The method for detecting network attacks based on the neuroimmune approach

V A Chastikova and A I Mitugov
Department of Computer Technologies and Information Security, Kuban State Technological University, Krasnodar, 350072, Russia

E-mail: chastikova_va@mail.ru

Abstract. The given paper proposes a procedure for detecting network attacks based on a hybrid model that combines deep learning methods and artificial immune systems and increases the efficiency of network traffic analysis. During the development process, the constituent components of a hybrid system for identifying network incidents have been specified with a preceding analysis of existing approaches to its construction. Conceptual architectures of the intrusion detection system have been proposed, functional simulation and data flow simulation for the system comprehensive description have been carried out. Theoretical analysis of the concepts selected for implementation of the development methods of network detection systems has been carried out and the procedures of their hybridization have been substantiated. A software package for comparative analysis of the neuroimmune approach with machine learning methods has been developed and tested.

1. Introduction
Due to the rapid development of schemes and the complexity of network attacks in the field of information security, there is a need to develop integrated information security systems. Therefore, when solving the problem of identifying network intrusions in organizations, they implement an intrusion detection system (IDS) as an intelligent component designed to search for unauthorized network events that potentially pose a threat to security [1].

The purpose of the given paper is to develop and study the efficiency of the network attack detection method using hybridization of a number of intelligent approaches. The result of the conducted research is the proposed and implemented neuroimmune approach for detecting network intrusions, as well as its comparative analysis with other methods for solving the task in hand.

To determine the procedures for identifying network incidents, it is necessary to analyze the existing most common approaches to IDS developing. The most popular among them are the following: systems based on the mechanisms of artificial neural networks (ANN), artificial immune systems (AIS), expert systems, signature methods and statistical analysis [1, 2].

The main disadvantage of expert and signature systems is the complexity of developing the rule bases, signatures, and the need for their regular updating, as well as low adaptability of methods to unknown types of traffic and modified network attacks. Statistical analysis is characterized by a high level of false positives [3].

In their turn, immune systems represent a promising direction in solving the problem of intrusion detection due to the main principles of immunology, which are the basis for such systems [4, 5]. Along
with neural networks they are flexible, adaptive and multipurpose; they can be trained on the same data sets as neural networks, where the latter, due to the high rates of technology development, are characterized by a constant complication of architectures, accompanied by an increasing efficiency of solutions [6, 7].

Accordingly, artificial neural networks and immune systems have been chosen as the basic approaches for the method development.

2. Architecture

To describe the procedures for detecting network attacks in an integrated intrusion detection system, it is further proposed to carry out methodological simulation of the IDS, which allows defining its main functional components, stages of work and structure.

The IDS can be represented by the following set of subsystems:

1. Sensing subsystem for collecting information – it consists of analyzers and is used to collect and unify raw data about the network functioning.
2. Subsystem for generating detectors – it implements the work of the neuroimmune system algorithms for generating detectors and their training on the prepared data set.
3. Data storage subsystem – it is a database that provides storage of records about network events and analysis results.
4. Traffic analysis subsystem – it carries out the detection of network attacks. Trained detectors analyze the information coming from the sensing subsystem and determine the class of connection.
5. Control subsystem that allows configuring the IDS, viewing the analysis results of the identified network events. It consists of a system of expert assessment and management [8].

IDEF0 methodologies have been chosen as the reference simulation procedures – functional simulation, which allows displaying the main functions performed by the intrusion detection system, control elements, mechanisms, and DFD – data flow diagrams, which allows identifying the main participants in the system functioning, stages of its operation and circulating data.

To determine the conceptual model of the integrated IDS in accordance with IDEF0 methodology, a context diagram (shown in figure 1) and its first level decomposition (shown in figure 2) have been made.

In accordance with the DFD functional simulation methodology, the system level context diagram of the target IDS is shown in figure 3, the subsystem level diagram is shown in figure 4.

Figure 5 shows a block diagram of the intrusion detection system based on the neuroimmune system. Accordingly, artificial neural networks and immune systems have been chosen as the basic approaches for the method development.
Figure 1. IDS context diagram of IDEF0 methodology.

Figure 2. Decomposition of IDS context diagram of the IDEF0 methodology.

Figure 3. The system level context diagram of the IDS of the DFD methodology.
3. Materials and methods

When developing an intrusion detection system, it was decided to use artificial immune systems (AIS) based on a clonal selection algorithm that provides the ability to train the system on a dataset describing network attacks. To improve the efficiency of the AIS algorithm, the clonal selection method has been hybridized with the metaheuristic algorithm – a modified genetic duelist method, which showed higher efficiency compared with other algorithms, it is a combination of the classical genetic algorithm and the duelist algorithm [9, 10]. The development and study of a hybrid artificial immune system (HAIS) in the given paper [11] have made it possible to determine the most effective scheme for their hybridization.

To improve the IDS efficiency, it has been proposed to use such deep learning method as convolutional neural networks, along with a hybrid AIS participating in the formation and training of antibody-detector images.

A similar approach to developing an IDS architecture proposed in the given paper and combining several machine learning methods was called a neuroimmune approach.

Figure 6 shows a block diagram of the method hybridization in the target system under design.
As part of the given paper, training and testing of the neuroimmune system is carried out on the “Intrusion Detection Evaluation Dataset” CIC-IDS2017 (Canadian Institute of Cybersecurity) data set [12, 13]. The selected set is one of the most relevant and extensively studied, as there are a number of studies describing the disadvantages of the given dataset and proposing solutions for their elimination, balancing, and feature map reduction by searching for interconnection, correlations and redundancy in records, in contrast to newer sets. At the same time, the dataset has a rather large sample, variability of the presented attack classes [14, 15].

4. Neuroimmune method for the network attack detection

Nowadays the use of deep neural networks is widespread in various applications, where their use makes it possible to solve with high accuracy the issues of recognition and classification, which are key ones for the network attack detection system [16].

A simple model of a deep network is the architecture of a multi-layer perceptron, referring to feedforward networks and consisting of an input layer, several hidden (deep) layers and an output layer [17]. The perceptron is often an integral component of more complex architectures due to its multifunctionality and efficiency with properly chosen architecture and high-quality training. Among deep artificial neural networks, convolutional neural networks have been significantly developed; these networks are an alternation of convolutional and subsampling (pooling) layers, where the output is a number of fully connected layers that actually make up the multilayer perceptron [18].

The architecture of the convolutional network used in the neuroimmune approach is shown in figure 7 and includes an input layer for receiving an attack image, two pairs of convolution and subsampling layers with subsequent output to a fully connected network – a perceptron containing a pair of hidden layers. To compensate for the significance loss of features corresponding to the corner zones of the image map, the same padding technique, which consists in adding zero pixels along the perimeter of the processed maps, is applied to the initial map and after the first subsampling layer.

Correspondingly, the pooling layers implement the max pooling approach, according to which subsampling consists in choosing the largest element within the position of the shifting window (kernel or filter), where at the first stage of pooling with the 2x2 kernel size, the stride parameter describing the kernel shift step is 2, which reduces the size of the map by half. At the second stage of pooling, the stride shift is equal to 1. The ReLu function is used as the activation function; the network learning algorithm is a hybrid artificial immune system.

Figure 6. The block diagram of the neuroimmune system method hybridization.

Figure 7. Convolutional neural network architecture of the neuroimmune system.
Figures 8 and 9, respectively, show algorithms for training and functioning of the intrusion detection system based on the neuroimmune approach combining the architectures of a hybrid artificial immune system and a convolutional neural network.

5. Results and discussion

The generalized results of comparing methods for detecting network attacks, namely: CNN (convolutional neural network), Perceptron (multilayer perceptron), HAIS (hybrid artificial immune system), NIS (neuroimmune system), – are presented in Table 1.

Table 1. Comparative analysis of the network attack detection methods.

| Method   | Root mean square learning error | Root mean square generalization error |
|----------|---------------------------------|--------------------------------------|
| NIS      | 0.031                           | 0.049                                |
| CNN      | 0.046                           | 0.063                                |
| HAIS     | 0.078                           | 0.134                                |
| Perceptron | 0.256                         | 0.361                                |

Architectures of the multilayer perceptron, convolutional neural network, and hybrid artificial immune system correspond to the previously described architecture of the neuroimmune system formed...
by means of hybridization of these three methods, which makes it possible to compare their independent implementations with an integrated neuroimmune approach. The number of tests consisted of 20 stages with 100000 iterations.

Studying the test results, it is possible to see the advantage of combining the HAIS and CNN architectures within NIS compared to the classic CNN convolutional network. At the same time, the implementations of the multilayer perceptron and the HAIS hybrid immune system are noticeably inferior to NIS and CNN, demonstrating lower detection accuracy.

### 6. Conclusions

As a result of the study, the neuroimmune model has demonstrated a higher accuracy in comparison with the methods presented in the computational experiment, which is reflected in an increase in the learning-rate and generalization parameters, as well as the speed of learning. The proposed neuroimmune method provides the most efficient search for the optimal weights, characteristics of the agent-detectors, identification of attack patterns from traffic representations, allowing us to obtain more productive results of the network attack identification by the intrusion detection system.

### References

[1] Khraisat A, Gondal I, Vamplew P and Kamruzzaman J 2019 Survey of intrusion detection systems: techniques, datasets and challenges Cybersecur 2 20

[2] Vasiliev V I and Shamsutdinov R R 2018 Distributed attack detection system based on the mechanisms of the immune system Information Technologies for Intelligent Decision Making 237-44

[3] Kostas K 2018 Anomaly Detection in Networks Using Machine Learning A thesis submitted for the degree of Master of Science in Computer Networks and Security 17

[4] Matveev M G, Sviridov A S and Aleinikova N A 2014 Models and Methods of Artificial Intelligence. Application in economics (INFRA-M Publishing House) 316-24

[5] Chastikova V A and Kartamyshev D A 2016 Artificial immune systems: basic approaches and features of their implementation Electronic network polythematic journal Scientific works of KubSTU 8 193-208

[6] Sukhov V E 2015 Network traffic anomaly detection system based on artificial immune systems and neural network detectors Bulletin of the Ryazan State Radio Engineering University 54(1) 84-90

[7] Lyngdoh J, Hussain M I, Majaw S and Kalita H K 2018 An intrusion detection method using artificial immune system approach Int. conf. on advanced informatics for computing research 379-87

[8] Elrawy M F, Awad A I and Hamed H F A 2018 Intrusion detection systems for IoT-based smart environments: a survey Journal of Cloud Computing 7(21) 20

[9] Chastikova V A and Mityugov A I 2018 Development and research of a modified genetic duelist algorithm Modern science-intensive technologies 8 144-9

[10] Biyanto T R, Fibriantoa H Y, Nugrohoa G, Listijorinib E, Budiatric T and Hudad H 2016 Duelist Algorithm: An Algorithm Inspired by How Duelist Improve Their Capabilities in a Duel Advances in Swarm Intelligence: 7th Int. Conf. 39-47

[11] Chastikova V A and Mityugov A I 2019 Development of an effective architecture of the artificial immune system based on its hybridization with a modified genetic duelist algorithm Caspian journal: control and high technologies 4(48) 42-51

[12] Chastikova V A and Sotnikov V V 2019 Method of analyzing computer traffic based on recurrent neural networks Journal of Physics: Conf. Series: Int. Conf. "High-Tech and Innovations in Research and Manufacturing" 012133

[13] Chastikova V A, Zherlitys S A, Volya Y I and Sotnikov V V 2021 Analysis of training of deep neural networks with heterogeneous architecture while detecting malicious network traffic IOP Conf. Series: Materials Science and Engineering 12135
[14] Sharafaldin I, Lashkari A H and Ghorbani A A 2018 Toward generating a new intrusion detection dataset and intrusion traffic characterization 4th Int. Conf. on Information Systems Security and Privacy 108-15

[15] Panigrahi R and Borah S 2018 A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems Int. Journal of Engineering & Technology 479-82

[16] Canziani A, Paszke A and Culurciello E 2017 An Analysis of Deep Neural Network Models for Practical Applications arXiv:1605.07678 [cs.CV]

[17] Geron A 2017 Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems (O'Reilly Media) 612

[18] Howard A G 2013 Some improvements on deep convolutional neural network based image classification arXiv:1312.5402 [cs.CV]