Primary Data Processing for Constructing Network Package Classifiers in Deep Packet Inspection Analysis and in the Intrusion Detection Systems

R. N. Ermakov, V. V. Alekseev

Institute “Research Institute“Масштаб”, St. Petersburg, Russia

Abstract. We consider the procedure for preprocessing the source packet information in a new method for classifying network packets of the application layer in order to determine their belonging to one of the known network protocols. Packets are classified based on the use of machine learning methods and fuzzy logic algorithms in Network Traffic Analysis (NTA) systems, in “deep” packet analysis (Deep Packet Inspection - DPI), in intrusion detection systems (IDS) and in other systems. To define the protocol, the principle of high-speed one-packet classification is used, which consists in analyzing the information transmitted in each particular packet. Elements of behavioral analysis are used, namely, the transition states of information exchange protocols are classified, which allows to achieve a higher level of accuracy of classification and a higher degree of generalization in new test samples.

Keywords: classification of network packets, neural networks, DPI methods, machine learning, definition of network protocols.

DOI 10.14357/20718632190404

Introduction

In recent years, there has been no increase in the mutual interest of the domestic telecommunications market and large foreign vendors (Procera, Allot, Sandvine, Cisco, etc.). According to an expert from VAS EXPERTS LLC [1], there are three foreign leaders on the Russian market (Procera, Allot, Sandvine), but not a single company has an official representative office. This publication emphasizes that integrators of the above-mentioned foreign leaders most often act as technical support for the first line for the customer, and in the event of a serious problem, contact the vendor directly, who solves the problem and sends it back to the integrator, and the integrator to the customer. Such a chain, as a rule, is not the most convenient and fast for solving problems that arise. At the same time, the target audience of foreign vendors lives in other requirements and conditions for doing business, as a result, only Russian developers will quickly adjust the system to local legislation. Thus, domestic developments look more attractive both from the cost of solutions and the possibility of implementation and support directly by the developers of the developer company. The initial stage of creating such a decision will be discussed in this article.

Many information security systems have been developed and operated. These systems include:

- access rights management system (IDM – Identity Management);
- systems for monitoring the actions of administrators (PAM – Privelege Accounts Management);
- advanced firewalls (NGFW – Next Generation Firewalls);

- security analysis tools (SIEM – Security Information and Event Management);
- antivirus solutions (AV – Antivirus, Antibot, Malware Protection);
- systems for detecting intrusions and anomalies (IDS - Intrusion Detection System, APIDS Application protocol-based IDS);
- attack prevention systems (IPS – Intrusion Prevention System);
- systems of audit and monitoring of security tools (NMS – Security Information and Event Management);
- denial of service attacks protection systems (DDoS PS – DDoS Protection Systems);
- network traffic policy management systems (PCEF – Policy and Charging Enforcement Function, PCRF – Policy and Charging Rules Function, NAC – Network Access Control);
- other systems.

Traffic analysis for many years remains a relevant area of research. Two main reasons contribute to this: (1) the growth of traffic, including malicious traffic, (2) the emergence of new technologies. NTA traffic analysis systems are a necessary tool for many of the classes of other information security systems, such as IDS, IPS, NMS, DDoS PS, etc.

Another factor limiting the use of multifunctional heavyweight foreign DPI-systems is the import substitution program that has gained momentum, which involves the transition of Russian companies to the use of modern domestic processors such as Elbrus [2]. In this regard, firstly, there is no complete certainty that such resource-consuming software will be installed without undue complexity, and secondly, there is no certainty that all the declared functionality will be properly executed. In accordance with the foregoing, we believe that the proprietary development of various functional elements of a DPI system, including in-depth packet analysis (DPI), and bringing these elements to the industrial level is, without a doubt, an actual direction in the development of information security systems, such as IDS, IPS, DDoS PS and others, in terms of the needs of domestic consumers.

Qualitative classification of network packets of application-level protocols, both in terms of classification characteristics (accuracy, time, reliability, etc.), and in terms of reducing computing power requirements, has an important impact on the functioning of NTA systems [3, 4], DPI traffic analysis [5], IDS / IPS [6], DDoS PS [7] and others, both for the entire technological process and for the quality of analysis.

This article presents a methodology for preprocessing primary data, including using machine learning procedures and fuzzy logic algorithms. A description of the formed factor space is given. A brief description of the structure of the neural network model for classifying network packets as belonging to one of the known network protocols is given.

1. Ways to Analyze Network Traffic

Currently, there is a significant proportion of traffic with encrypted content (about 65-70 percent) and there is a growth trend (Fig. 1).

For the analysis of open and encrypted traffic in the Russian and global Internet space, as a rule, three basic DPI methods are used: signature, behavioral, and hybrid.

Considering the significant share of encrypted traffic in the process of recognition of network applications of the application layer, the most relevant is behavioral analysis. Behavioral analysis assumes control of functional characteristics of network packets, for example, packet size and payload, used ports, etc., as well as tracking changes in protocol states of packets forwarded during a session, where a certain model of client and server behavior is assumed for certain types of connections.

At the same time, a significant part of the network applications of the application layer operates using such secure protocols as SSL / TLS (for example, Skype, Viber, etc.).

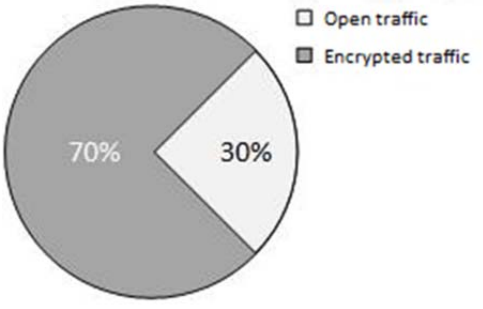

Fig. 1. The share of traffic with encrypted content

The principle of SSL operation consists of two phases [8]:

- Handshake phase;
- Phase of data transfer.

The approximate fragment of the interaction via the SSL protocol is presented in Fig. 2.

During the handshake phase, the client and server use public key encryption to determine the parameters of the private key used by the client and server to encrypt during the data transfer phase.

The client initiates a handshake by sending a “hello” message to the server. This message contains a list of symmetric encryption algorithms supported by the client. The server responds with a similar “hello” message, while selecting the most appropriate encryption algorithm from the resulting list. Next, the server sends a certificate that contains its public key. The handshake phase ends with sending the “finished” messages as soon as both parties are ready to begin using the secret key. Fig. 2 shows the detailed interaction mechanism at the handshake stage. Next, the data transfer phase begins.

Thus, firstly, knowledge of the behavior of a protocol in the process of information exchange between the client and the server (its life cycle), and secondly, the ability to recognize the states in which a particular protocol may be located increases the accuracy and reliability of network classification application layer applications.

As a rule, to analyze network traffic, researchers in their works determine an application-level protocol using machine-learning algorithms “with a teacher” [9 - 11]. In [9], the classification problem was solved by the method of support vectors and with the help of the random forest algorithm. The results of studies on test samples in this work showed that both approaches lead to high classification accuracy, 98% and higher. However, nothing is said about the average time for classifying packets by algorithms on specific hardware platforms and operating systems. The question remains: is it possible to use such "heavy" classification algorithms in real traffic analysis systems, taking into account the requirements for computing performance? To classify network packets in [12], Mamdani’s fuzzy inference model and machine learning methods, in particular neural networks, namely, logistic regression, were used.

Currently, in order to ensure information security, extensive research and search for new ways to identify DDoS attacks are underway. As a rule, these methods rely on the identification of network activities and anomalies [13]. Similar problems can also be effectively solved using the classifier

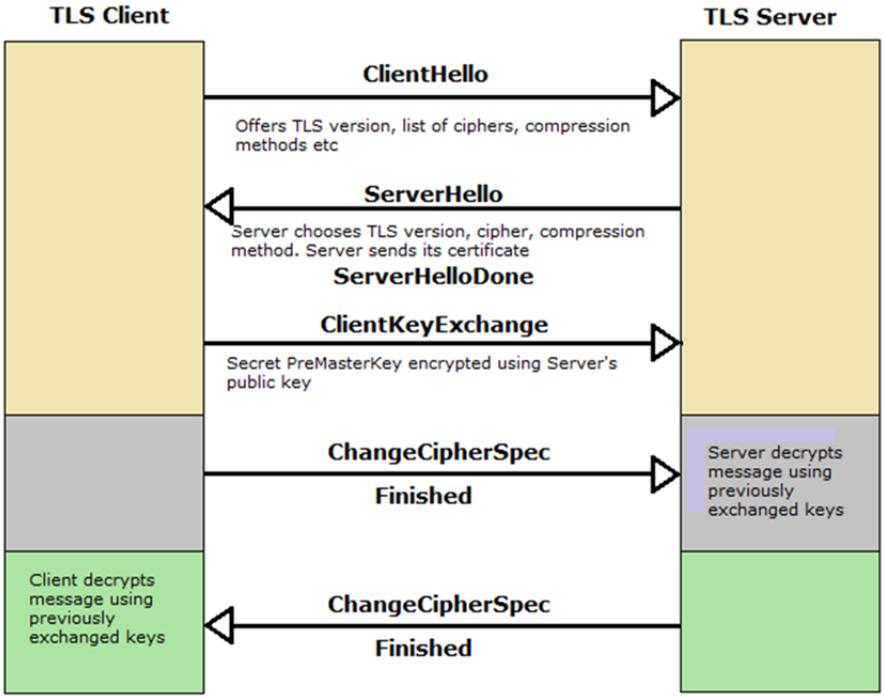

Fig. 2. Example fragment of the SSL protocol

of network packets (CNP) of the application level [12]. Initially, using the CNP, the information exchange protocol and the types of devices involved in the exchange can be classified. Further, applications on information exchange devices and then application-level network applications can be identified. This method of identifying potential network threats is not high speed. However, it can be very effective within the framework of a test environment for conducting comprehensive comprehensive research in the identification of DDoS attacks.

At the same time, the application layer network packet classifier (CNP) can be very useful in recognizing the internal state in which a particular protocol may be in the process of information exchange at the stage of handshake, which is an important element of behavioral analysis.

In [12], the development of a network packet classifier consisted of the following steps: (1) monitoring, collecting and pre-processing packet statistics of the most well-known network traffic protocols, (2) building a network packet classifier, and (3) testing. The procedure for preprocessing the initial packet information consisted of two main stages. At the first stage, monitoring and collection of packet statistical information of the most well-known and frequently encountered network traffic protocols were carried out. At the second stage, preprocessing of the initial (primary) packet statistical information was carried out.

2. Statement of the Problem of Traffic Classification

The formulation of the traffic classification problem can be formulated as follows. There are many studied objects of application-level IP packets:

$$P = \{P_1, P_2, \cdots, P_W\} \quad (1)$$

where P_w is a classified packet from a sequence of packets (traffic) of dimension W. Each object (IP packet) is characterized by a set of variables (attributes):

$$P_w = \left\{X_1^w, X_2^w, \cdots, X_{10}^w,\ H_j^w, H_{j+n}^w, H_{j+n+\cdots+k}^w\right\}, \quad (2)$$

$$Z = \{Z_1, Z_2, Z_3\}, \quad (3)$$

where, X_n^w– is the observed n-attribute of the w-packet, the range of admissible values of which is contained in the RFC (Request for comments), H_j^w – is the *Payload_hex* byte sequence of size – J, Z – is the dependent set that needs to be determined. The set Z includes: type of protocol – Z_1, probability of belonging to the identified type of protocol – Z_2, internal state of the protocol in the process of information exchange – Z_3. Moreover, each variable $X_n$takes a value from some set:

$$X_n = \{Xn_1, Xn_2, \cdots, Xn_M\}, \quad (4)$$

where, Xn_M are options for attribute values.

Thus, the classification problem is reduced to determining the set Z based on the values of the attributes of the packet sequence.

In [12], the following set of attributes was distinguished:

X_1 - *EtherType* (type of standard Ethernet protocol);

X_2 - *Source IP Address* (IP address of the sender);

X_3 - *Destination IP Address*;

X_4 - *Multicast* (takes the value 1 if multicast, otherwise 0);

X_5 - *IP Protocol* (transport layer type);

X_6 - *Packet Length* (length of the network packet in bytes);

X_7 - *Source Port* (port [TCP / UDP] of the sender);

X_8 - *Destination Port* (recipient [TCP/UDP] port);

X_9 - *Hex_length* (the number of bytes in the string content [part payload] of the top-level protocol);

X_{10} – *Payload_type* (attribute for providing training models for the classification of network packets according to the scheme with the teacher);

X_{11} – *Payload_hex* (attribute for providing training models for the classification of network packets according to the scheme with the teacher: H).

At the same time, an additional parameter was included in [12] - marking of the payload type class in order to be able to train models for classifying network packets according to a scheme with a teacher.

3. Monitoring and Collecting Packet Statistics of the Most Famous and Common Network Traffic Protocols

In [12], the monitoring and collection of packet statistical information of the most common network traffic protocols (TLS v1, TLS v1.2, SSH v2, HTTP, FTP, etc.) was carried out using the open Wireshark software and included the solution of the following tasks:

a) selection of the most suitable input variables for constructing a classification model for network packets;

b) the formation of a set of primary representative samples - DUMP in PCAP-format with packet information on the above protocols (traffic volume ~ 1 GB);

c) automatic generation of secondary samples for analysis.

4. Preprocessing Source Packet Information

The preprocessing of primary packet information consists of three sequentially executed blocks, which are presented in Fig. 3.

In the first preprocessing block the following functionality is involved:

- check payload for encrypted content information (required the implementation of a separate special technology software in Python);
- payload processing for better visual perception and the possibility of heuristic (behavioral) analysis;
- separation of received classified network packets into homogeneous groups (A, B, C, D) based on the values of some input parameters (type of Ethernet protocol standard, Multicast and type of transport layer), as well as the formation of test and training sets.

The classification of network packets classified as belonging to protocols (DHCP v6, DNS, FTP, HTTP и др.) into groups ($GROUP_A$, $GROUP_B$, $GROUP_C$, $GROUP_D$) is based on the following logical rules:

$GROUP_A = if$ (ethertype == IPv4) &&($Multicast$ == 0) && (IP_PROTO == TCP);

$GROUP_B = if$ (ethertype == IPv4) &&($Multicast$ == 0) && (IP_PROTO == UDP);

$GROUP_C = if$ (ethertype == IPv4) &&($Multicast$ == 1) && (IP_PROTO == UDP);

$GROUP_D = if$ (ethertype == IPv6) &&($Multicast$ == 1) && (IP_PROTO == UDP);

As a result of calculations by expression (4), classified network packets are distributed into groups to identify the corresponding communication protocols:

$GROUP_A = \{\text{TLSv1, TLSv1.2, TCP, SSHv2, HTTP}\}$;

$GROUP_B = \{\text{UDP, STUN, QUIC, NBNS, DNS, BROWSER}\}$;

$GROUP_C = \{\text{SSDP, MDNS, LLMNR}\}$;

$GROUP_D = \{\text{SSDP, MDNS, LLMNR, DHCPv6}\}$;

The protocols that fall into one group will be considered largely similar, and the total sample in the group will be considered homogeneous. Within each group, data is divided into training and test data sets.

At the present stage of the development of mathematical modeling, it is considered that representative initial data sets in many respects provide the ultimate success of the entire modeling - obtaining adequate models. As a rule, statistical checks of the initial data are carried out, highly noisy or redundant initial data are identified and excluded from the training samples. In the second block of the preprocessing algorithm, good data sets are allocated for the further construction of classification models for network packets of the application level.

In the third block of the algorithm, the following data preprocessing procedures are used, as a rule, used in machine learning methods:

1) *processing of categorical data*,

2) *scaling of signs, which includes bringing different signs to the same scale (in practice, there are two general approaches to bringing different signs to the same scale*:

- normalization;
- standardization**,**

3) *selection of substantive features*.

After completion of the normalization procedure for input variables, some of which then go through the fuzzification procedure and are transformed into fuzzy indicators characterized by lin-

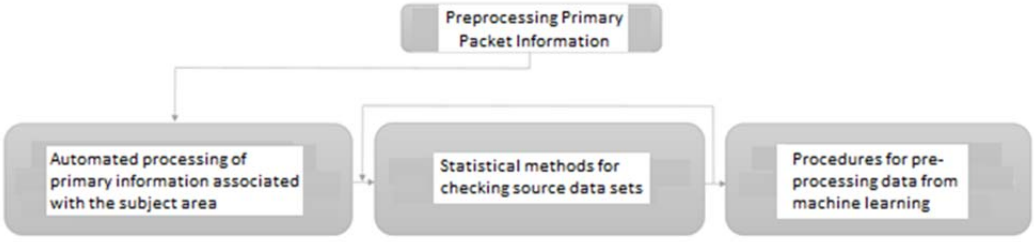

Fig. 3. Intelligent automated preprocessing of primary packet data

guistic variables (LV). A fuzzy indicator is a number in the range [0, 1] that characterizes the rating of the indicator used as an attribute.

The fuzzy indicator is based on an expert's assessment, which is modeled by the membership function, while the carrier is an allowable set of values of the analyzed indicator.

In the general case, various models of the membership function can also be used, for example, such as triangular, or trapezoidal or generalized bell-shaped (Fig. 4).

To identify the state of the protocol (block MLR1 in Fig. 5), there is not enough information from the packet header; additional information must be extracted from the Payload_hex field of the packet (attribute H). In this case, the identifying sign of the protocol state is information extracted from the hexadecimal payload data of the network packet from the Payload_hex field. The internal state is determined on the basis of logical decision rules based on information from the RFC (TLS 1.0 RFC 2246, TLS 1.1 RFC 4346, TLS 1.2 RFC 5246, TLS 1.3 RFC 8446). The main states of a TLS exchange session: initial connection, exchange of cryptographic keys, determination of connection parameters, authentication, warning, data exchange, session termination. For example, the rules for determining the state of a connection can be:

SessionInternalSost = -1;

IF (H[2] == 0x03) AND (H[3] == 0x00) then SessionInternalSost = 0;

IF (H[2] == 0x03) AND (H[3] == 0x01) then SessionInternalSost = 1;

IF (H[2] == 0x03) AND (H[3] == 0x02) then SessionInternalSost = 2;

IF (H[2] == 0x03) AND (H[3] == 0x03) then SessionInternalSost = 3.

Thus, at the output of MLR1, if the status of the *SOST* protocol is established, it will have a positive value.

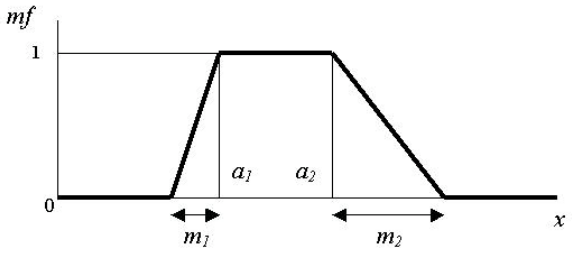

Fig. 4. Trapezoidal membership function of a fuzzy set

Currently, the idea of sharing a neural network approach to the classification of network packets in DPI, NTA analysis is being discussed by researchers and specialists [14]. In [12], the procedure for determining network protocols was presented. After performing the initial transformations in the initial procedures for preprocessing the source data, each object (IP packet) can be expressed by a new set of variables (attributes):

$$P_w = \{Y_1^w, Y_2^w, \cdots, Y_{10}^w,\ H_j^w, H_{j+n}^w, H_{j+n+\cdots+k}^w\}, \quad (7)$$

where, Y_n^w– is the observed n-attribute of the w-packet, H_j^w – are elements of the *Payload_hex* byte sequence of size – J (или X_{11}^w), involved in the recognition of network protocols.

Fig. 5 shows a block diagram of a two-step procedure for determining network protocols, where input indicators characterize:

Y_1 is the port number of the [TCP / UDP] sender;

Y_2 – the port number [TCP/UDP] of the recipient;

Y_3 – the value of the first byte in the string content (part of the payload) of the top-level protocol;

Y_4 – degree of belonging to a small value of the packet length (fuzzy set);

Y_5 is the degree of belonging to a large packet length value (fuzzy set);

Y_6 – the degree of belonging to the average value of the packet length (fuzzy set);

Y_7 is the degree to which the sender's [TCP / UDP] port number is a small value (fuzzy set);

Y_8 – the degree of belonging to the large value of the port number [TCP/UDP] of the sender (fuzzy set);

Y_9 – the degree of belonging to the small value of the port number [TCP / UDP] of the recipient (fuzzy set);

Y_{10} – the degree of belonging to the large value of the port number [TCP / UDP] of the recipient (fuzzy set);

X_{11} – membership of the Content Type integer range defined in RFC 2246 and RFC 5246 for TLSv1 and TLSv1.2, respectively.

Output indicators have the form:

Z_1 - type of protocol;

Z_2 – probability of belonging to the identified type of protocol;

Z_3 is the internal state code of the most probable class (the resulting indicator).

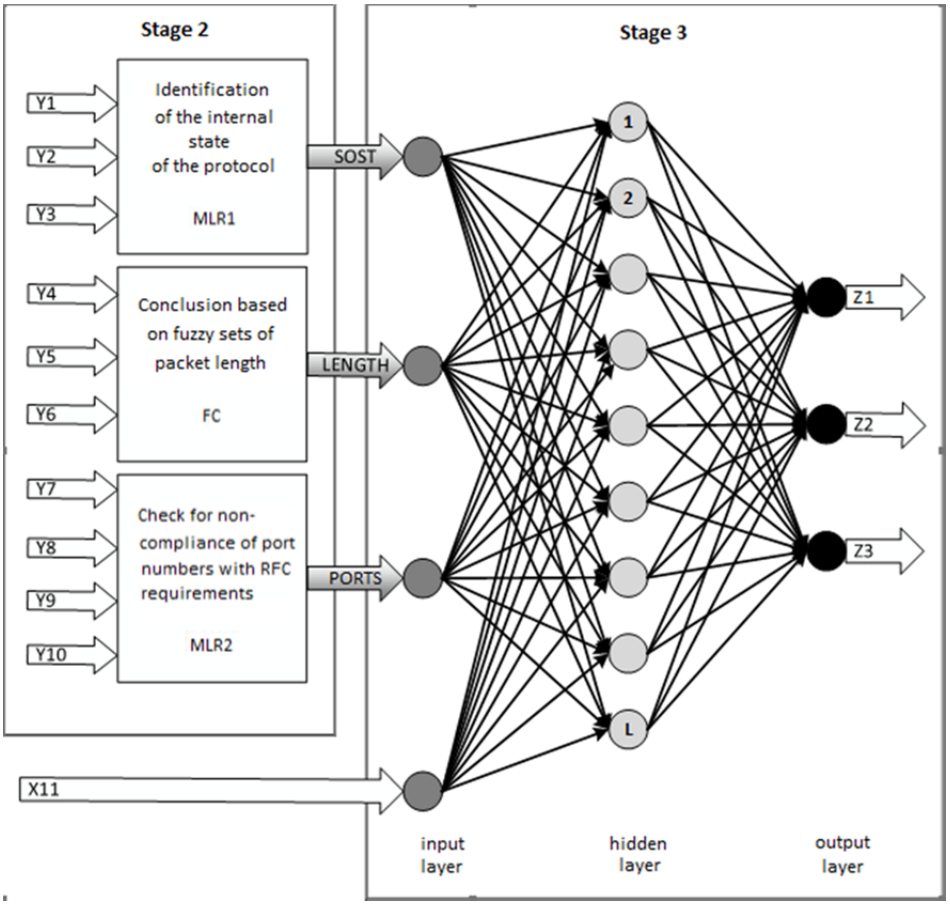

Fig. 5. Block diagram of a two-step procedure for determining network protocols

In the future, we plan to expand the number of output effective indicators by including Z_4 – the type of network application of the application level and Z_5 – the probability of belonging to the found type of application.

Thus, the signs Y_4, Y_5, Y_6, Y_7, Y_8, Y_9, and Y_{10} received at the input of the network packet classifier are fuzzy linguistic variables that underwent the fuzzification procedure at the stage of preprocessing the initial data, which consists in the fact that a sequentially formed array of IP packets of dimension W enters the input of the processing unit. The array contains the values of all input attributes X_n^w. The purpose of the stage is to obtain membership function values for all conditions from the rule base:

$$Y_n^w = \widetilde{X_n^w} = \mu\,(X_n^w) = \begin{cases} \mu(X_4^w) \\ \mu(X_5^w) \\ \cdots \\ \mu(X_{10}^w) \end{cases}, \qquad (8)$$

where, it turns out the matrix of sets of values $Y_n^w (or\ \widetilde{X_n^w})$, where $w = 1, \ldots, W$ – are classified packets; n =4,…,*10*.

Given the significant amount of data analyzed, to optimize the calculations, the decomposition (convolution) of the input factor space was used in [12]. For this purpose, machine learning specialists often use linear discriminant analysis (LDA) [15] and / or deep convolutional neural networks [16]. In [12], models based on logical rules and fuzzy logic algorithms are used for this purpose (the Mamdani fuzzy inference algorithm [17–20] was used).

When implementing the Deep Analysis of Packets in [12], a combined traffic classification method based on the application of theories of neural networks and fuzzy sets is considered. In this case, a significant gain in the classification of traffic was obtained in a two-stage solution of the problem, including:

- the first stage consists of the procedure for reducing the dimension of the input feature space (convolution);

- the second stage completes the classification of traffic using logistic regression "with the teacher" or using the fuzzy inference algorithm of Mamdani. At the first stage of calculations, fuzzy controllers (FC) and models based on logical rules (MLR) are used, for example, in the unit for checking the mismatch of used port numbers with RFC requirements, based on simple logical rules, the port numbers for the studied protocols TLS v1 and TLS v1.2 are checked, as a rule, port 443 and the port number from the integer interval, the lower limit of which exceeds 50,000, are used for the transmitting and receiving parties. And in the unit for identifying the internal state of the network protocol for determining the internal states, a hex sequence is used (from *Payload_hex*). By means of logical rules, the input hex-values are identified with the reference ones. In this case, the logical rule for determining some j-th internal state S_j of some *i*-th protocol can be of the form:

IF ($hex_i[0]$ == 0xA3 AND $hex_i[1]$ == 0x3D AND $hex_i[4]$ = 0xC2) THEN ($Z_2 = S_j$). (9)

The second stage uses logistic regression methods or fuzzy logic algorithms, namely, the Mamdani fuzzy inference algorithm. However, it should also be noted that the final internal state of the protocols under study is highly useful - Z_3. This resulting feature is very useful for further optimization of the classifier of network packets of the application level, as evidenced by the results of tests [12].

Conclusion

The methodology for preprocessing primary packet data presented in this work in the process of determining known application level protocols illustrates the development of domestic traffic analysis systems under the conditions of import substitution programs. The pre-processing procedure involves the use of machine learning algorithms and intelligent data processing.

There is the prospect of the emergence of a neural network CLASSIFIER OF NETWORK PACKAGES of an industrial level with indicators not inferior to the known DPI solutions, but working at a completely different level.

The paradigm of the neural networked CNP and the Elbrus platform architecture are based on parallel computing, which will provide the highest performance on a trusted hardware platform.

A new methodology for collecting and processing primary statistical information using machine learning procedures at the initial stage of designing an industrial neural network classifier of network packets in the aspect of the needs of domestic consumers is presented.

References

1. Khazov V. 2016. Introduction to DPI: Analytics, market conditions and trends. - URL: https://vasexperts.ru/blog/privet-mir/
2. Bychkov I.N., Glukhov V.I., Trushkin K.A. Trusted Elbrus hardware and software platform. Domestic solution for ACS TP KVO // ISUP - No. 1 (49).
3. Rehak M., Pechoucek M., Grill M., Stiborek J., Bartos K., and Celeda P Vol. 24 (3), 2009. Adaptive multiagent system for network traffic monitoring. IEEE Intelligent Systems. Pp 16 – 25.
4. Anu Gowsalya R.S., Miruna Joe Amali S. - "SVM Based Network Traffic Classification Using Correlation Information", International Journal of Research in Electronics and Communication Technology (IJRECT 2014), ISSN : 2348 - 9065 (Online) ISSN : 2349 – 3143.
5. Elagin V.S., Zarubin A.A., Onufrienco A.V. Efficiency of DPI-system for traffic identification and maintenance off OTT-services quality // Scientific and Technical Journal. 2018. Vol. 10. № 3. p.40-53. doi: 10.24411/2409-5419-2018-10074.
6. Singh J., Nene M.J. A Survey on Machine Learning Techniques for Intrusion Detection Systems. International Journal of Advanced Research in Computer and Communication Engineering. Vol.2, Issue 11, November 2013. Department of Computer Engineering, DIAT, Pune, India. Pp 4349 – 4355.
7. Abraham S. and Nair S. Cyber Security Analytics: A stochastic model for Security Quantification using Absorbing Markov Chains. Journal of Communications. December 2014. Vol. 9(12):pp. 899-907.
8. ITMO University. – URL: https://neerc.ifmo.ru/wiki/index.php?title=SSL/TLS.
9. Ryzhkov D.O. Determination Of The Application Level Protocol For Analysis Of Network Traffic Using Machine Learning Algorithms // Materials of the IX International Student Scientific Conference "Student Scientific Forum". – URL: https://scienceforum.ru/2017/article/2017032799.
10. Multi-level Machine Learning Traffic Classification System. Szabo G., Szule J., Turanyi Z., Pongracz G. // ICN 2012: The Eleventh International Conference on Networks. Pp 69 – 77.
11. Traffic Classification Using Probabilistic Neural Networks. Sun R., Yang B., Peng L., Chen Z., Zhang L., and Jing S. // Sixth International Conference on Natural Computation (ICNC 2010). Pp. 1914-1919.

12. Ermakov R.N. Detection Of Network Protocols With Application Of Machine Learning Methods And Fuzzy Logic Algorithms In Traffic Analysis Systems // Automation of management processes. 2019. Vol 3 (57). Pp. 53-64.
13. Ageev S.A., Saenko I.B., Kotenko I.V. Method and algorithms for detecting anomalies in the traffic of multiservice communication networks based on fuzzy inference // Information-control systems. 2018. №3. С. 61-68. Doi: 10.15217/issn1684-8853.2018.3.61.
14. Lim Y., Kim H., Jeong J., Kim C., Kwon T., Choi Y. Internet Traffic Classification Demystified: On the Sources of the Discriminative Power. 2010. – URL: http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/09-Lim.pdf
15. Izenman A.J. Linear Discriminant Analysis. In: Modern Multivariate Statistical Techniques. Springer Texts in Statistics. Springer, New York, NY. 2013. 733 p.
16. Gulli A., Pal S. Deep Learning with Keras. Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK. 2017. 318 p.
17. Mamdani E.H., Assilian S. 1975. An experiment in linguistic synthesis thesis with a fuzzy logic controller.- International Journal of Man-Machine Studies, vol. 7, no. 1, pp. 1-13.
18. Mamdani E.H. 1976. Advances in the linguistic synthesis of fuzzy controllers. - International Journal of Man-Machine Studies, vol. 8, pp. 669-678.
19. Mamdani E.H., "Applications of fuzzy logic to approximate reasoning using linguistic synthesis," IEEE Transactions on Computers, Vol. 26, No. 12, pp. 1182-1191, 1977.
20. A. Piegat. Fuzzy Modeling and Control / Springer, 2014. 744 p.

Ermakov R. N. PhD. Institute “Research Institute“Масштаб”, 5 Kantemirovskaya str. St. Petersburg, Russia, PhD, Graduated from St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich in 2007. 14 published articles. Topics of interest: Information security, computer vision, mathematical modeling, intelligent decision-making systems and control systems. E-mail: romul151925@mail.ru

Alekseev V. V. Institute “Research Institute“Масштаб”, 5 Kantemirovskaya str. St. Petersburg, Russia, Graduated from St. Petersburg State University ITMO. Topics of interest: Information security e-mail: v.alekseev@mashtab.org