The Neural Network Model of DDoS Attacks Identification for Information Management

Fail Fanilevich Mukhametzyanov[1], Alexey Sergeevich Katasev[2], Amir Muratovich Akhmetvaleev[2], Dina Vladimirovna Kataseva[2]

[1]*Kazan Federal University*

[2]*Kazan National Research Technical University named after AN Tupolev*

fail_muhametzyanov@mail.ru

***Abstract*— The paper discusses the concept and problem of identifying DDoS attacks for information management. The main starting mechanisms and types of DDoS attacks are analyzed. To identify them, signature and behavioral methods of analyzing network traffic are used. Analysis of the advantages and disadvantages of these methods actualized the need for their combined use. To detect and classify DDoS attacks, the need to develop and use a neural network model has been updated. The training and testing of the model were made on the initial data from the NSL-KDD set. All lines in this set are represented as sequences of TCP packets, UDP packets, and ICMP packets of network traffic transmitted from the source of the attack to the attacked network node. The total sample size was 8067 lines. Of these, half of the data corresponded to DDoS attacks, and the rest of the data characterized clear connections. The Deductor modelling environment was used to build the neural network model. The constructed neural network model was a single-layer perceptron with 11 input neurons, 23 hidden neurons and 1 output neuron. The accuracy of the constructed model was calculated based on contingency tables. The accuracy of the initial data classification at the training stage was 97.94%. The classification accuracy at the testing stage was 97.87%. To assess the quality of the neural network model, the errors of the first (0.93%) and second (3.3%) type are calculated. Testing the model showed good results since almost all DDoS attacks were successfully classified. Thus, the neural network model for detecting DDoS attacks has successfully solved the task of identifying and classifying malicious network connections.**

Keywords*— *DDoS attack, information security, neural network, classification, information management.

1. Introduction

As a rule, three basic properties of information [1] can be distinguished from the point of view of information security: confidentiality of information resources and access objects, their integrity and availability. The availability property is primarily related to the availability of information resources and the readiness of various services to service a user and program requests [2]. Today, information security incidents are increasingly occurring in various information systems related to attempts to disrupt the availability of information resources and information stored there [3]. Attacks aimed at the occurrence of these incidents relate to a type of "denial of service" attacks - DoS attacks [4]. If the attack is distributed, then it is called a DDoS attack [5].

Such attacks on information resources are the most frequent since they are relatively easy to organize using all sorts of malicious tools [6 -10]. Attackers implement DDoS attacks and, as a rule, for the purpose of additional earnings, as well as the ability to inflict material and reputational damage to a competing company. Therefore, among the objects of DDoS-attacks are often various banks and online stores, for which the loss of reputation is more important than material damage [11, 12].

2. Methods

As is well known, a DDoS attack is a distributed attack to an information system [7]. At the same time, network traffic, which characterizes DDoS attacks, is generated by several sources and, as a rule, has a single governing body. Attackers implementing this type of attack often use an attacking system that has cluster architecture. Such a system necessarily has a control mechanism that can be a computer that synchronizes the system as a whole. In addition, there is a number of main computers, as well as zombie computers, jointly generating and sending a series of requests to the attacked system. In practice, DDoS attacks are often implemented by preliminary collusion of a group of users which, at a certain point in time, all together begin to attack a selected computer or some service in an organization's information system. With a large number of users, the probability of successful implementation of such an attack is high [8-12].

Modern means of detecting DDoS attacks use both signature and behavioral methods for analyzing data transmitted over the network [9,10]. Individually, these methods have both advantages and disadvantages. Therefore, the creation of

hybrid methods for detecting DDoS attacks [11, 13-16] based on the use of both approaches is currently topical.

In this paper, a neural network model of the type of a single-layer perceptron was proposed as an effective hybrid method for solving the problem set [12,17-20]. For training and testing of the model, the NSL-KDD dataset [13, 21] from a publicly available source was used. This set is often used by developers and researchers for a comparative evaluation of the effectiveness of various intellectual analysis algorithms: neural networks [22-38], fuzzy neural networks [17], decision trees [18, 19], cluster analysis algorithms [20], etc. All entries in this set are time series [21, 22, 39] and consist of sequences of TCP packets, UDP packets, and ICMP packets of network traffic transmitted from the source of the attack to the attacked network node [40].

In the NSL-KDD data set, there are 41 parameters by which DDoS attacks are recognized. In addition, this kit describes 6 different types of DDoS attacks: Back, Land, Neptune, Ping-of-death, Smurf and Teardrop. The initial data were prepared for analysis by eliminating duplicates and inconsistencies from them, deleting records that are not relevant to the types of DDoS attacks under consideration, and also evaluating and selecting a system of informative input characteristics from the point of view of their influence on the output result [23]. In addition, during the formation of the training and test samples, the obtained data were normalized by the formula [24]:

$$N = \frac{X - X_{\min}}{X_{\max} - X_{\min}}, \quad (1)$$

Where X is the original value of the feature, $X_{\max}$ - the maximum value of the feature, $X_{\min}$ - the minimum value of the feature, N - the normalized value of the feature.

After preprocessing of the initial data, a sample ready for analysis was obtained, comprising 8068 lines, half of which characterized DDoS attacks, and the remaining data were clear compounds that did not characterize any attacks. The neural network model was built (trained and tested) on the data obtained [25].

The analytical platform Deductor was chosen as a tool for building the neural network model. This software product allows a client to download data for analysis, evaluate their quality, initialize, train and test neural network models of various architectures, as well as perform visualization of the results obtained at each stage of model construction.

Before to train a neural network, we need to determine its structure, select the appropriate neuron activation function, and also choose the algorithm used to configure the neuron weights. The structure of any neural network model is partially determined by the data of their training sample. Thus, the number of input parameters in the sample corresponds to the number of input neurons in the model, and the number of output parameters corresponds to the number of neurons in the output layer. In our case, the training sample consisted of 11 input parameters and 1 output parameter. Accordingly, the input layer of the neural network model contained eleven neurons, and the output layer consisted of a single neuron.

In this paper, a single-layer direct propagation neural network was developed to detect DDoS attacks, which is a single-layer perceptron. This network includes one layer of hidden neurons. To determine the optimal number of neurons in this layer, we use the conclusion from the Arnold – Kolmogorov – Hecht-Nielsen theorem [26]:

$$N_h \le 2 * N_{in} + 1, \quad (2)$$

Where N_{in} is the number of neurons in the input layer, and N_h is the number of neurons in the hidden layer.

Consequently, the total number of neurons contained in the hidden layer of a single-layer perceptron should be no more than 23. This follows from formula (2) taking into account the fact that the number of neurons in the input layer in a given neural network is 11. In the future, the number of neurons in the hidden layer can be reduced if, when training and testing the neural network model, this reduction will increase its accuracy.

To calculate the output values of each neuron in the hidden layer, the logistic activation function, sigmoid, is chosen; its analytical form is set by the following expression [27]:

$$f(x) = \frac{1}{1 + e^{-\alpha x}}, \quad (3)$$

Where a is the steepness of sigmoid.

To train the neural network model, the classical back-propagation error algorithm was chosen [28]. In this algorithm, the input signals propagating from the input to the output of the neural network, as a rule, give the root-mean-square output error of a certain magnitude. To reduce this error, a phase of the reverse propagation of the signal is performed, at which the weights are adjusted.

3. Results and Discussion

In order to assess the accuracy of the trained neural network, an adjacency matrix was constructed, which is presented in Table 1.

Table 1. Results of the trained neural network accuracy evaluation

	The result of neural network classification		
Actual data	False	True	Total
False	3855	145	4,000
True	21	4046	4067
Total	3876	4191	8067

According to the data from the presented table, the accuracy of the neural network model was calculated at the stage of its training, the accuracy was 97.94%.

To assess the generalizing ability of the trained neural network, a test data sample was used; it contains 1500 lines, half of which characterize DDoS attacks, and the remaining data is clear connections. Table 2 presents the results of the neural network model testing.

Table 2. The classification results for the data from the test sample

	The result of neural network classification		
Actual data	False	True	Total
False	725	25	750
True	7	743	750
Total	732	768	1500

According to the data from the table, the accuracy of the neural network model was calculated at the testing stage; the accuracy was 97.87%.

For the purpose of a more detailed assessment of the trained neural network accuracy, errors of type I and type II were obtained using test data. In this case, the type I error is considered to be network connections related to DDoS attacks but classified by the neural network as clear connections. Accordingly, a type II error is considered to be network connections that are not related to DDoS attacks but classified by a neural network as DDoS attacks.

The formula for calculating a type I error is as follows:

$$E_1 = \frac{n_1}{N_1} * 100\% \quad (4)$$

Where n_1 is the number of records in the test sample of data related to DDoS attacks but classified by the neural network as clear records;

N_1 is the total number of rows in a test sample of data related to DDoS attacks.

The formula for calculating a type II error is as follows:

$$E_2 = \frac{n_2}{N_2} * 100\% \quad (5)$$

where n_2 is the number of records in the test sample of data not related to DDoS attacks but classified by a neural network as a DDoS attack;

N_2 is the total number of clear network connections in the test data sample.

The numerical value of the type I error is calculated as:

$$E_1 = \frac{n_1}{N_1} * 100\% = \frac{7}{750} * 100\% = 0{,}93\%$$

;

The value of the type II error:

$$E_2 = \frac{n_2}{N_2} * 100\% = \frac{25}{750} * 100\% = 3{,}3\%$$

.

Errors of the first and second types turned out to be insignificant, which indicates the high efficiency of the constructed neural network model in solving the problem of detecting DDoS attacks.

4. Summary

According to the results of the research, it can be concluded that, despite the difficulty of identifying DDoS attacks, neural networks do a good job with this task. In all the experiments carried out related to the training and testing of the constructed neural network model, as well as with the calculation of the error values of the first and second type, the neural network showed high accuracy. Consequently, the neural network model is adequate and allows effectively to solve the problem of identifying and classifying DDoS attacks in computer systems and networks.

5. Conclusions

Thus, we can conclude that the neural network described in this paper is an effective tool for solving the problems posed and is suitable for use in decision support systems for detecting DDoS attacks. In the future, with the aim of developing a solution to this problem, it is planned to develop and test other methods and data analysis algorithms [29-36], as well as assess and compare the effectiveness of various approaches to identifying, classifying DDoS attacks and resisting them.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. This work was

supported by the Russian Federation Ministry of Education and Science, project № 8.6141.2017/8.9.

References

[1] Kravchenko Y., Vialkova V. The problem of providing functional stability properties of information security systems // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016. – P. 526-530.

[2] Olaode J.A. An operational model situation in ensuring availability of information security through the help of satellite communication infrastructures in digital society // Proceedings of the 2018 IEEE Communication Strategies in Digital Society Workshop, ComSDS 2018. – P. 42-45.

[3] Vance A., Lowry P.B., Eggett D. Using accountability to reduce access policy violations in information systems // Journal of Management Information Systems. – 2013. – No. 29(4). – P. 263-289.

[4] Chen H.-C., Kuo S.-S. DoS Attack Pattern Mining Based on Association Rule Approach for Web Server // Advances in Intelligent Systems and Computing. – 2019. – No. 773. – P. 527-536.

[5] Serrano Mamolar A., Pervez Z., Alcaraz Calero J.M., Khattak A.M. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks // Computers and Security. – 2018. – No. 79. – P. 132-147.

[6] Mahjabin S. Implementation of DoS and DDoS attacks on cloud servers // Periodicals of Engineering and Natural Sciences. – 2018. – No. 6(2). – P. 148-158.

[7] Saied A., Overill R.E., Radzik T. Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept // Communications in Computer and Information Science. – 2014. – No. 430. – P. 300-320.

[8] Xiang G., Xin Z., Xiao W. The design and implementation of IP traceback method of DDoS attack using fastICA traffic analysis // Journal of Convergence Information Technology. – 2012. – No. 7(23). – P. 57-65.

[9] Jeong S., Yoo H.H. Nonlinear structural analysis of a flexible multibody system using the classical Rayleigh–Ritz method // International Journal of Non-Linear Mechanics. – 2019. – No. 110. – P. 69-80.

[10] Sato T., Akamatsu M. Analysis of drivers control methods of task demands based on behavioral data in actual road environments // Proceedings of the SICE Annual Conference. – 2011. – P. 2137-2142.

[11] Jia B., Huang X., Liu R., Ma Y. A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning // Journal of Electrical and Computer Engineering. – 2017,4975343.

[12] Amato F., Cozzolino G., Mazzeo A., Vivenzio E. Using multilayer perceptron in computer security to improve intrusion detection // Smart Innovation, Systems and Technologies. – 2018. – No. 76. – P. 210-219.

[13] Wutyi K.S., Thwin M.M.S. Heuristic rules for attack detection charged by NSL KDD dataset // Advances in Intelligent Systems and Computing. – 2016. – No. 387. – P. 137-153.

[14] Mustafin A.N., Katasev A.S., Akhmetvaleev A.M., Petrosyants D.G. Using models of collective neural networks for classification of the input data applying simple voting // Journal of Social Sciences Research. – 2018. – Special Issue 5. – P. 333-339.

[15] Katasev A.S., Kataseva D.V. Neural network diagnosis of anomalous network activity in telecommunication systems // Proceedings of IEEE Conference Dynamics of Systems, Mechanisms and Machines, Dynamics 2016.

[16] Jannela V., Rodda S., Uppuluru S.N., Koratala S.C., Chandra Mouli G.V. Performance analysis of NSL_KDD data set using neural networks with logistic sigmoid activation unit // Smart Innovation, Systems and Technologies. – 2018. – No. 77. – P. 171-181.

[17] Katasev A.S., Kataseva D.V., Emaletdinova L.Yu. Neuro-fuzzy model of complex objects approximation with discrete output // Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016.

[18] Ingre B., Yadav A., Soni A.K. Decision tree based intrusion detection system for NSL-KDD dataset // Smart Innovation, Systems and Technologies. – 2018. – No. 84. – P. 207-218.

[19] Hota H.S., Shrivas A.K. Decision tree techniques applied on NSL-KDD data and its comparison with various feature selection techniques // Smart Innovation, Systems and Technologies. – 2014. – No. 27(VOL 1). P. 205-212.

[20] Vinutha H.P., Poornima B. Analysis of NSL-KDD dataset using k-means and canopy clustering algorithms based on distance metrics // Studies in Computational Intelligence. – 2019. – No. 771. – P. 193-200.

[21] Perfilieva I.G., Yarushkina N.G., Afanasieva T.V., Romanov A.A. Web-based system for enterprise performance analysis on the basis of time series data mining // Advances in

Intelligent Systems and Computing. – 2016. – No. 450. P. 75-86.

[22] Romanov A., Filippov A., Yarushkina N. Extraction and forecasting time series of production processes // Studies in Systems, Decision and Control. – 2019. – No. 199. – P. 173-184.

[23] Akhmetvaleev A.M., Katasev A.S. Neural network model of human intoxication functional state determining in some problems of transport safety solution // Computer Research and Modeling. – 2018. – Vol. 10, No. 3. – P. 285-293.

[24] Ismagilov I.I., Khasanova S.F., Katasev A.S., Kataseva D.V. Neural network method of dynamic biometrics for detecting the substitution of the computer // Journal of Advanced Research in Dynamical and Control Systems. – 2018. – No. 10(10 Special Issue). – P. 1723-1728.

[25] Emaletdinova, L.Y., Matveev, I.V., Kabirova, A.N. Method of designing a neural controller for the automatic lateral control of unmanned aerial vehicles // Russian Aeronautics. – 2017. – No. 60(3). – P. 365-373.

[26] Hecht-Nielsen R. Kolmogorov's mapping neural network existence theorem // IEEE First Annual International Conference on Neural Networks. – San Diego, 1987. – Vol. 3. – P. 11-13.

[27] Zadeh M.R., Amin S., Khalili D., Singh V.P. Daily Outflow Prediction by Multi-Layer Perceptron with Logistic Sigmoid and Tangent Sigmoid Activation Functions // Water Resources Management. – 2010. – No. 24(11). – P. 2673-2688.

[28] Li Y., Zhao J., Ji S. Thermal positioning error modelling of machine tools using a bat algorithm-based back propagation neural network // International Journal of Advanced Manufacturing Technology. – 2018. – No. 97(5-8). – P. 2575-2586.

[29] Anikin I.V., Makhmutova A.Z., Gadelshin O.E. Symmetric encryption with key distribution based on neural networks // Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016.

[30] Katasev A.S., Kataseva D.V. Expert diagnostic system of water pipes gusts in reservoir pressure maintenance processes // Proceedings of 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2016.

[31] Ceisil U. E-Awareness of University Student through Smart Phones and Developing Social Networks. Journal of Humanities Insights. 2018;02(03):139-45.

[32] Hosseini Z, Farzadnia E, Riahi A. Improvement of Company Financial Performance through Supply Chain and Review of Human Resource Effects on it. Journal of Humanities Insights. 2017;01(01):1-6.

[33] Kumar S, Gapta V. Advantages and Disadvantages of Social Websites on Young Students. Journal of Humanities Insights. 2017;01(01):34-6.

[34] Roopit K. Providing Location Privacy of Vehicle through a Real Time Implementation of Short Range Communication. Journal of Humanities Insights. 2018;02(04):156-60.

[35] Saraninezhad M, Ramezany M. Optimal Placement of Wind Turbines for Reducing Losses and Improving Loadability and Voltage Profile in Distribution Networks by Data Clustering and NSGA-II Algorithm. Medbiotech Journal. 2019;03(02):77-83.

[36] Kord, H., Noushiravani, Y., Bahadori, M. D., & Jahantigh, M. (2017). Review and Analysis of Telework Perspective in the Administrative Systems. *Dutch Journal of Finance and Management, 1*(2), 44. https://doi.org/10.29333/djfm/5820

[37] Tian, L., Thalmann, N. M., Thalmann, D., & Zheng, J. (2019). Nature grasping by a cable-driven under-actuated anthropomorphic robotic hand. *Telkomnika*, *17*(1).

[38] Villalón, J. C., Agustin, G. C., Gilabert, T. S. F., & Puello, J. D. J. J. (2016). A review of software project testing. *Journal of Information Systems Engineering & Management, 1*(2), 141-148. https://doi.org/10.20897/lectito.201619

[39] Deyhim, T., & Zeraatkish, y. (2016). Investigate the trend of rural development in Gachsaran city with Morris method. *UCT Journal of Management and Accounting Studies, 4*(1), 23-28.

[40] Puspitasari, L., In'am, A., & Syaifuddin, M. (2019). Analysis of Students' Creative Thinking in Solving Arithmetic Problems. *International Electronic Journal of Mathematics Education, 14*(1), 49-60. https://doi.org/10.12973/iejme/3962