DOI: 10.18721/JCSTCS.13303
УДК 004.492.3

TECHNIQUES FOR HYBRIDIZATION OF INTELLIGENT METHODS FOR DETECTING MALICIOUS TRAFFIC

V.E. Chumakov

Don State Technical University,
Rostov-on-Don, Russian Federation

In the modern world of IT technologies, there is a trend of ever-increasing flow of network traffic, network connections and, consequently, a growing number of vulnerabilities of centralized and decentralized systems. The urgency of the research lies in the necessity to modernize and improve existing mechanisms for better malicious traffic detection and enhanced security of the entire network infrastructure. The paper presents a new approach to network traffic research. The advantages of the proposed techniques are given in comparison with modern intrusion detection system based on standard algorithms and intelligent methods. The article indicates the direction in the area of modernization and improvement of algorithms for detection of network anomalies and network intrusions. The main features of the network traffic classification subsystem and the logic of work of each stage are displayed, the results of the system research and testing are presented, recommendations on the application and practical significance of the developed algorithm are described.

Keywords: IDS, IPS, security, network anomalies, intelligent methods.

Citation: Chumakov V.E. Techniques for hybridization of intelligent methods for detecting malicious traffic. Computing, Telecommunications and Control, 2020, Vol. 13, No. 3, Pp. 31–43. DOI: 10.18721/JCSTCS.13303

МЕТОДИКА ГИБРИДИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ ДЛЯ РАСПОЗНАВАНИЯ ЗЛОВРЕДНОГО ТРАФИКА

В.Е. Чумаков

Донской государственный технический университет,
Ростов-на-Дону, Российская Федерация

В современном мире IT-технологий наблюдается тенденция постоянно растущего потока сетевого трафика, сетевых подключений и соответственно постоянно растущего количества уязвимостей централизованных и децентрализованных систем. Актуальность темы заключается в необходимости модернизации и усовершенствования уже существующих механизмов для более точного распознавания зловредного трафика и повышения уровня защищенности всей сетевой инфраструктуры. Представлен новый подход к исследованию сетевого трафика. Описаны преимущества предлагаемой методики по сравнению с современными системами обнаружения вторжений, основанными на стандартных алгоритмах и интеллектуальных методах. Обозначены направления в области модернизации и усовершенствования алгоритмов по обнаружению сетевых аномалий и сетевых вторжений. Отображены основные моменты работы подсистемы классификации сетевого трафика и логика работы каждого этапа, представлены результаты исследования и тестирования системы, описаны рекомендации по применению и практической значимости разработанного алгоритма.

Ключевые слова: IDS, IPS, безопасность, сетевые аномалии, интеллектуальные методы.

Ссылка при цитировании: Чумаков В.Е. Методика гибридизации интеллектуальных методов для распознавания зловредного трафика // Computing, Telecommunications and Control. 2020. Vol. 13. No. 3. Pp. 31–43. DOI: 10.18721/JCSTCS.13303

Introduction

At present, the quality of commercial information provides the required economic benefits for any line of business of modern company, so it becomes important to find methods to protect mission-critical data from malfeasance. This allows companies to compete successfully in the labor market.

However, the methods applied in modern systems are not sufficiently effective and use outdated algorithms, provided that the exact characteristics of the attacks are known [2–5, 11–15]. Consequently, network attacks are constantly changing, and network traffic has become imperfect information, which includes data that is not completely reliable, inaccurate, or uncertain.

In view of this, it can be concluded that nowadays to provide an adequate level of network security the use of intrusion and anomaly detection systems (IDS/ADS) is a priority in the construction of network infrastructure of any company.

The aim of the developed method is to increase the efficiency of the IDSs through the proposed techniques for hybridization of intelligent methods.

Scientific novelty lies in the developed method of combined attack detection with the help of a two-level algorithm for detecting contention mechanisms when classifying mixed network traffic and the possibility of assigning arbitrary nesting of data about a network connection, thereby making it possible to work with "raw" data rather than using a well-structured signature base structure, which means that hardware attachment disappears when network anomalies are detected.

Existing methods of operation with the IDS/ADS

Modern IDS and ADS are modular architectures and typically consist of three modules, as follows:

1) The information gathering subsystem module, which serves to accumulate primary information on the network infrastructure portion protected and collects information both on the circulating network flow of the enterprise and on the services in operation, and software on protected workstations [1].

2) The module of the analysis subsystem assumes all the functions of detecting intrusion into the network infrastructure by using the existing analyzers which at the system output either confirm the fact of a host being hacked or a penetration into the enterprise network occurring, or disprove the existence of these actions by detecting the response of several types, such as false positive or false negative discoveries. As a rule, such a module works according to the Bayesian statistics rule, using the following common formula:

$$P\left(I\middle|\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\right) = P\left(\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\middle|I\right)\frac{P(I)}{P\left(\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n\right)}, \quad (1)$$

where I is responsible for detected intrusions, $\mathrm{A}_1, \ldots, \mathrm{A}_n$ is a recorded sequence of events, while each individual event of Am is a feature accumulation for calculating the estimate of the protected infrastructure, and $P(I \mid \mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n)$ is the empirical probability of the intrusion into the network infrastructure.

3) The event alert subsystem module which is recorded by the IDS/ADS, in some cases with the possibility of access rights differentiation as several information security officers responsible for monitoring the various parts of the network infrastructure often work in the same enterprise.

In addition to the conventional and constantly modernized IDSs, there are also developments similar to the system proposed by the author based on the use of neural networks or fuzzy logic [2–5] used. In the next section, we will present the advantages of the proposed system as compared to the IDS/ADS and the systems being developed based on intelligent methods.

Advantages of the proposed system

After analysis and empirical research, it can be concluded that the existing IDSs have the malfunction module algorithm shown in Fig. 1 and the following drawbacks.

Modern IDS/ADS work on the principle of previously developed antivirus solutions, but to detect intrusions instead of malicious section of the code, the malicious section of the record in the header of the resulting frame is used, which is compared with the available IDS/IPS signature base. Thus, all the above

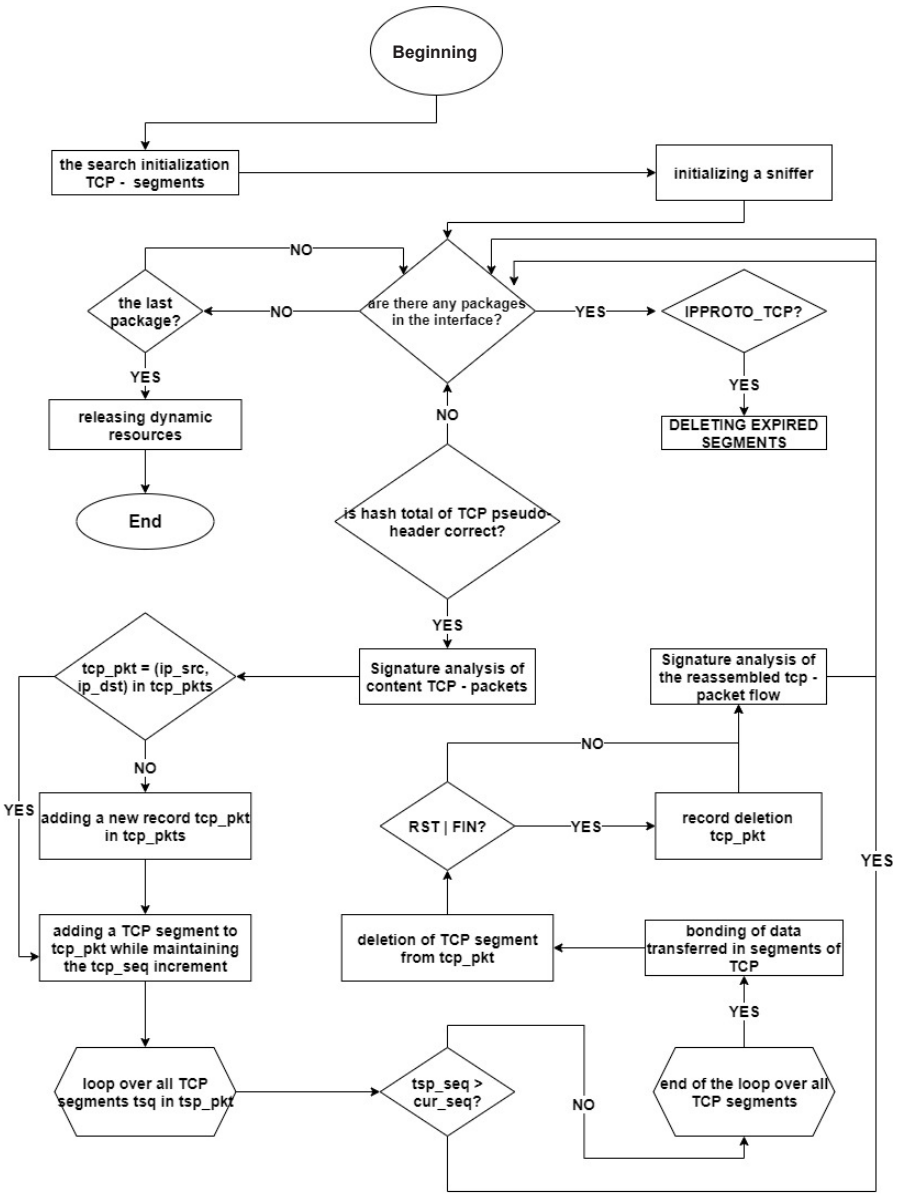

Fig. 1. Standard criteria selection algorithm

mentioned solutions start their activities when a section of the network infrastructure has already become contaminated. The signature base must be constantly updated as well, otherwise the system can miss malicious traffic due to outdated information. Thus, the flow of network traffic is exposed to zero-day attacks.

Existing systems based on the use of intelligent methods have other disadvantages. The systems developed on the basis of neural networks are not used in the branch under consideration due to the prolonged model training and the inflexible structure of work. This causes some difficulties in operation with network traffic, due to the constantly updated protocols, services and service quality elements (QoS) [6]. Systems developed on the basis of fuzzy logic have a very complex business logic of the work of the whole system, due to the constantly upgradable mathematical model of the system operation, which in its turn increases the malicious traffic detection time, and have a rule base too large to trigger the activation function, thereby increasing the number of false-negative responses [7].

The hybridization method proposed by the author is primarily aimed at work with input traffic. The first step of the proposed system is to pre-process raw data through the machine-learning algorithms. This reduces the load on the fuzzy logic module and the number of rules in the rule base by a several-fold factor, thereby reducing the operating time of the accumulative apparatus of the activation function triggering.

Research methodology

Currently, network traffic is standardized under different protocols of the common OSI model, which consists of seven levels and allows different network devices to interact with each other [8]. However, for an intelligent IDS, the input network flow is raw data and a heap about incoming frame, with introductory information such as flags, window sizes, packet length and various headers.

The empirical investigation involved the Friday_DDos array, which contains a classified set of weekly network traffic with a number of attacks of different type [9]. The array used consists of 80 columns indicating criteria and 215000 rows indicating the number of network connections received.

As discussed earlier, the standard criteria selection methods have very complex business logic, consisting of different triggers for a positive response to one of the parameters, such as whether the last packet is used in a session, whether the batch total is correct, which protocol is used. Therefore, all these parameters slow down the system, which in its turn destabilizes the flexibility, modularity and the operating principle of the system in real time.

The method of using machine-learning algorithms proposed by the author makes it possible to correct the deficiencies described above. Thus, machine-learning algorithms to recognize already classified attacks in the Friday_DDos set were compared, the results of comparisons are presented in Table 1.

Table 1

Results of comparison of machine-learning algorithms

	Accuracy, %
Principal Components Analysis (PCA)	76
Logistic regression	99.7
Support vector machine (SVM)	99.2
K-mean method	99.5
Feedforward neural networks (FF)	89
Decision trees	99

Based on the above table, it can be concluded that four algorithms have shown the highest recognition accuracy, but only one algorithm, namely the decision tree algorithm, allows for the informative visualization of distribution of the recognition weights. This algorithm was chosen, because the visualization gives

the information security officer a great idea of the stability of the recognition system and the absence of false positive and negative responses.

Because the data set used consists of multiple features, the task of identifying the main attribute that will be located in the root tree is a complex process. To solve this problem, the algorithm uses several additional operations. Consider each of them.

Entropy is used as a definition of the coefficient dimensionality of the information to be analyzed. It is worth noting that the higher the indicator, the more difficult it is to draw conclusions when collecting data. This parameter is defined by the formula:

$$\mathrm{E}(\mathrm{T}, X) = \sum_{c \in X} P(c)\mathrm{E}(c), \tag{2}$$

where T shows the state of the object, X describes the selected criterion, c is one of the notations in the term set, and E is the probability of the object belonging to a process.

IG is a process that reduces the value of entropy, which is calculated by the following formula:

$$\mathrm{IG} = Entropy(before) - \sum_{j=1}^{K} Entropy(j, after), \tag{3}$$

where (*before*) is a state of the dataset before the partition, (*j*, *after*) is respectively a state after partition, K is a number of criteria that are generated for the further partition.

Gini is a specialized index that determines the value of each element in which the dataset is divided. It is calculated by the formula:

$$\mathrm{Gini} = 1 - \sum_{i=1}^{c} (p_i)^2, \tag{4}$$

where c is also one of the elements of the state and p is defined by the target variable of success.

GR is defined by a gain factor that helps to solve the problem of data increase during the dataset partition, taking into account the number of branches that will grow as the most significant coefficients are determined. The formula is as follows:

$$\mathrm{GR} = \frac{IG}{SI} = \frac{Entropy(before) - \sum_{j=1}^{k} Entropy(j, after)}{\sum_{j=1}^{k} w_j \log_2 w_j}, \tag{5}$$

where (*before*) is a dataset before the partition by criteria, k is a number of the selected parameters for the partition, (*j*, *after*) is a subset obtained after the partition of the dataset.

As a result of the operation of the selected algorithm of 80 indicators, the input data is reduced to 4, as shown in Fig. 2. Thus, we have 3 levels of immersion and only 4 indicators by which we can classify the traffic as malicious, by means of the following piece of code shown in Listing 1.

After an analytical review of the existing classification methods, it can be concluded that modern solutions have a number of shortcomings, namely:

– The input data of such systems is a crisp set like $\{X, \mu^*A(x)\}$, where $\mu^*A(x)$ is an ownership function, which in its turn forces the systems to standardize their solutions to a certain traffic array, thereby skipping and not identifying zero-day threats.

```
dot_data = StringIO()
dt_feature_names = list(X)
export_graphviz(clf, out_file=dot_data,
filled=True, rounded=True,
special_characters=True,class_names=['Benign','Ddos'],max_depth=3,
feature_names=dt_feature_names)
graph = pydotplus.graph_from_dot_data(dot_data.getvalue())
Image(graph.create_png())
```

Listing 1. Start of the Decision Trees algorithm

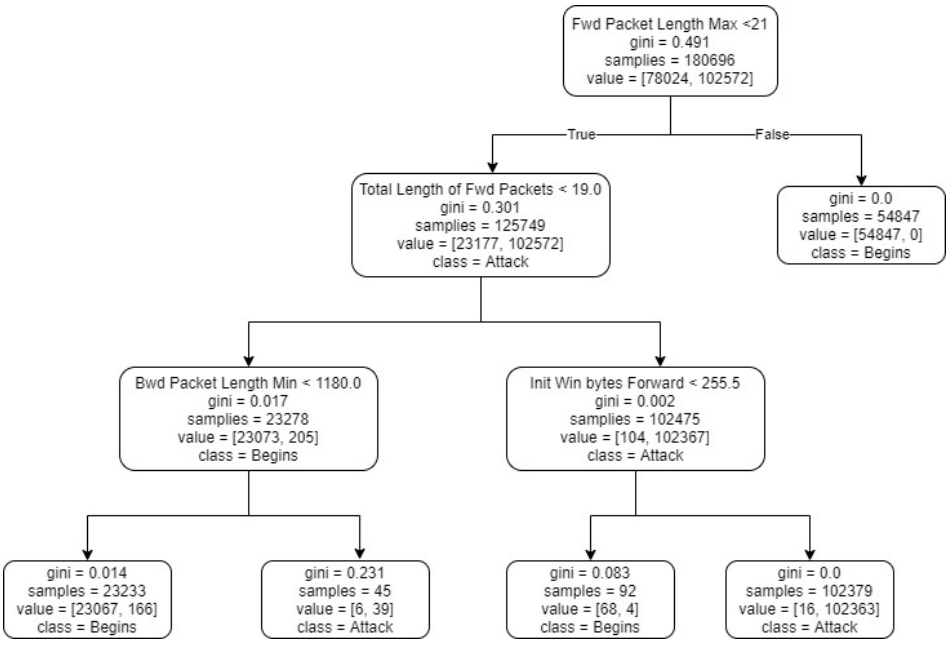

Fig. 2. Result of the algorithm operation

– As an activation function, a condition of compliance with a signature base within the standard solutions and a set of several activation functions with fuzzy logic to partition a strongly expanding rule base are used.

– The size of the rule base is hundreds of thousands of conditions for different protocols, various levels of interaction, and distinct scenarios of potential penetrations into the network infrastructure.

The solution for hybridization of machine-learning algorithms and fuzzy logic proposed by the author makes it possible to eliminate the listed disadvantages. It is proposed to use the Mamdani architecture as a fuzzy logic model, which in our case consists of 4 input functions obtained after the operation of the machine-learning algorithm, the module of calculation and activation of the activation function, and 1 output function, which is responsible for the classification of traffic as legitimized, malicious or mixed. The structure of this model is shown in Fig. 3.

As an activation function, we use a triangular function that has three points (a, b, c), two of which determine the position on the X-axis and one which is the vertex of the triangular function determining

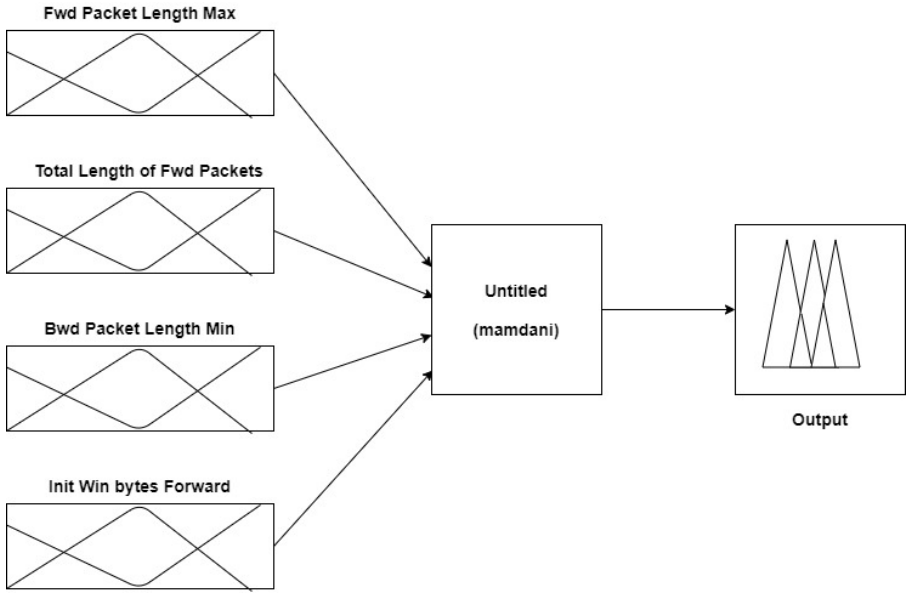

Fig. 3. Mamdani model structure

the position on the Y-axis [10]. According to this function, its value F (x) is calculated by the following formula:

$$F(x) = \begin{cases} 1 - \dfrac{b-x}{b-a}, & a \le x \le b, \\ 1 - \dfrac{x-b}{c-b}, & b \le x \le c, \\ 0, & x \notin (a;d). \end{cases} \quad (6)$$

After processing raw data as incoming network traffic and identifying markers through machine-learning algorithms, fuzzy logic model identification and activation function construction, direct recognition of incoming network connections is carried out in several steps, namely:

1. The first step is a procedure of fuzzification. At this stage, the degree of ownership of the function for the extremities of each input variable was determined. To do this, the following code fragment, shown in Listing 2, must be executed:

```
Fwd_lo = fuzz.trimf(Fwd_Packet_Length_Max, [0, 0, 21])
Fwd_md = fuzz.trimf(Fwd_Packet_Length_Max, [17, 20, 25])
Fwd_hi = fuzz.trimf(Fwd_Packet_Length_Max, [22, 27, 27])
Total_lo = fuzz.trimf(Total_Length_of_Fwd_Packets, [0, 0, 19])
Total_md = fuzz.trimf(Total_Length_of_Fwd_Packets, [10, 18, 22])
Total_hi = fuzz.trimf(Total_Length_of_Fwd_Packets, [21, 27, 27])
Init_lo=fuzz.trimf(Init_Win_bytes_forward,[0,0,255])
Init_md=fuzz.trimf(Init_Win_bytes_forward,[220,250,300])
Init_hi=fuzz.trimf(Init_Win_bytes_forward,[260,300,300])
Bwd_lo = fuzz.trimf(Bwd_Packet_Length_Min,[0,0,1180])
Bwd_md=fuzz.trimf(Bwd_Packet_Length_Min,[900,1180,1300])
```

```
Bwd_hi=fuzz.trimf(Bwd_Packet_Length_Min,[1190,1300,1300])
tip_lo = fuzz.trimf(x_tip, [0, 0.2, 0.5])
tip_md = fuzz.trimf(x_tip, [0.5, 0.65, 0.79])
tip_hi = fuzz.trimf(x_tip, [0.8, 0.89, 1])
```

Listing 2. Start of the procedure of fuzzification

2. This was followed by a cut off procedure for one part of a separate rule and ownership function. To do this, the following code fragment shown in Listing 3 must be executed:

```
tip_activation_lo = np.fmin(active_rule6, tip_lo)
tip_activation_md = np.fmin(serv_level_md, tip_md)
tip_activation_hi = np.fmin(active_rule7, tip_hi)
```

Listing 3. Start of the cut off procedure

3. Then the truncations of the function obtained at the second stage were accumulated by calculating the maximum value from the presented fuzzy sets. To do this, the following code fragment shown in Listing 4 must be executed:

```
active_rule1 = np.fmax(qual_level_lo, serv_level_lo)
active_rule4=np.fmax(active_rule1,Init_level_lo)
active_rule6=np.fmax(active_rule4,bwd_level_lo)
active_rule3 = np.fmax(qual_level_hi, serv_level_hi)
active_rule5=np.fmax(active_rule3,Init_level_hi)
active_rule7=np.fmax(active_rule5,bwd_level_hi)
```

Listing 4. Start of the accumulation procedure of the truncated functions

4. The final step is a defuzzification procedure. That is, at this stage, fuzzy procedures were brought to crisp sets in order to obtain a crisp classification of traffic according to one of the indicators contained in the term set. The centroid method and the following fragment of the code shown in Listing 5 were used for defuzzification:

```
aggregated = np.fmax(tip_activation_lo,
                     np.fmax(tip_activation_md, tip_activation_hi))
tip = fuzz.defuzz(x_tip, aggregated, 'centroid')
tip_activation = fuzz.interp_membership(x_tip, aggregated, tip)
```

Listing 5. Start of the defuzzification procedure

After the completed stages, the system was tested for recognition of the legitimacy of traffic, potential attack, zero-day attack and the actual state of the system during the penetration.

Thus, when the values of the attributes selected by the machine-learning algorithm are like presented in the figure below the operation of the algorithm is tested.

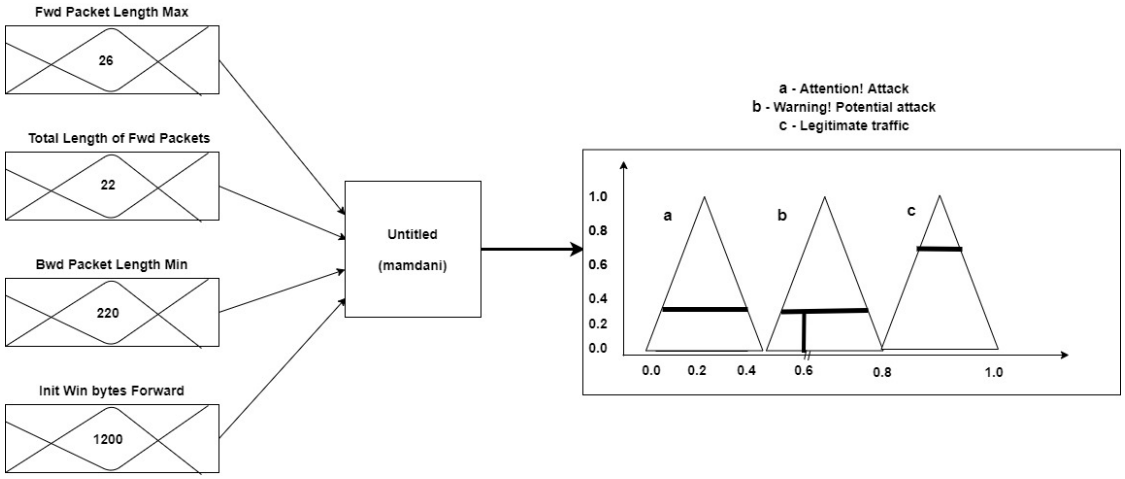

Fig. 4. Recognition testing on the potential penetration into the network infrastructure

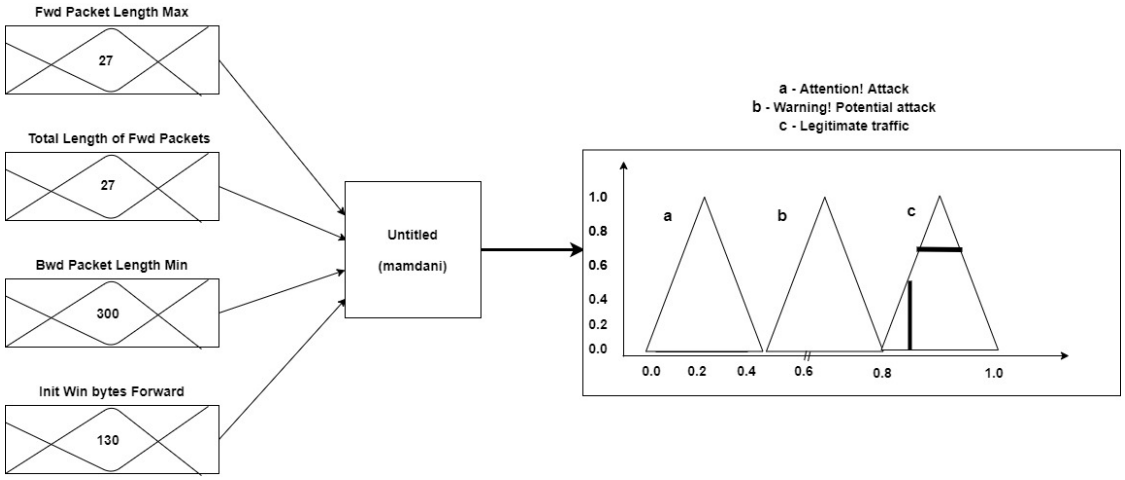

Fig. 5. System testing to classify network legitimate traffic

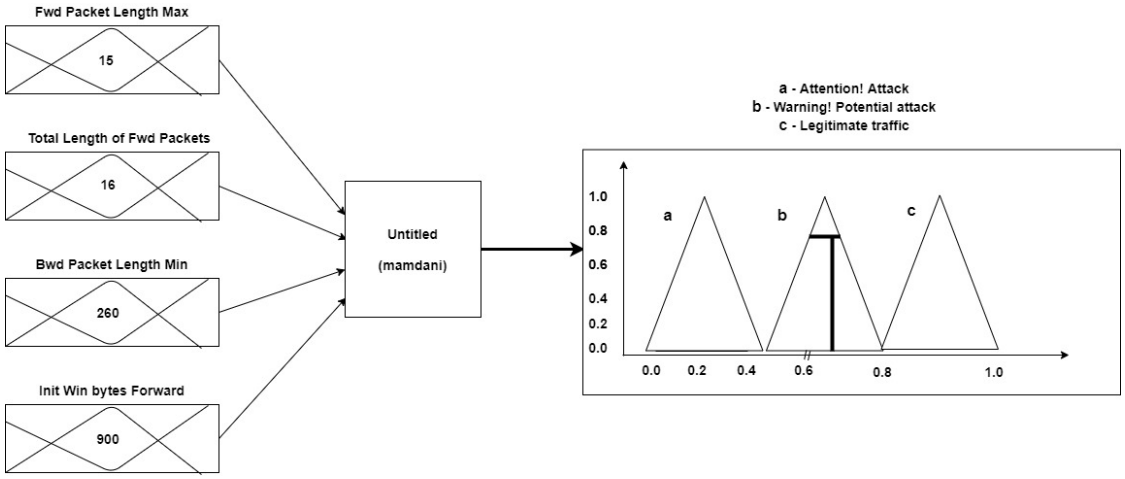

Fig. 6. Recognition testing on zero-day vulnerability

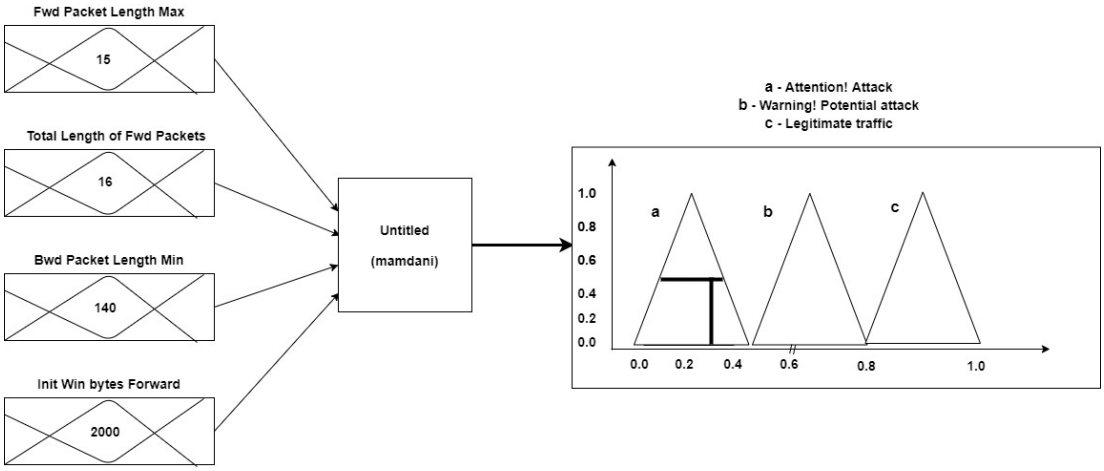

Fig. 7. System testing for current attack recognition

After a series of experiments, it can be concluded that the system performs its task and classifies network traffic as a potential attack (Fig. 4), legitimate traffic (Fig. 5), a zero-day attack (Fig. 6) or a current attack (Fig.7).

Conclusion

In conclusion we can say that the developed technique for hybridization of intelligent methods based on the preprocessing of network traffic, through the machine-learning algorithm and subsystem operation of fuzzy logic for recognition of malicious traffic, enables a reduction of a number of false responses and improves the efficiency of detecting network anomalies by an average of 15-17 % compared to the standard methods in the field under consideration.

The advantages of the developed technique include the possibility to reduce the rule base for fuzzy logic subsystem by 16 % compared to the existing IDS developments based on fuzzy logic, due to the preprocessing of raw data and reducing key parameters by a several-fold factor, on the basis of which the network traffic classification is carried out. As a result of system testing for 215000 connections after data preprocessing, only 4 parameters have been selected and the rule base has only 6 rules.

Thus, a technique for combined searching of attacks based on the detecting of abuse and network anomalies has been developed during the study. A new approach to network traffic processing is presented, which consists in predicting the target variable value on the basis of several variables at the input rather than on the use of known signature bases. The advantages of the proposed anomaly detection system architecture are shown and the results of the testing on weekly network traffic are given.

It can be concluded that the developed approach completely fulfils the given tasks and can be used both to detect the known, previously encountered attacks and to detect the new ones. The algorithm makes it possible to reduce the number of questionable and controversial responses and can also be used in the development of new solutions for detecting network anomalies and malicious network traffic.

REFERENCES

1. **Le C.M., Fang H.A., Nguyen A.C., Nguyen C.T.** Integrated IDS/IPS Open-Source Model with Improved Machine Learning. *Results of Applied and Research Studies in Natural History and Technology: Compendium of Scientific Papers on the Proceedings of the International Scientific and Practical Conference on 27 Dec. 2019.* Belgorod: LLC Advanced Scientific Research Agency (APNI), 2019. Pp. 81–87. Available: https:///apni.ru/article/152-integrirovannaya-sipidsips-model-mezh-duotkr

2. **Chumakov V.E.** Analysis of Modern Methods of Network Infrastructure Security. International Journal of Applied Sciences and Technology. Collection 4, 2019. Available: *https:///e-integral.ru/rubriki/tehnicheskiekienauki/d0-b8-0-0-bd-d1-82-d0-b5-d0-b3--d1-80-d0b-0---d0-b0--d0-b0-Bbie-4---20192-42* (Accessed: 29.08.2020).

3. **Shanmugavadivu R., Nagarajan Dr.N.** Network Intrusion Detection System using Fuzzy Logic. Indian Journal of Computer Science and Engineering. 2. Available: *https:///www.researchgate.net/publication/50417996_Network_Intrusion_Detection_System_using_Fuzzy_Logic* (Accessed: 01.09.2020).

4. **Seo H.S., Cho T.H.** Application of Fuzzy Logic for Distributed Intrusion Detection. Computational Intelligence and Security. Lecture Notes in Computer Science. Vol. 3802. Springer, Berlin, Heidelberg. Available: *https:///doi.org/10.1007/11596981_51* (Accessed: 02. 09. 2020).

5. **Shanmugam B., Idris N.B.** Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anamoly and Misuse Type of Attacks. *International Conference of Soft Computing and Pattern Recognition*, Malacca, Pp. 212–217. DOI: 10.1109/Soc.2009.51

6. **Kesavulu Reddy Ekambaram.** Neural Networks for Intrusion Detection and its Applications. Lecture Notes in Engineering and Computer Science. 2. 1210–1214. Available: *https:///www.researchgate.net/publication/286697952_Neural_Nworkets_for_Intrusion_Detection_and_Its_Applications* (Accessed: 04.09.2020).

7. **Vishnu Balan E., Priyan M.K., Gokulnath C., Usha Devi G.** Fuzzy Based Intrusion Detection Systems in MANET. Procedia Computer Science, Vol. 50, Pp. 109–114. Available: *https:///doi.org/10.1016/j.procs.2015.04.071.* (Accessed: 04.09.2020).

8. Network Protocols of the OSI Model. Full articles about networks and computer security. Available: *http://blogsisadmina.ru/seti/setevye-protokoly-modeli-osi.html* (Accessed: 04.09.2020).

9. The Archive Data Set. The Archive to Test Machine Learning Algorithms. Available: *http://archive.ics.uci.edu/ml/machine-learning-databases/* (Accessed: 05.09.2020).

10. **Olivas E., Martín-Guerrero J., Camps-Valls G., Serrano-López A., Calpe J., Gómez-Chova L.** A Low-complexity Fuzzy Activation Function for Artificial Neural Networks. IEEE Transactions on Neural Networks. 14. 1576–1579. 10.1109/TNN.2003.820444. Available: *https://www.researchgate.net/publication/220279588_A_low-complexity_fuzzy_activation_function_for_artificial_neural_networks* (Accessed: 06.09.2020).

11. **García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E.** Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 2009, Vol. 28, Iss. 1–2, Pp. 18–28. Available: *http://www.sciencedirect.com/science/article/pii/S0167404808000692* (Accessed: 29.08.2020).

12. **Zhang J., Zulkernine M.** Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection. *2006 IEEE International Conference on Communications*, Istanbul, 2006, Pp. 2388–2393. DOI: 10.1109/ICC.2006.255127

13. **Samrin R., Vasumathi D.** Review on Anomaly. Based Network Intrusion Detection System. *2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, Mysuru, 2017, Pp. 141–147. DOI: 10.1109/ICEECCOT.2017.8284655

14. **Schindler T.** Anomaly Detection in Log Data using Graph Databases and Machine Learning to Defend Advanced Persistent Threats. Informatik e.V. (Hrsg.): Informatik 2017. Available: *https://arxiv.org/pdf/1802.00259.pdf* (Accessed: 01.09.2020).

15. **Bahlali A.R.** Anomaly-Based Network Intrusion Detection System: A Machine Learning Approach. 2019. DOI: 10.13140/RG.2.2.29553.84325

Received 14.07.2020.

СПИСОК ЛИТЕРАТУРЫ

1. **Le C.M., Fang H.A., Nguyen A.C., Nguyen C.T.** Integrated IDS/IPS open-source model with improved machine learning // Results of Applied and Research Studies in Natural History and Technology: Com-

pendium of Scientific Papers on the Proc. of the Internat. Scientific and Practical Conf. on 27 Dec. 2019. Belgorod: LLC Advanced Scientific Research Agency (APNI), 2019. Pp. 81–87 // URL: https:///apni.ru/article/152-integrirovannaya-sipidsips-model-mezh-duotkr

2. **Chumakov V.E.** Analysis of modern methods of network infrastructure security // Internat. J. of Applied Sciences and Technology. Collection. 2019. No. 4 // URL: https:///e-integral.ru/rubriki/tehnicheskiiekienauki/d0-b8-0-0-bd-d1-82-d0-b5-d0-b3--d1-80-d0b-0---d0-b0--d0-b0-Bbie-4---20192-42 (Дата обращения: 29.08.2020).

3. **Shanmugavadivu R., Nagarajan Dr.N.** Network intrusion detection system using fuzzy logic // Indian Journal of Computer Science and Engineering. 2 // URL: https:///www.researchgate.net/publication/50417996_Network_Intrusion_Detection_System_using_Fuzzy_Logic (Дата обращения: 01.09.2020).

4. **Seo H.S., Cho T.H.** Application of fuzzy logic for distributed intrusion detection // Computational Intelligence and Security. Lecture Notes in Computer Science, Vol. 3802. Springer, Berlin, Heidelberg // URL: https:///doi.org/10.1007/11596981_51 (Дата обращения: 02.09.2020).

5. **Shanmugam B., Idris N.B.** Improved intrusion detection system using fuzzy logic for detecting anomaly and misuse type of attacks // Internat. Conf. of Soft Computing and Pattern Recognition. Malacca. Pp. 212–217. DOI: 10.1109/Soc.2009.51.

6. **Kesavulu Reddy Ekambaram.** Neural networks for intrusion detection and its applications // Lecture Notes in Engineering and Computer Science. 2. 1210–1214 // URL: https:///www.researchgate.net/publication/286697952_Neural_Nworkets_for_Intrusion_Detection_and_Its_Applications (Дата обращения: 04.09.2020).

7. **Vishnu Balan E., Priyan M.K., Gokulnath C., Usha Devi G.** Fuzzy based intrusion detection systems in MANET // Procedia Computer Science. Vol. 50. Pp. 109–114 // URL: https:///doi.org/10.1016/j.procs.2015.04.071. (Дата обращения: 04.09.2020).

8. Network protocols of the OSI model // Full articles about networks and computer security. URL: http://blogsisadmina.ru/seti/setevye-protokoly-modeli-osi.html (Дата обращения: 04.09.2020).

9. The archive Data Set // The archive to test machine learning algorithms // URL: http://archive.ics.uci.edu/ml/machine-learning-databases/ (Дата обращения: 05.09.2020).

10. **Olivas E., Martín-Guerrero J., Camps-Valls G., Serrano-López A., Calpe J., Gómez-Chova L.** A low-complexity fuzzy activation function for artificial neural networks // IEEE Transactions on Neural Networks. No. 14. Pp. 1576–1579. DOI: 10.1109/TNN.2003.820444 // URL: https://www.researchgate.net/publication/220279588_A_low-complexity_fuzzy_activation_function_for_artificial_neural_networks (Дата обращения: 06.09.2020).

11. **García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E.** Anomaly-based network intrusion detection: Techniques, systems and challenges // Computers & Security. 2009. No. 28. Iss. 1–2. Pp. 18–28 // URL: http://www.sciencedirect.com/science/article/pii/S0167404808000692 (Дата обращения: 29.08.2020).

12. **Zhang J., Zulkernine M.** Anomaly based network intrusion detection with unsupervised outlier detection // 2006 IEEE Internat. Conf. on Communications. Istanbul, 2006. Pp. 2388–2393. DOI: 10.1109/ICC.2006.255127

13. **Samrin R., Vasumathi D.** Review on anomaly based network intrusion detection system // 2017 Internat. Conf. on Electrical, Electronics, Communication, Computer, and Optimization Techniques. Mysuru, 2017. Pp. 141–147. DOI: 10.1109/ICEECCOT.2017.8284655

14. **Schindler T.** Anomaly Detection in Log Data using Graph Databases and Machine Learning to Defend Advanced Persistent Threats. Informatik e.V. (Hrsg.): Informatik 2017 // URL: https://arxiv.org/pdf/1802.00259.pdf (Дата обращения: 01.09.2020).

15. **Bahlali Ahmed Ramzi.** Anomaly-based network intrusion detection system: A machine learning approach. 2019. DOI: 10.13140/RG.2.2.29553.84325. (Дата обращения: 03.09.2020)

Статья поступила в редакцию 14.07.2020.

THE AUTHOR / СВЕДЕНИЯ ОБ АВТОРЕ

Chumakov Vladislav E.
Чумаков Владислав Евгеньевич
E-mail: chumakov.dssa@mail.ru