immune network and modified genetic operators is proposed. The constructed algorithm is used to fill the genetic library minimizing errors when testing the system for abnormal queries. The information is a set of populations of artificial immune cell elements [11]. The purpose of which is to form a gene database that will be replenished with the best solutions after each cycle of the algorithm execution. In the developed algorithm (Fig.3.), a request processing block UUA=<zapr; W; in_sol; reg_at; gen_op, attr> is introduced,

where zapr is a set of requests (identifiable (normal), unidentifiable (animal)); W is a mathematical model; in_sol is the initial solution; reg_at are signs queries; gen_op – genetic operators; attr – various attributes for the algorithm to work.

Mathematically, the immune system can be represented as follows: [12]

$$W=B\cup B\hat{}m=(\beta\_1...\beta\_k)\cup(\beta\_1\hat{}m...\beta\_s\hat{}m),$$

where

B- cells of the studied set

B^m is a cell having in its structure an element of a stable solution

β=(C,P), c – class of the cell identifying the threat;

P=(p_1…p_n)∈R^n

The immune search procedure is based on the following processes: mutation, cloning, inversion, reproduction, destruction.

The mutation mechanism is implemented as follows:

1. Set the break point x, with x∈[0,1]
2. The mutation mechanism of G (its point) is determined by

$$G=L*Z*x,$$

where Z=(expf_0(aff(β_i,β_j)))/(expf_0(n-n_0)/k)

aff – affinity the degree of proximity of two elements is calculated by the formula aff=1/√(∑_(s=1)^n ⟦(β_is-β_js)⟧ ^2);

n is the number of iterations, k is the regulating parameter of the rate of change expf_0(n-n_0); L is the length of the descendant.

3. The permutation occurs to the right and left of the break point. The mutation operation simulates a high-frequency changing mechanism in the immune response. And this operator generates cells with high convergence and enhances their diversity in the population [13].

The cloning mechanism produces groups of clones for each element in the population. Then, by changing the clone groups, elements with high convergence are created [14]. The cloning mechanism also includes the suppression of cloning, i.e. we will assume the retention of elements with high convergence from groups of clones and the rejection of the remaining cloned individuals [15]. Cloning suppression involves the selection of elements with high convergence from a time set that is composed of parent elements and groups of clones that have a convergence higher than the parent elements and are not in the parent population [16].

Inversion mechanism:

A point d is randomly generated, where

$$1 \le d \le L-1,\ d1 = L-d+1,\ d \ne d1$$

According to the rules of inversion construction, we invert only the middle part of the cell [17].

Next, select the number d again and calculate d1, go to step 2. Calculate the suitability of each clone in the inversion group. If the specified criterion is met, the mechanism stops working [18].

The reproduction mechanism creates the possibility of migration of elements from one subset of elements-alternative solutions to another subset. The reproduction group includes all the initial elements and alternative solutions obtained as a result of the operation of the above mechanisms, if their suitability is higher than at least one of the initial elements [19].

The destruction mechanism is implemented as follows: elements with an aff value above the average. Mechanisms of mutation, reproduction, cloning and inversion are used. The remaining elements are destroyed, their place is taken by clones of new elements. [20].

3 Conclusion

The paper considers the features of artificial immune systems, their elements. An algorithm for detecting intrusions into information networks has been developed, which uses artificial immune systems to detect the presence of anomalies in network traffic, and allows to increase the effectiveness of threat detection.

The experimental results show that compared with other algorithms, the presented algorithm has a lower error and a high chance of identifying potential threats.

References

1. A.Y. Poluyan, et al., *Adaptive algorithm of selecting optimal variant of errors detection system for digital means of automation facility of oil and gas complex*. J. Phys. Conf. Ser. **1015**, 022013 (2018)
2. Y.O. Chernyshev, et al., *Swarm-intelligence-based algorithm of connections permutation between pins*. Journal of Theoretical and Applied Information Technology **80(1),** 466-473 (2015)
3. O. Agibalov, *On the issue of using intuitionistic fuzzy sets for describing the expediency of solving optimization problems by genetic algorithms with given parameters,* E3S Web of Conf. **224,** 01008 (2020)

4. D. Fugarov, *Development and Mathematical Modeling of the AC Sensor for Refinery Automation Systems,* Smart Innovation, Systems and Technologies **247,** 271–281 (2022)
5. A.Yu. Poluyan, et al., *Solution of task on the minimum cost data flow based on bionic algorithm,* J. Phys. Conf. Ser. **1333,** 032056 (2019)
6. D.D. Fugarov, et al., *Magnetodielectric AC measuring transducer for automation systems in oil refineries.* Journal of Physics: Conference Series **1333(6),** 062020 (2019)
7. N.N. Ventsov, et al., *Studying the effect of paralleling settings on the functioning of a barcode recognition app,* International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017, 8076476 (2017)
8. A.I. Sukhinov, et al., *Accounting method of filling cells for the solution of hydrodynamics problems with a complex geometry of the computational domain,* Mathematical Models and Computer Simulations **12(2),** 232-245 (2020)
9. D. Onyshko, et al., *Synchronization system in wireless sensor networks of oil and gas complex,* E3S Web of Conf. **164,** 03030 (2020)
10. K.Yu. Solomentsev, et al., *Interference elimination in digital controllers of automation systems of oil and gas complex.* J. Phys. Conf. Ser. **1015**, 032179 (2018)
11. A.Yu. Poluyan, et al., *Application of bionic and immune algorithms for the solution of ambiguous problems of transportation routing,* J. Phys. Conf. Ser **1333,** 032057 (2019)
12. A.Gazizov, et al., *Theoretical aspects of the protection of personal data of employees of the enterprise by the method of pseudonymization,* E3S Web of Conf. **210,** 11001 (2020)
13. D.D. Fugarov, et al., *Methods for Revealing Hidden Failures of Automation System for Technological Processes in Oil and Gas Sector*. J. Phys. Conf. Ser **1118,** 012055 (2018)
14. Y.O. Chernyshev, et al., *Swarm-intelligence-based algorithm of connections permutation between pins*. Journal of Theoretical and Applied Information Technology **80(1),** 13-20 (2015)
15. A.I. Kozinkina, et al., *A Magneto Dielectric AC Measuring Transducer for Refinery Automation Systems*. Journal of Machinery Manufacture and Reliability **49(11),** 963-970 (2020)
16. O. Purchina, et al., *The algorithm development based on the immune search for solving unclear problems to detect the optical flow with minimal cost.* E3S Web of Conf. **258**, 06052 (2021)
17. Y. Gerasimenko, et al., *Mathematical modeling and synthesis of an electrical equivalent circuit of an electrochemical device.* Advances in Intelligent Systems and Computing **1259**, 471-480 (2021)
18. M. Ganzhur, et al., *Modeling of storage processes using Petri nets,* E3S Web of Conf. **175,** 05038 (2020)
19. D. Fugarov, *Technological Control of the Granulometric Composition of Active Materials of Chemical Current Sources*, Lecture Notes in Networks and Systems **510**, 1417–1423 (2023)
20. O. Purchina, et al., *Securing an Information System via the SSL Protocol*, International Journal of Safety and Security Engineering **12(5)**, 563–568 (2022)