ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse256942020.pdf
https://doi.org/10.30534/ijatcse/2020/256942020

Methods and Tools for Protecting Information Systems based on the Neural Network Apparatus Register of State Property

Natalia L. Krasyukova[1], Tatyana G. Popadyuk[2], Lyubov A. Plotitsyna[3], Vyacheslav V. Zubenko[4], Galina S. Izotova[5]

[1] Federal state educational budgetary institution of higher education "Financial University under the Government of the Russian Federation", Russia
[2]Federal state educational budgetary institution of higher education "Financial University under the Government of the Russian Federation", Russia
[3]Federal state educational budgetary institution of higher education "Financial University under the Government of the Russian Federation", Russia
[4]Federal state educational budgetary institution of higher education "Financial University under the Government of the Russian Federation", Russia
[5]Federal state educational budgetary institution of higher education "Financial University under the Government of the Russian Federation", Russia

ABSTRACT

The article considers methods and means of protection of distributed computer systems. A new approach based on the neural network apparatus is proposed. A complex adaptive system consisting of subsystems for threat recognition, classification, and intelligent control based on intelligent agents is implemented and described. This combination made it possible to implement adaptive management of the information system security system, ensure timely response to the threat and make independent decisions in real time. Experiments were conducted to determine the level of correctness of detecting threats and recognizing them.

Key words : Protection of distributed computer systems, neural network, intelligent agent, complex adaptive systems.

1. INTRODUCTION

This big present and in cases when you need quick information processing uses distributed computer system, the structure of which is the lack of control center and distribution functions, resources among all nodes in the system. A typical example is the well-known Internet, which provides an open and scalable communication system [1-4]. This principle is the basis for all distributed systems and unfortunately this has weakened their security level. In the network, anyone can send any package to anyone, and the recipient must process the package that came properly. The security weakness is that an attacker can form a false identity and send malicious traffic (traffic) with impunity, so all nodes of the system connected are potentially at risk, since the openness makes them accessible to the attacking party [5]. Security methods for distributed computer systems are based on standard methods for verifying authorization data. unfortunately, they cannot fully counteract these threats [6].

As evidenced by the statistics of Kaspersky Lab, most attacks in recent years have been aimed at gaining access to the system and executing arbitrary code with local user privileges, as well as manipulating data, performing DoS attacks on the failure of system resources, or creating a significant load on the system itself. The rating also includes vulnerabilities that allow data manipulation, circumventing the security system, and conducting XSS attacks. [9]
Features of modern attacks are increasing the complexity of the attacking action and technological level. Most often, they have a multi-level algorithm and a distributed structure, which proportionally increases their negative effect [7]. The task of modern security systems is to process and analyze large amounts of data using an intelligent approach. They must perform threat recognition and classification, and if there is no information about such a threat, adapt to the new attacking action. Based on the analysis of these features of building security mechanisms, neural networks and intelligent control agents are the most suitable for solving this problem [8].

2. MATERIALS AND METHODS

There are two ways to protect your computer system. The first is to try to build an absolutely secure system, that is, to complicate the authentication process, access rights mechanisms, and so on. However, this method has several disadvantages. First, it protects you from your own users. Secondly, the authentication protocols themselves have weak points, and passwords can be stolen and picked up. Such systems will always have weak points. The second way is to complicate the mechanisms for detecting anomalies in user behavior and resource usage [10].

As already noted, the most common and dangerous attack is the failure attack. A typical denial attack scenario involves blocking resources, services, and software from a particular node. The attacker, having gained access in a certain way, initiates an attack using the machines of third parties taken under control, called agents. An attack can block a key resource by exploiting certain vulnerabilities in the victim's software (vulnerability attacks) or by forwarding large volumes of traffic that the victim must process (overflow attacks – flooding attacks) [11-13].

Distributed denial-of-service (DDoS) attacks)) this is a failure attack that is implemented from several controlled machines (agents). In the most common scenario, all the machines involved in the scheme simultaneously start sending packets to the victim with maximum intensity [15]. A large number of agents allows you to quickly download the main and backup resources of the victim. A typical DDoS attack consists of two stages. The first step is to search for vulnerabilities and install attack tools on them [14]. This stage is also known as turning computers into "zombies". In the second stage, the attacker commands his "zombies" through a secure channel to launch an attack against the selected node. Note that attack traffic packets can use a fake source IP address to make it harder to identify attacking computers. The number of managed agents in a distributed denial-of-service attack can range from several tens to tens of thousands of compromised machines. [1,2]

Among the considered and analyzed methods of protection of distributed computer systems proposed in other works, it should be noted such methods as: decision trees, Bayesian network, hidden Markov network, fuzzy logic, the method of reference vectors. All of them perform threat analysis and response algorithms in their own way, but the best results of recognizing new and modified threats are marked by systems with the implementation of neural networks, that is, those that are characterized by an intelligent approach to detecting danger in the system [16].

The basis of such systems is the prototype of a biological neuron. Based on the received input data and previous experience obtained in the form of weights of connections between the input layer and the intermediate result obtained, which is a consequence of activation of the neural network. [3,4]

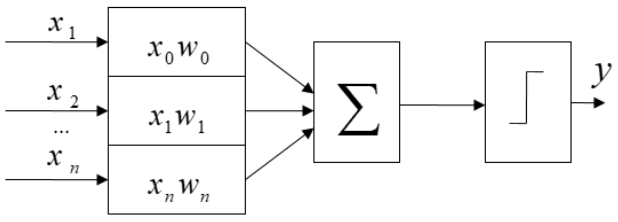

Figure 1: Neuron, an element of a neural network

Figure 1 shows a formal neural network neuron. The combination of this structure into a system makes it possible to analyze the input parameters and with some probability answer the question of which class or type of source information belongs to. [5]

Intrusion detection based on a modified neural network

Neural networks are characterized by the ability to learn. Unlike conventional programs, they do not have a standard algorithm and can learn by changing the coefficients of connections between neurons. During training, the network can identify complex dependencies between input and output data and generalize the resulting image. [6] according to the method of training, neural networks are divided into those that require preliminary training and self-learning networks [17]. The latter include Kohonen networks, which are characterized by a distributed memory structure. This structure allows you to avoid failure in the event of a failure of one of the neurons. This effect is achieved due to the fact that a cluster of neurons, rather than a single neuron, is responsible for classifying input data. Each input signal vector $X = \{x_1, x_2 ... x_n\}$ is sent to the input of each neuron in a two-dimensional matrix of neurons. The set of weighting factors is also shown as a matrix W. [7]

$$W = \begin{pmatrix} w^{11} & w^{12} & w^{1j} \\ w^{21} & w^{22} & w^{2j} \\ w^{i1} & w^{i2} & w^{ij} \end{pmatrix} \quad (1)$$

The elements of this matrix are vectors of weight coefficients $w^{ij} = \{w_1^{ij}, w_2^{ij} ... w_n^{ij}\}$. At the beginning of training, the network weights are set randomly. In the next step, the distance between the input signal vector and a set of neurons in the network is calculated using the formula 2.

$$d_{ij} = \sum_{p=1}^{n} (x(t) - w_p^{ij}(t))^2 \quad (2)$$

where $x(t)$ is the input vector at time t, $w_p^{ij}(t)$ and is the vector of weighting coefficients at time t. In the third stage, a search is performed for the neuron with coordinates (i, j) for which this distance is the smallest. Then the weights are changed, which is calculated using the following formula for network training.

$$w^{ij}(t+1) = w^{ij}(t) + k(t)(x(t) - w^{ij}(t)) \quad (3)$$

where k(t) is the learning coefficient, or the learning rate that decreases over time.

Thus, the Kohonen network is trained using sequential approximations. In the process of learning, data is fed to the inputs, but the network adjusts itself not to the reference value of the output, but to patterns in the input data. Training begins with a randomly selected initial location of the centers.

In the process of sequential input of a network of training examples, the most similar neuron is determined (the one with the scalar product of weights and the input vector is minimal). This neuron is declared the winner and is the center of the test of the scales of neighboring neurons. This training rule assumes "competitive" training, taking into account the distance of neurons from the "winning neuron".

Training in this case does not consist in minimizing the error, but in determining the desired weights (internal parameters of the neural network) for the greatest match with the input data.

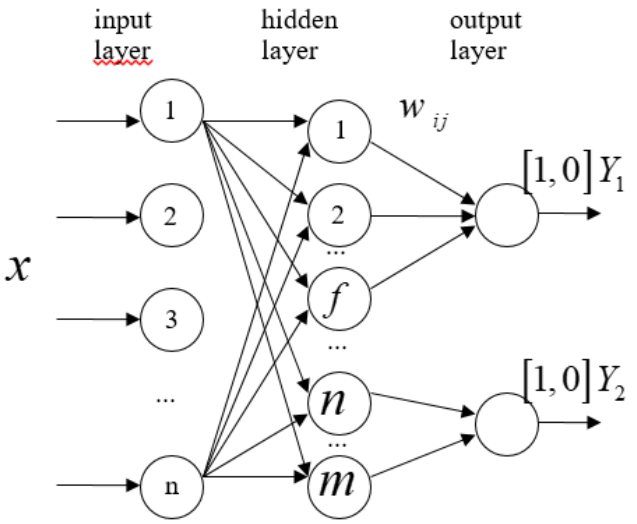

Figure 2: Neural network the definition of the attack

The basis of the network is the hidden layer of Kohonen. However, to improve the result of the analysis of the system status and intrusion detection was proposed a modified neuron of Kohonen network. As shown in figure 2. the hidden layer of Kohonen consists of two parts. The first set of neurons $[1...f]$ is responsible for determining the type and class of attack. Changing the input weights on the source layer triggers activation of the linear function Y_1. In this case, the value of zero corresponds to the allowed state of the system, and units correspond to the attack. The second set of neurons $[n...m]$ analyzes the normal state of the system Y_2, which allows you to Supplement and Refine the result of the output layer of the attack class Y_1 [18]

Parameters that are used as input data for recognizing system attacks can include: parameters of network records and events, data about the time when users log in and out, the number of processes, file access, time intervals, and requests to resources and objects of the computer system. This mechanism can also use computer network settings, the number of users, user privileges, access settings, the number and nomenclature of ports, network services, and administrator settings to detect vulnerabilities [19].

To detect an attack, analysis and data collection must be performed at several levels of the information system, in this case, a distributed computer system. Therefore, the following information sources were selected: network packet data, router log data, operating system security log, operating system registry, and operating system process data [20].

An intelligent agent is attached to each data collection level, as shown in figure 3.

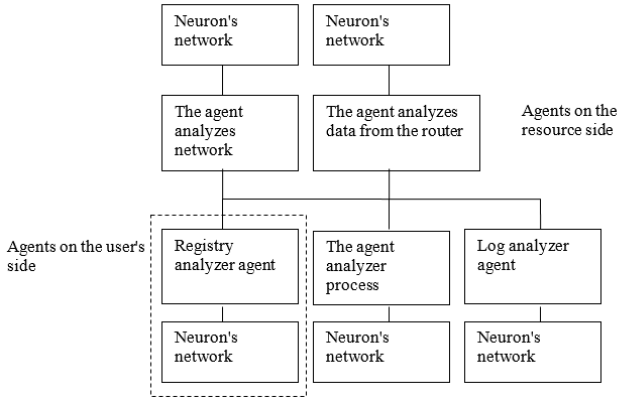

Figure 3: Architecture of the attack detection system

This diagram shows a complex adaptive system based on a neural network and intelligent agents. Each of the attached intelligent agents has its own neural network, which is responsible for classifying threats and attacks on the scale of its analysis. Accordingly, to increase the percentage of attack recognition, it was proposed to use intelligent agents that would interact with each other. A detailed diagram of the interaction of an intelligent agent and a neural network is shown in figure 4.

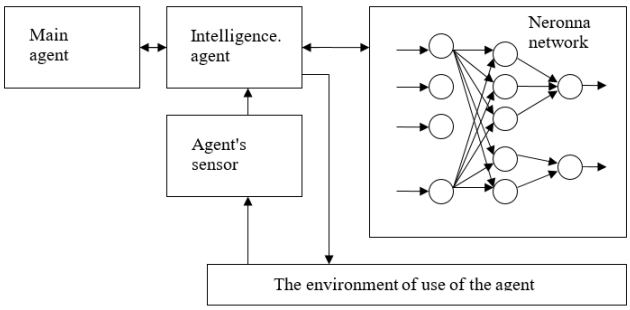

Figure 4: Architecture of a complex adaptive security system

The presented diagram shows the structure of an intelligent agent that uses neural network technology to detect and classify threats, if there is one [24]. The input parameters of the system fall on the agent's sensor, which continuously reads data from the environment provided to it and feeds it to the inputs of the neural network. In addition to system data, an intelligent agent can also provide data about the user, their activity, and so on as input information. All this depends on the task at hand [21].

After receiving a neural network result on the type and class of attack or normal state of the system, information from it is transmitted through the agent's connections to other agents, as well as to the main agent on the receiving side of the system. This way, information about the threat is analyzed by the entire structure of the security mechanism and increases the accuracy of the analysis [23].

Since we use the Kohonen network neuron as a hidden layer, all parameters are fed to a matrix of neurons to form a fully connected neuron network. It is important to note that this type of neural network is characterized by a large number of connections. Therefore, it would be appropriate to perform simplifications and verbalizations of the neural network. This

means that elements (input parameters, neurons) that have little effect on the recognition error can be excluded from the network without significantly impairing the quality of recognition. [8]

During experiments, it was found that when analyzing the selected DoS attacks, certain parameters do not play a large role in recognition. As shown in figure 5, if there are more than 11 input parameters of the neural network, the recognition result does not differ much from each other, which means that their number can be reduced to this number [22].

However, when new input parameters for training appear, this method can damage neural networks, and it can lose its generalization property. Thus, this algorithm for reducing input parameters should be used in static problems, rather than in problems with variable conditions.

3. CONCLUSION

In the face of increasing attacks and their complexity, protecting information systems requires an intelligent approach, that is, one that can learn and make security decisions independently and identify threats by classifying them according to certain characteristics.

A software package based on neural networks and intelligent agents has been developed to detect and classify attacks. The proposed mechanism is based on the Cochogene neural network and is characterized by such properties as the accuracy of attack detection even in conditions when one of the neurons has failed because a certain number of neurons corresponds to the classification of the attack – a cluster. In addition, the property to analyze the state of the system without the entire set of system parameters, as shown by experiments, allows you to avoid an incorrect result in their absence, or damage them.

REFERENCES

1. Akhmadulina A.T. **Evaluation of the management efficiency of municipal unitary enterprises** (on the example of the municipal formation "Orenburg city") [Text] / A.T. Akhmadulina, O.V. Skryniknikova // Innovative economy: prospects for development and improvement. - 2016.- No. 2 (12) .- P. 10-15. (In Russian)
2. Baranova I.V. **Types and criteria for evaluating the effectiveness of unitary enterprises** // Siberian Financial School.- 2011.- No. 4 (87) .- P. 43-50. (In Russian)
3. Bogataya I.N. **Improving internal risk control and management in commercial organizations**. In the collection: Development of finance, accounting and auditing in modern management concepts. Materials of the I international scientific and practical conference. 2018.- P. 286-290. (In Russian)
4. Vorobyov Yu.N. **Technological transformation of the economy and its impact on the financial and economic security of business entities**. In the collection: Financial and economic security of the Russian Federation and its regions. Proceedings of the II International Scientific and Practical Conference. 2017.- P. 11-14. (In Russian)]
5. Vygolko TA **Analysis of economic power in the works of JK Galbraith** // Bulletin of the Institute of Economic Research. 2016. №4 (4). URL: https://cyberleninka.ru/article/n/analiz-ekonomicheskoy-vlasti-v-rabotah-dzh-k-gelbreyta (In Russian)
6. **The public sector in the Russian economy** // Bulletin on the development of competition, March 2019 [Electronic resource] - Access mode: http://ac.gov.ru/files/publication/a/21642.pdf (In Russian)
7. Gubareva, A.O., Gurkina, D.A. **Plyusy gosudarstvennoj sobstvennosti.** URL: https://moneyprofy.ru/pljusy-gosudarstvennoj-sobstvennosti/ (In Russian)
8. Gubina O.V., Ivanova N.A., Gerasimova S.V. **Assessment of the quality of the financial results of the organization**. In the collection: Problems of managing sustainable development of business structures in various fields of activity Collection of scientific papers of the International Economic Forum. Edited by N.A. Lytneva. 2017.- P. 67-74. (In Russian)
9. Dementyev VV, **The Problem of Power and Political Economy** / V.V. Dementev // European vector of economic development. - 2012 - N0.2 (13). - pp. 183-189. (In Russian)
10. Zavarin D.A. **Types of ownership in modern Russia** // Science among us 2 (2) 2017 nauka-sn.ru - p. 67 – 71 (In Russian)
11. Zavarin DA **Innovative geodetic GNSS technologies for determining spatial characteristics** / DA Zavarin, OK. Kraeva, N.D. Porscheva // Vuzovskaya Nauka - Region: Proceedings of the XV All-Russian Scientific Conference. - Vologda: VOU, 20167. p. 296–298. (In Russian)
12. Lytneva N.A. **Development of the system of state and municipal administration in the context of public sector reform** / A. Polyanin, E. Bobrova, T. Golovina, M. Goncharova, I. Dokukina, S. Dolgova, E. Kyshtymova .A., Makarova Yu.L., Lytneva N.A., Popova O.V., Rudakova O.V., Tychinskaya I.A., Shipunov A.S. Collective Scientific Monograph / Edited by A.V. Glade. Oryol, 2017. -228 p. (In Russian)
13. Lytneva N.A., Daniy I.S. **Methodology for analyzing the directions of optimizing municipal budget expenditures** // Basic Research.- 2017.- No. 7.- P. 162-166. (In Russian)
14. Mantoriy GA. **Institute of Property in the Soviet State** // Philosophy of Law. 2014. №5 (66). URL: https://cyberleninka.ru/article/n/institut-sobstvennosti-v-sovetskom-gosudarstve (In Russian)
15. Tesalovsky A., **Accuracy of the description of cadastral accounting objects in three-dimensional space** / A. A. Tesalovsky, Yu. S. Gorshkova, MV Konovalova, LA Sizova // Vuzovskaya Nauka - Region: Proceedings of the XIV All-Russian Scientific conferences. - Vologda: VOU, 2016. p. 183–185. (In Russian)
16. Cheglakova S.G. **Analytical tools of resource management in ensuring the economic security of an**

economic entity // Economics and Entrepreneurship .- 2018.- No. 1 (90) .- P. 617-621. (In Russian)

17. Ellman M. (1989). **Socialist Planning**. Cambridge University Press. p. 327.
18. Engels F. (1970). **Socialism: Utopian and Scientific**. Marx/Engels Selected Works, Volume 3, p. 95-151; Publisher: Progress Publishers.
19. Gregory Paul R., Stuart Robert C. (2003). **Comparing Economic Systems in the Twenty-First Century**. Boston: Houghton Mifflin. p. 27.
20. Tupper A. (2006). «**Public Ownership**» URL: https://www.thecanadianencyclopedia.ca/en/article/public-ownership
21. Aharonovich, A. R., Sergeevich, S. M., & Vyacheslavovna, D. S. (2019). **Institutional framework for entrepreneurship of regional innovation systems of the union state**. Academy of Entrepreneurship Journal, 25(Special Issue 1).
22. Kruzhilin, S., Baranova, T., Mishenina, M., & Zaitseva, M. (2018). **Regional specificity creation of protective afforestations along highways**. World Ecology Journal, 8(2), 22-32. https://doi.org/https://doi.org/10.25726/NM.2018.2.2.003
23. Alqudah, A. M., Alquraan, H., Qasmieh, I. A., Alqudah, A., & Al-Sharu, W. (2019). **Brain tumor classification using deep learning technique - A comparison between cropped, uncropped, and segmented lesion images with different sizes**. International Journal of Advanced Trends in Computer Science and Engineering, 8(6), 3684–3691. https://doi.org/10.30534/ijatcse/2019/155862019
24. Alqudah, A., Ashour, A. M., & Alboon, S. A. (2020). **Controlling of wind turbine generator system based on genetic fuzzy-pid controller**. International Journal of Advanced Trends in Computer Science and Engineering, 9(1), 409–425. https://doi.org/10.30534/ijatcse/2020/58912020