International Journal of Research and Review
Vol. 10; Issue: 9; September 2023
Website: www.ijrrjournal.com
Research Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Development of a Clone Selection Algorithm for Detecting Network Attacks

Sherzod Gulomov[1], Mir-khusan Kadirov[2], Nargiza Karimova[2]

[1]Dean of Cybersecurity faculty, Tashkent University of Information Technologies, Tashkent city, Uzbekistan
[2]Department Information Technologies, Faculty of Electronics and Automation, Tashkent State Technical University, Tashkent city, Uzbekistan

Corresponding Author: Mir-khusan Kadirov

DOI: https://doi.org/10.52403/ijrr.20230930

ABSTRACT

This article discusses the development of a clonal selection algorithm for detecting network attacks. A scheme for generating detectors by an algorithm for clonal selection of an artificial immune system for detecting network attacks is presented. The developed modification of the clonal selection algorithm of the artificial immune system is presented, which allows one to determine intentional changes in the controlled data, taking into account the use of an external optimization structure. A developed software module has been implemented designed to detect distributed denial of service network attacks. As a result, the detection of missing suspicious packets will optimize the filtering of network packets in networks.

Keywords: *Security features, clonal selection, software module, network attacks, suspicious packets, packet filtering, traffic filtering.*

INTRODUCTION

In the world, special attention is paid to the development and improvement of information security systems in information and communication systems [1]. At the current level of development of information and communication systems, the issues of information protection in computer networks [2, 3], which is one of the most important mechanisms for ensuring effective information security [4], become especially relevant.

Clonal selection algorithms [5, 6] are a class of algorithms [7] that use clonal selection methods and the theory of acquired immunity [8]. The theory is that in each individual, the antibody-producing cell system contains all the information necessary to synthesize any of the most diverse antibodies even before it encounters an antigen. The antigen does not deliver information to these antibody cells, but simply selects those cells that synthesize the antibodies corresponding to it and induces them to multiply, as well as to increased production of these antibodies [9]. Cells synthesizing this type of antibody belong to one clone, composed of all the descendants of one parent cell, which, as a result of a random process, has acquired the hereditary ability to respond to this antigen. Until this antigen appears, the clone remains relatively small [10]. The presence of an antigen stimulates the propagation of a clone capable of synthesizing the corresponding antibodies, and the better the recognition of the antigen, the more progeny (clones) will be generated [11, 12].

MATERIALS & METHODS

In the process of reproduction, individual cells - antibodies undergo a mutation that allows them to have a higher correspondence to a recognized antigen - antibody affinity. The higher the affinity of the parent cell, the less they undergo mutation, and vice versa. Learning [13] is achieved by increasing the relative population size and affinity of those

antibodies that have proven to be of value in recognizing the presented antigen. Each new generation contains a higher ratio of characteristics that the best members of previous generations have [14, 15]. The scheme of generating detectors by the clonal selection algorithm of the artificial immune system (AIS) [16, 17] for detecting suspicious actions is shown in Figure 1.

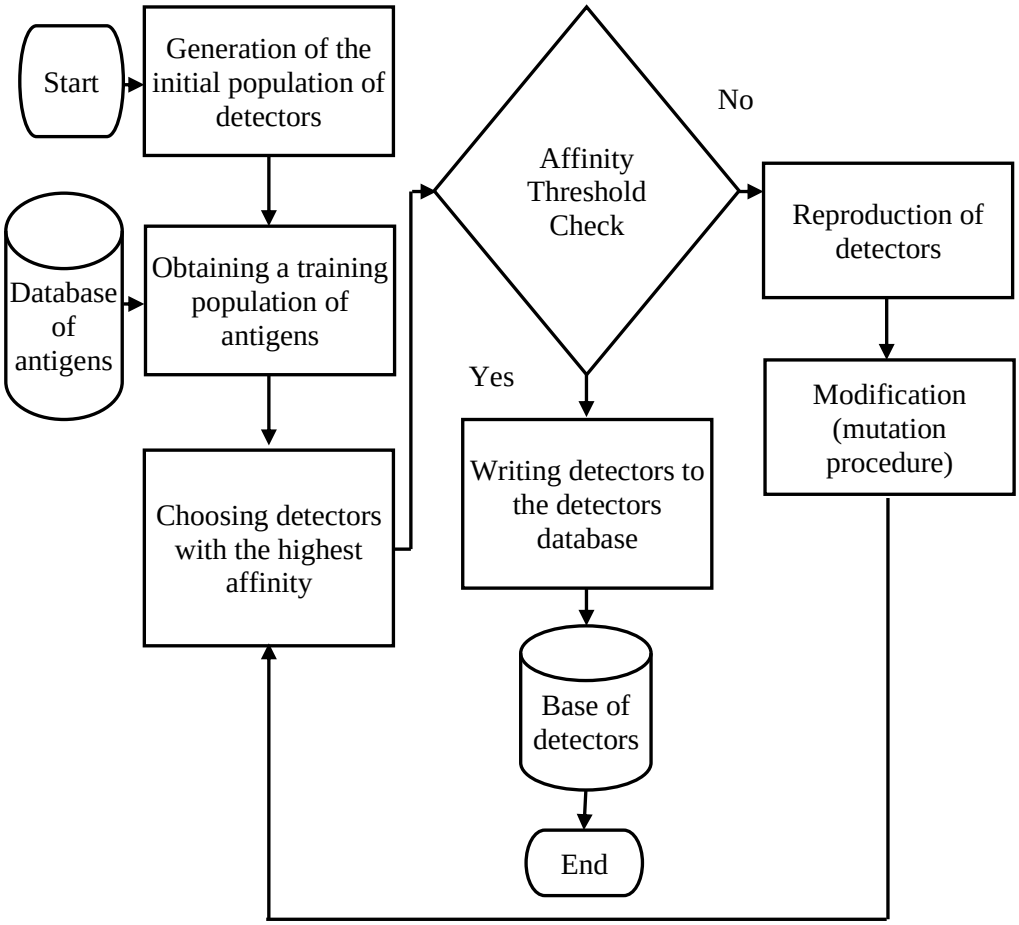

Figure 1. Scheme of generating detectors by the clonal selection algorithm of the artificial immune system for detecting suspicious activities

The clonal selection algorithm of AIS allows you to detect intentional changes in controlled data [18].

Modified AIS algorithm with clonal selection [19]. Due to the fact that AIS belongs to the class of bioinspired algorithms, for the formation of detectors, it is proposed to replace the mechanism of reproduction and mutation of detectors, which is standard for the clonal selection algorithm, with an external optimization procedure, the principle of which is based on the application of the strategy of evolutionary algorithms [20].

The evolutionary algorithm within the allocated resource explores the search space and generates a set of high-affine detectors, iteratively improving their quality by implementing the principle of inheritance and natural selection. The resulting set of AIS detectors is used to detect suspicious activities and antigens. Taking into account the application of the evolutionary strategy, the modified AIS algorithm will have the form presented above in Figure 2. Detectors are generated for a block of antigens, and not for each individual antigen.

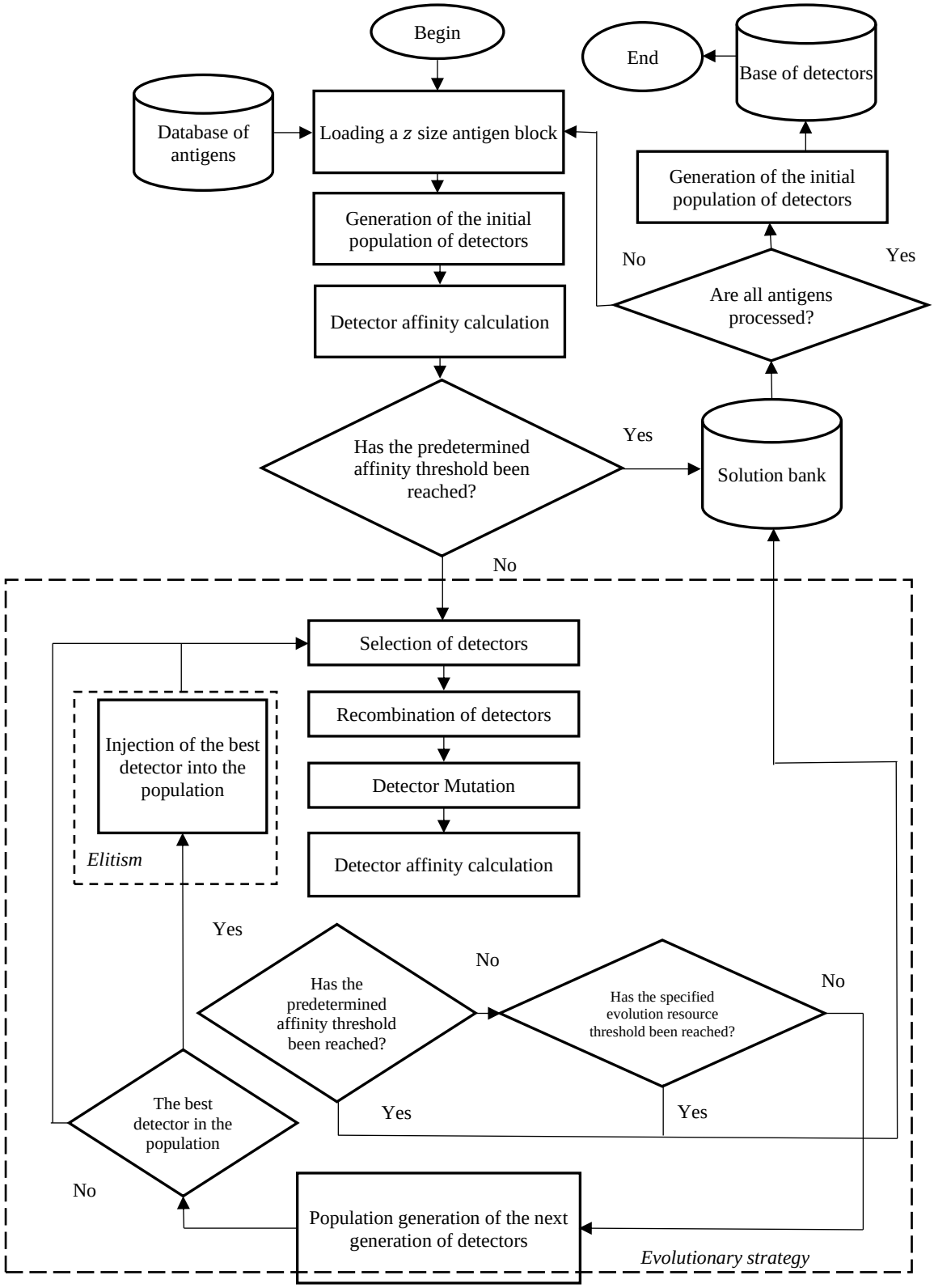

Figure 2. Scheme of generating detectors by a modified clonal selection algorithm of the artificial immune system for detecting suspicious activities

In AIS, detectors and antigens are formally represented as sets of elements of a given length over a finite alphabet. Let us assume that the power of the sets of detectors D and antigens A is the same and is set statically. In this case, the affinity of antigens with detectors is understood as a partial or complete correspondence of the element $a_j \in A$ to the element $d_j \in D$. Affinity increases

with the number of identical elements and is calculated in this research work using the metric [21] "percent agreement":

$$y = count_x(a[x] = d[x]) = \sum_{x=1}^{m} \begin{cases} 1, if\ a[x] = d[x]; \\ 0, else, \end{cases} \quad (1)$$

Were

$$m = |a| = |d|.$$

The affinity function is also the fitness function for the evolutionary algorithm. The initial population of detectors is generated using a pseudo-random number generator based on the BBS algorithm [22, 23].

At the selection stage, using the tournament selection strategy, a subset of $S \subset D$ detectors is formed, which are allowed to participate in the formation of a new generation of detectors.

At the recombination stage, using the pseudo-random number generator BBS, two elements are selected from the subset S, to which the multipoint crossing operator is applied according to the following scheme:

a) in the range $[1; M-1]$ k positions are selected using a pseudo-random number generator, and the following constraint is set:

$$k \leq \frac{1}{2} \cdot M$$

where $M -$ is the number of bits allocated for storing the detector value;

b) the generated k values are sorted in ascending order and duplicate values are removed;

c) the selected two elements of the set S exchange fragments between adjacent positions k, resulting in the formation of descendant detectors.

It is assumed that the detectors can be a certain set of encoded values of several parameters, then the steps "a" - "c" of the recombination operator are performed for each parameter separately [24, 25]. The recombination operator is executed $|S|$ times, the result is a set of descendant detectors with a power equal to $|D|$.

The mutation operator is executed for each descendant detector with probability $P_m = 1/y$, using protected division.

Proportional selection is used to form a plurality of next generation detectors.

The next step is the presence in the set of detectors of the next generation of the best detector with the highest affinity value. In the absence of such, it is added instead of the lowest affine detector.

The process of generating detectors continues until the criterion for stopping the algorithm execution is reached. The criterion for stopping the execution of the algorithm is the achievement of p generations of detectors or the 60% threshold of affinity of the set of detectors D for each antigen.

The result of the algorithm operation is the number of detected antigens in the controlled set of test data E, the number of type I errors (a regular event was detected as an abnormal (false positive)) and type II errors (an abnormal event was detected as a regular one), averaged over multiple runs [26].

In filtering mode, it processes each packet at the channel, network, and transport levels, and each of them is checked for compliance with the rules for conducting the specified process [27, 28].

Below is an experiment to detect the probability of skipping suspicious packets.

Let $x_1 -$ be a factor characterizing the use of filtering by IP addresses and $x_2 -$ be a factor characterizing the use of filtering by ports. Then:

$- x_1 = 1$- filtering by IP addresses is used;

$- x_1 = -1$ - IP address filtering is not used;

$- x_2 = 1$ - port filtering is used;

$- x_2 = -1$, - no port filtering is used.

Then $p = (x_1), (x_2) -$ probability of missing suspicious packets is determined. Denoted $p = (x_1, x_2) -$ the probability of skipping suspicious packets [4-5]. An analytical model in the form of a polynomial is used as a model of the object of the experiment

$$p = (x_1, x_2) = b_0 + b_1 x_1 + b_2 x_2 + b_3 x_1 x_2.$$

RESULT

The experiments obtained on a conventional computer are shown below. The experiment simulated the generation of 1000 TCP type packets by IP addresses and ports.

Figure 3 shows the results of the absence of filtering by IP addresses ($x_1 = -1$) and ports ($x_2 = -1$), while the factors ($x_1 = -1, x_2 = -1$) take the same values, and the probability of missing a suspicious packet $p = 0.47$.

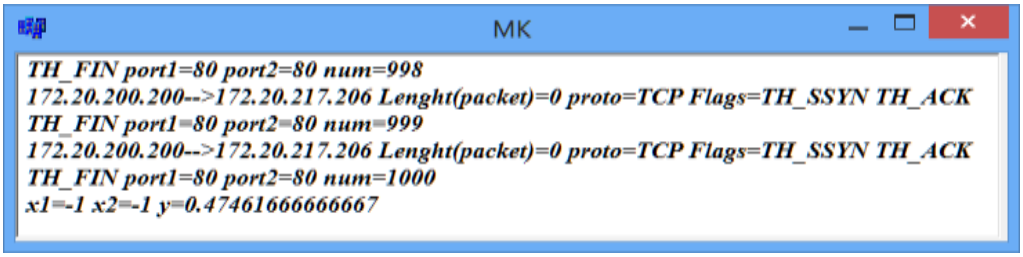

Figure 3. No filtering window by IP addresses and ports

Figure 4 shows the results of the absence of filtering by IP addresses ($x_1 = -1$) and the presence of filtering by ports ($x_2 = 1$), while the factors ($x_1 = -1, x_2 = 1$) take different values, and the probability of missing a suspicious package $p = 0.33$.

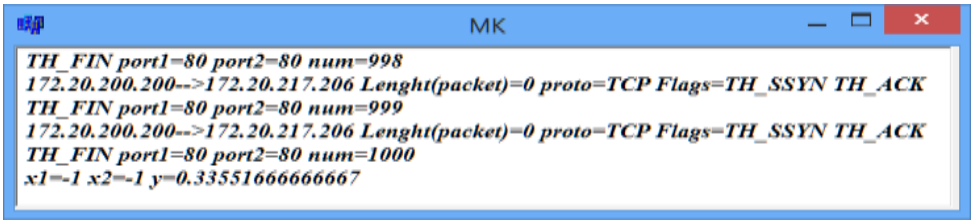

Figure 4. The window of no filtering by IP addresses and presence of filtering by ports

Figure 5 shows the results of the presence of filtering by IP addresses ($x_1 = 1$) and the absence of filtering by ports ($x_2 = -1$), while the factors ($x_1 = 1, x_2 = -1$) take different values, and the probability of missing a suspicious package $p = 0{,}32$.

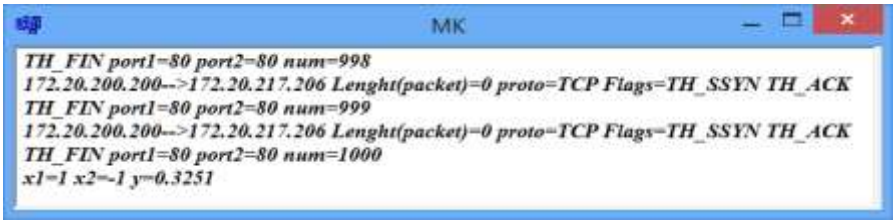

Figure 5. Window with filtering by IP addresses without filtering by ports

Figure 6 shows the results of filtering by IP addresses and by ports, with the factors ($x_1 = 1$, $x_2 = 1$) taking the same values, and the probability of missing a suspicious packet $p = 0{,}29$.

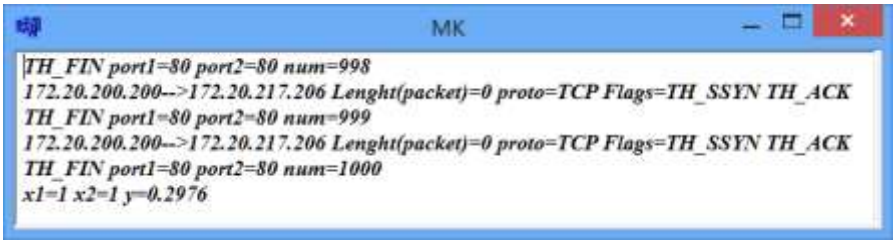

Figure 6. Filtering presence window by IP addresses by ports

Table 1 shows the values of both factors, which are measured at these points.

Table 1. The value of factors by IP addresses and port

Experiments \ Factors	x_1	x_2	$p_i = (x_1, x_2)$
Lack of filtering by IP addresses and ports	-1	-1	p_1 =0,47
Lack of filtering by IP addresses and presence of filtering by ports	-1	1	p_2 =0,33
Lack of filtering by IP addresses and presence of filtering by ports	1	-1	p_3 =0,32
Availability of filtering by IP addresses and ports	1	1	p_4 =0,29

The system of linear equations for the experiments performed has the following form:
$b_0, b_1, b_2, b_3 -$ model parameters:

$$\begin{cases} p_1 = b_0 + b_1(-1) + b_2(-1) + b_3(1) = 0{,}47 \\ p_2 = b_0 + b_1(-1) + b_2(1) + b_3(-1) = 0{,}33 \\ p_3 = b_0 + b_1(1) + b_2(-1) + b_3(-1) = 0{,}32 \\ p_4 = b_0 + b_1(1) + b_2(1) + b_3(1) = 0{,}29 \end{cases}$$

The system of linear equations is described below in matrix form and solved by the Gauss method.

$$\left(\begin{array}{cccc|c} 1 & -1 & -1 & 1 & 0{,}47 \\ 1 & -1 & 1 & -1 & 0{,}33 \\ 1 & 1 & -1 & -1 & 0{,}32 \\ 1 & 1 & 1 & 1 & 0{,}29 \end{array}\right) = \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0{,}35 \\ 0 & 1 & 0 & 0 & -0{,}04 \\ 0 & 0 & 1 & 0 & -0{,}04 \\ 0 & 0 & 0 & 1 & 0{,}02 \end{array}\right)$$

The result is
$b_0 = 0{,}35;$
$b_1 = -0{,}04;$
$b_2 = -0{,}04;$
$b_3 = 0{,}02.$

Based on the results obtained, factorial experiments were carried out:

$a_1 -$ is the main effect of factor x_1 on filtering by IP addresses;
$a_2 -$ is the main effect of factor x_2 on port filtering.

Taking into account the formulas of the factorial experiment, we obtain

$$a_1 = \frac{(p_3 - p_1) + (p_4 - p_2)}{2} = \frac{(0{,}32 - 0{,}47) + (0{,}29 - 0{,}33)}{2} = -0{,}095$$

$$a_2 = \frac{(p_2 - p_1) + (p_4 - p_3)}{2} = \frac{(0{,}33 - 0{,}47) + (0{,}29 - 0{,}32)}{2} = -0{,}085$$

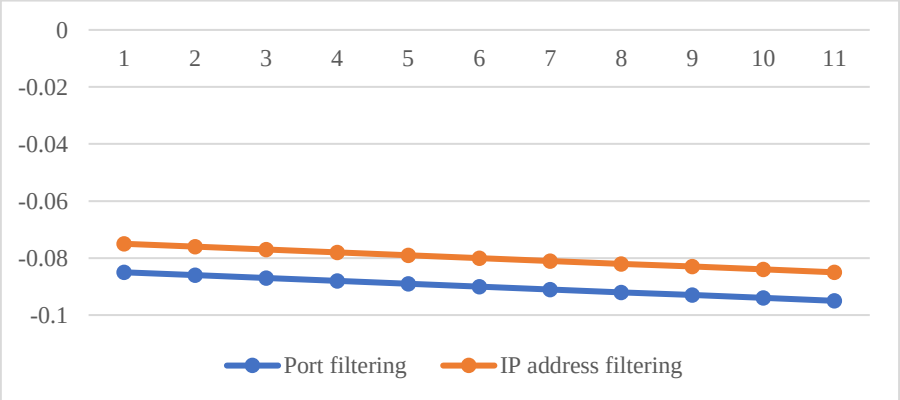

Figure 7. Result of filtering by IP addresses and by ports.

CONCLUSION

From the formula, it becomes clear that the IP address filtering factor is of greater importance than the port filtering factor.

Based on the above results, we can conclude that the detection of missing suspicious packets allows you to optimize the filtering of network packets in networks.

When building intrusion detection systems, it was found that the clonal selection algorithm of the artificial immune system is effective. When using several neural networks, the method allows increasing the probability of detecting and preventing new network attacks in computer networks. To improve the efficiency of computer networks, a modification of the clonal selection algorithm of the artificial immune system has been developed, which makes it possible to determine intentional changes in controlled data, taking into account the use of an external optimization structure.

A developed software module designed to detect distributed network denial-of-service attacks and to detect suspicious packets. It has been established that the detection of the probability of missing suspicious packets makes it possible to optimize the filtering of network packets, which ensures a high level of network security.

Declaration by Authors

Acknowledgement: None
Source of Funding: None
Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

1. Sagatov M., Irgasheva D., Mirhusan K. Construction Hardware Protection Infocommunication Systems from Network Attacks //Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE). – International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE), 2015. – pp 271.
2. Karimov M. M., Arzieva J. T., Rakhimberdiev K. Development of approaches and schemes for proactive information protection in computer networks //2022 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2022. – pp. 1-5.
3. Liu S. Computer network information security and protection measures under the background of big data //Journal of Physics: Conference Series. – IOP Publishing, 2021. – T. 1881. – №. 3. – pp. 032092.
4. Soomro Z. A., Shah M. H., Ahmed J. Information security management needs more holistic approach: A literature review //International journal of information management. – 2016. – T. 36. – №. 2. – pp. 215-225.
5. Haktanirlar Ulutas B., Kulturel-Konak S. A review of clonal selection algorithm and its applications //Artificial Intelligence Review. – 2011. – T. 36. – pp. 117-138.
6. Luo W., Lin X. Recent advances in clonal selection algorithms and applications //2017 IEEE Symposium Series on Computational Intelligence (SSCI). – IEEE, 2017. – pp. 1-8.
7. Luo W. et al. A clonal selection algorithm for dynamic multimodal function optimization //Swarm and Evolutionary Computation. – 2019. – T. 50. – pp. 100459.
8. Chen D. et al. A multi-objective trajectory planning method based on the improved immune clonal selection algorithm //Robotics and computer-integrated manufacturing. – 2019. – T. 59. – pp. 431-442.
9. Luo W., Lin X. Recent advances in clonal selection algorithms and applications //2017 IEEE Symposium Series on Computational Intelligence (SSCI). – IEEE, 2017. – pp. 1-8.
10. Liu J. et al. A novel hybrid immune clonal selection algorithm for the constrained corridor allocation problem //Journal of Intelligent Manufacturing. – 2022. – pp. 1-20.
11. Wang Y. et al. Locating and sizing of charging station based on neighborhood mutation immune clonal selection algorithm //Electric Power Systems Research. – 2023. – T. 215. – pp. 109013.
12. Hatata A. Y., Osman M. G., Aladl M. M. A review of the clonal selection algorithm as an optimization method //Leonardo Journal of Sciences. – 2017. – T. 16. – №. 30. – pp. 1-14.
13. Shang R. et al. Immune clonal selection algorithm for capacitated arc routing problem //Soft Computing. – 2016. – T. 20. – pp. 2177-2204.
14. Ojewumi T. O. et al. Performance evaluation of machine learning tools for detection of phishing attacks on web pages //Scientific African. – 2022. – T. 16. – pp. e01165.

15. Della Porta D. Deconstructing generations: Concluding remarks //American Behavioral Scientist. – 2019. – Т. 63. – №. 11. – pp. 1578-1596.
16. Aickelin U., Dasgupta D., Gu F. Artificial immune systems //Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques. – Boston, MA: Springer US, 2013. – pp. 187-211.
17. Timmis, J., Hone, A., Stibor, T., & Clark, E. (2008). Theoretical advances in artificial immune systems. *Theoretical Computer Science*, *403*(1), 11-32.
18. Corus D., Oliveto P. S., Yazdani D. Fast artificial immune systems //Parallel Problem Solving from Nature–PPSN XV: 15th International Conference, Coimbra, Portugal, September 8–12, 2018, Proceedings, Part II 15. – Springer International Publishing, 2018. – pp. 67-78.
19. Padmanabhan S. et al. Optimal solution for an engineering application using modified artificial immune system //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2017. – Т. 183. – №. 1. – С. 012025.
20. Salami M., Hendtlass T. A fast evaluation strategy for evolutionary algorithms //Applied Soft Computing. – 2003. – Т. 2. – №. 3. – pp. 156-173.
21. Catal C. Software fault prediction: A literature review and current trends //Expert systems with applications. – 2011. – Т. 38. – №. 4. – pp. 4626-4636.
22. Yu, X., Wei, X., & Lin, X. (2010). Algorithms of BBS opinion leader mining based on sentiment analysis. In Web Information Systems and Mining: International Conference, WISM 2010, Sanya, China, October 23-24, 2010. Proceedings (pp. 360-369). Springer Berlin Heidelberg.
23. Rajaboevich G. S., Mirpulatovich K. M., Yakubdjanovich T. Z. The Methodology of the Ways for Increasing the Efficiency of Intrusion Detection Systems //International Journal of Engineering Innovations and Research. – 2016. – Т. 5. – №. 5. – pp. 296.
24. Rajaboevich G. S., Mirpulatovich K. M. X., Tileubaevna A. J. Method for implementing traffic filtering in SDN networks //2022 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2022. – pp. 1-3, doi: 10.1109/ICISCT55600.2022.10146873.
25. Mirpulatovich K. M., Zakirovna T. N., Ismoilovna K. G. Classification of Modern Security Monitoring Systems in Computer Systems and Networks //International Journal of Advanced Research in Science, Engineering and Technology. – Т. 5. – №. 9. – pp. 6764-6769.
26. Malikovich K. M. et al. Differentiated Services Code Point (DSCP) Traffic Filtering Method to Prevent Attacks //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – pp. 1-4.
27. Mai, D. T. T. (2023). DDoS Attacks Detection using Dynamic Entropy in Software-Defined Network Practical Environment. International Journal of Computer Networks & Communications (IJCNC), 15, 113-128.
28. Sultan, M. T. (2023). An intrusion detection mechanism for manets based on deep learning artificial neural networks (anns). International Journal of Computer Networks & Communications (IJCNC), 15, 1-15.

How to cite this article: Sherzod Gulomov, Mirkhusan Kadirov, Nargiza Karimova. Development of a clone selection algorithm for detecting network attacks. *International Journal of Research and Review*. 2023; 10(9): 281-288. DOI: *https://doi.org/10.52403/ijrr.20230930*

******