ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

Study of Traffic Filtering Methods for Protecting Information from Network Attacks

GulomovSherzodRajabayevich, KadirovMirhusanMirpulatovich, KhoshimovaCharosSaidaminovna,YuldashevaNafisaSalimovna

Assistant professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Assistant, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: The article discusses methods for filtering network traffic. Currently, many methods of filtering traffic have been developed for use on various computer networks. The article presents the advantages and disadvantages of traffic filtering methods.

KEYWORDS: networks attacks, traffic filtering, protecting information, filtering methods, firewall, request, packages, neural network.

I. INTRODUCTION

Currently, systems for detecting network attacks and detecting signs of computer attacks on information systems have long been used as one of the necessary defense lines of information systems. The developers of information security systems and consultants in this field actively use such concepts as perimeter protection, stationary protection and dynamic protection. Own terms began to appear, for example, “projective” means of protection. The signs of attacks are investigated, methods and means of detecting unauthorized intrusion attempts through protection systems, both internetwork and local, at the logical and even at the physical levels, are being developed and operated.

At the moment, all systems can be divided into network and local. Network systems are usually installed on dedicated computers and analyze the traffic circulating in the local area network. Intrusion detection systems are located on individual computers that need protection, and allow you to analyze various events. There are also methods for detecting abnormal behavior and detecting malicious user behavior [1].

Systems for detecting anomalous behavior are based on the fact that the attack detection system knows some of the signs that characterize the correct or acceptable behavior of the object of observation. Under the normal or correct behavior refers to actions performed by the object and not contrary to security policy. Malicious behavior detection systems are based on the fact that the attack detection system is aware of some of the signs that characterize an attacker's behavior. The most common implementation of the technology of detecting malicious behavior are expert systems.

It should be noted that there are two extremes when using this technology:

• Detection of anomalous behavior that is not an attack, and attributing it to the class of attacks (error of the second kind);

• skipping an attack that does not fall under the definition of anomalous behavior (error of the first kind). This case is much more dangerous than the false assignment of anomalous behavior to the class of attacks.

Statistical analysis of computer attacks. The use of statistical analysis methods is the most common type of implementation of the technology for detecting anomalous behavior. Statistical sensors collect various information about the typical behavior of an object and form it in the form of a profile.

Analysis of systems using signature methods. Signature methods allow you to describe an attack with a set of rules or with the help of a formal model, which can be used as a character string, a semantic expression in a special language, etc.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

The further direction of improvement is related to the introduction of the attack detection system, methods of the theory of synthesis and analysis of information systems, and a specific device of the pattern recognition theory into the theory and practice, since these sections of the theory provide specific research methods for the area of attack detection systems.

Due to the presence of a significant number of factors of different nature, the functioning of the attack detection system has a probabilistic nature. Therefore, it is relevant to justify the type of probability laws of specific parameters of functioning. Special mention should be made of the task of justifying the loss function of an information system, specified in accordance with its objective function and in the area of system operation parameters. At the same time, the objective function should be determined not only at the expert level, but also in accordance with the set of parameters of the functioning of the entire information system and the tasks assigned to it. Then the quality indicator of the attack detection system will be determined as one of the parameters affecting the objective function, and its allowable values will be determined by the allowable values of the loss function.

II. TRAFFIC FILTERING METHODS

Currently, many methods of filtering traffic have been developed for use on various computer networks [2].

Simulation method for filtering network traffic. It is proposed to assess the effectiveness of the use of a firewall, depending on the configuration of its parameters, using a simulation model. Based on the structure of the organization's computer network connection, the structural-functional scheme of the simulation model, shown in Figure 1, was developed.

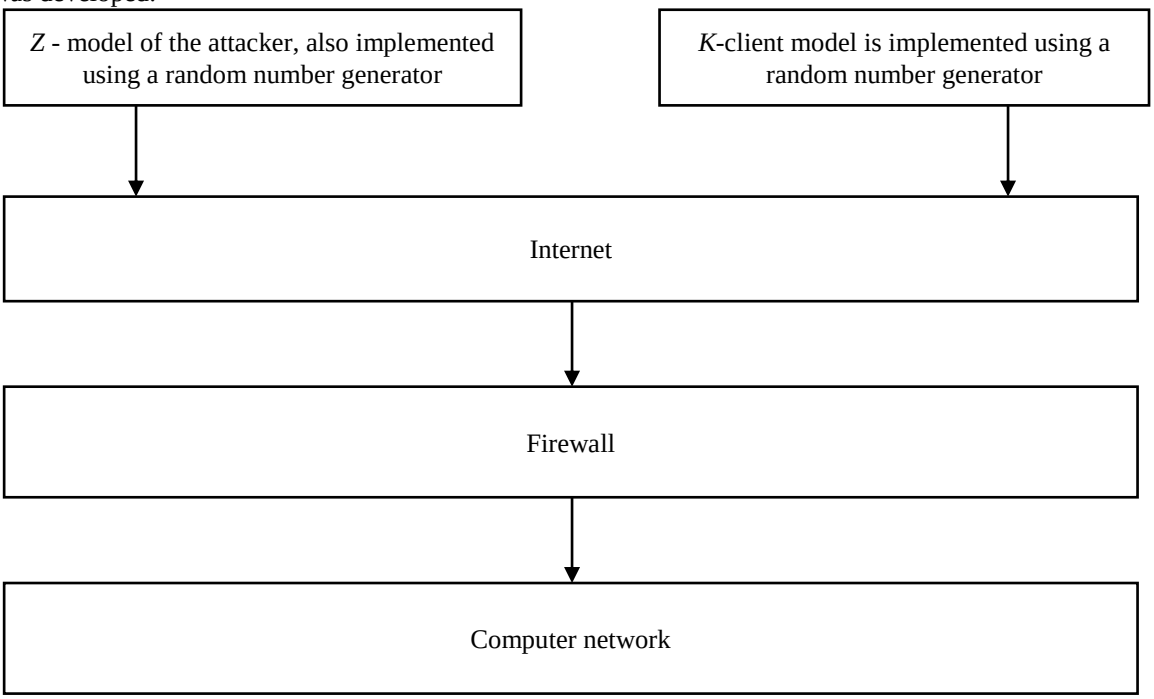

Figure 1 - Structural and functional diagram of the simulation model

The *K*-model of the client model is implemented using a random number generator that generates two random numbers per model time unit:

- ID of the requested Internet service organization;
- querylength.

The value of the identifier of the requested service by the client in the model is determined by the following expression.

$$K_s = \begin{cases} 21, t \ mod \ 2 = 0 \\ 80, t \ mod \ 2 > 0 \end{cases}, \quad (1)$$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

where t is model time, values 21 and 80 correspond to the most popular services provided by organizations on the Internet, these are FTP and HTTP services. The query length is lognormally distributed with parameters$K1_a, K1_b$. These random numbers mimic a fragment of a network packet built over IP. These numbers are generated at intervals distributed lognormally with parameters K_a, K_b.

Module Z-model of the attacker, also implemented using a random number generator. It generates two random numbers with an interval distributed exponentially with the parameter Z_λ. These generated numbers also determine the ID of the requested service and the length of the request. The identifier of the requested Internet service is a random number distributed according to a uniform law with parameters $Z_a = 0, Z_b = 2^{32}$. The request length is a random number distributed according to a uniform law with parameters $Z1_a = 1, Z1_b = 4096$. The model of the work of ME is implemented using two components: the first component verifies the correctness of the identifiers of the requested services of the company from incoming packets. Which incoming packet will be classified as good (generated by the client), and which bad packet (generated by an attacker) based on the identifier of the requested service is determined by the expression.

$$P_g = \begin{cases} 1, S = 21 \wedge S = 80 \\ 0, S \gtrless 21 \vee S \gtrless 80 \end{cases}, \quad (2)$$

The second component, checks the correct length of the request from the incoming packet. The correctness of the request length is determined by

$$P_g = \begin{cases} 1, L > Lw_{min} \wedge L < Lw_{max}, S = 80 \\ 0, L \geq Lf_{min} \wedge L < Lf_{max}, S = 21 \end{cases}, \quad (3)$$

where Lw_{min} _min is the minimum request length when accessing the company's HTTP service, Lw_{max} −is the maximum, Lf_{min} −the minimum request length when accessing the company's FTP service, Lf_{max}, −is the maximum [2].

The input and output data of the simulation model are defined.

K_i −number of generated packets by client model.

Z_i − the number of generated packets by the attacker model.

K_0 −is the number of packets generated by the client model that passed Firewall.

Z_0 −is the number of packets generated by the attacker's model that did not pass through Firewall.

The performance of the firewall is determined by the expression

$$B_k = \frac{\frac{K_0}{K_i} + 1 - \frac{Z_0}{Z_i}}{2} \times 100\% \quad (4)$$

The high efficiency factor of the $B_k -$ firewall parameters is explained by the fact that most of the requests in the model were cut off at the port filtering level, since in the model the attacker showed interest in all sorts of ports. From the obtained formula, it can be seen that filtering by the length of the request, in case of incorrect setting of parameters, can lead to the fact that part of the client's requests will not reach its goal. Therefore, to increase the efficiency of filtering requests by port, it is recommended to set filtering by request length. But the filtering parameters by the length of the request should cover the minimum possible and maximum possible length of requests from the client [3].

The method of filtering incoming traffic based on a two-layer recurrent neural network. To build a training and test base for filtering traffic based on a two-layer recurrent neural network, the following ratio was determined - 60/25/15, where 65% of the records were used to train the system, 25% were tested, and 15% were used to select the most optimal state system. This relationship was obtained empirically and does not claim to be universal. Figure 2 shows the evolution of a threat when the number of requests has begun to exceed the physical capabilities of the node (server).

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

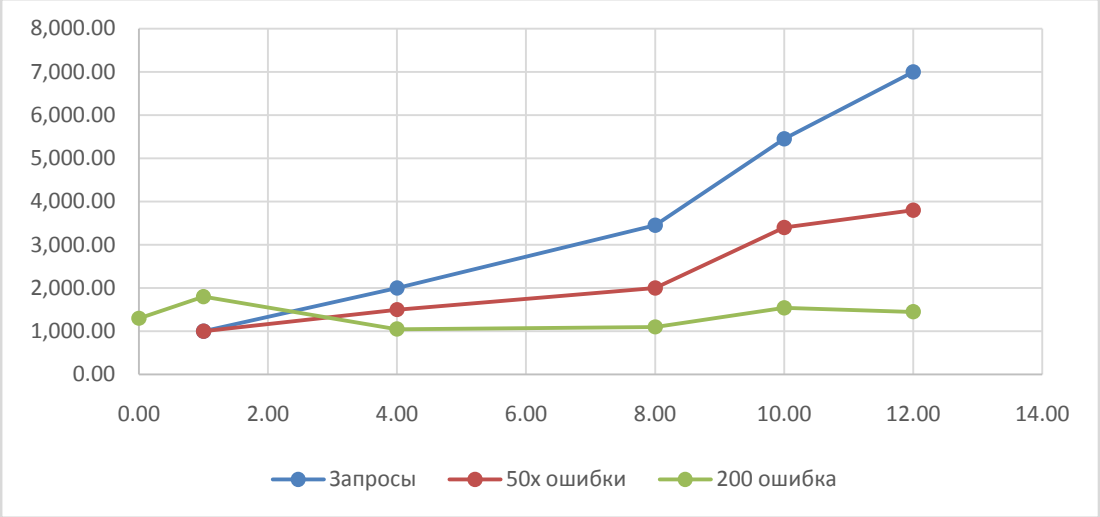

Figure 2 - Graphs of growth in the number of requests for 12 hours of server operation (DDos attack)

After the implementation of the filtering method based on a two-layer recurrent neural network, the speed of creating restrictions on the host firewall has increased dramatically. This made it possible to reduce the number of illegitimate requests to this node (Figure 2). 200th type of errors - useful queries in Figure 3 do not differ much from the similar parameter in Figure 2.

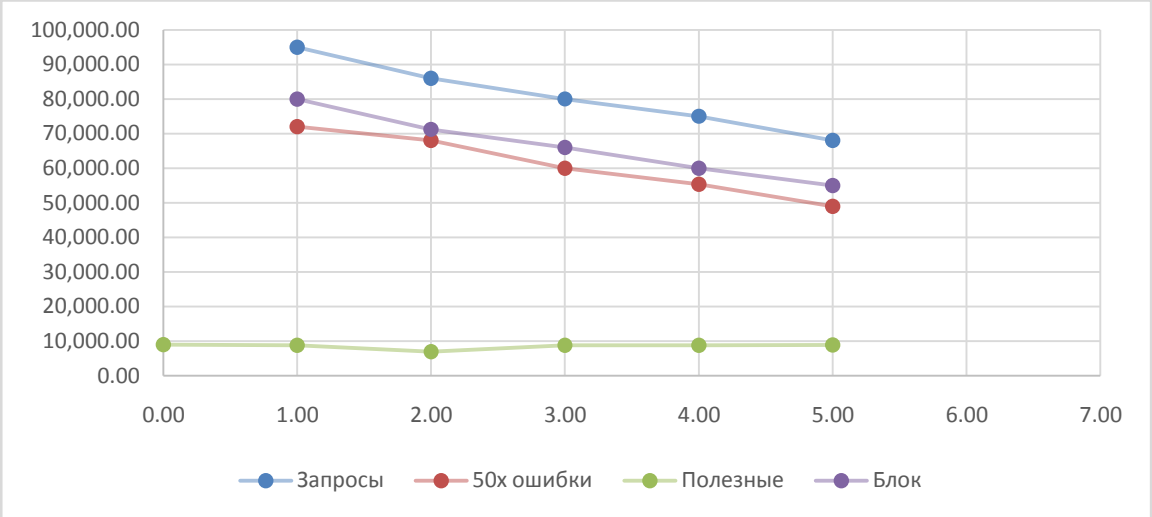

Figure 3 - Applications of the filtering system based on the neural network per hour after implementation

This parameter allows you to show the physical data of the server by the number of simultaneously processed requests. Thus, the implemented filtering method allows to increase the security of computer systems.

Verification of filtering rules with temporal characteristics using the "model checking" method. Verification of filtering rules is a pressing issue for many corporate computer network management systems based on security policies [4]. With the growth of the network size, and hence the number of shared resources and users, the filtering rules multiply and do not respond well to manual analysis[5]. Application of the method - model checking for verification of filtering rules reduces the risk of violation of such security properties as availability and confidentiality. The results of the experiments are presented in Figure 4 a, b. The calculations were performed on 12 samples, in which the number of rules and the number of anomalies changed. The number of rules increased from 5 to 50, and the number of anomalies from 0 to 15. According to the results of the experiments, all anomalies were detected.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 6 , June 2019

III. RESULT

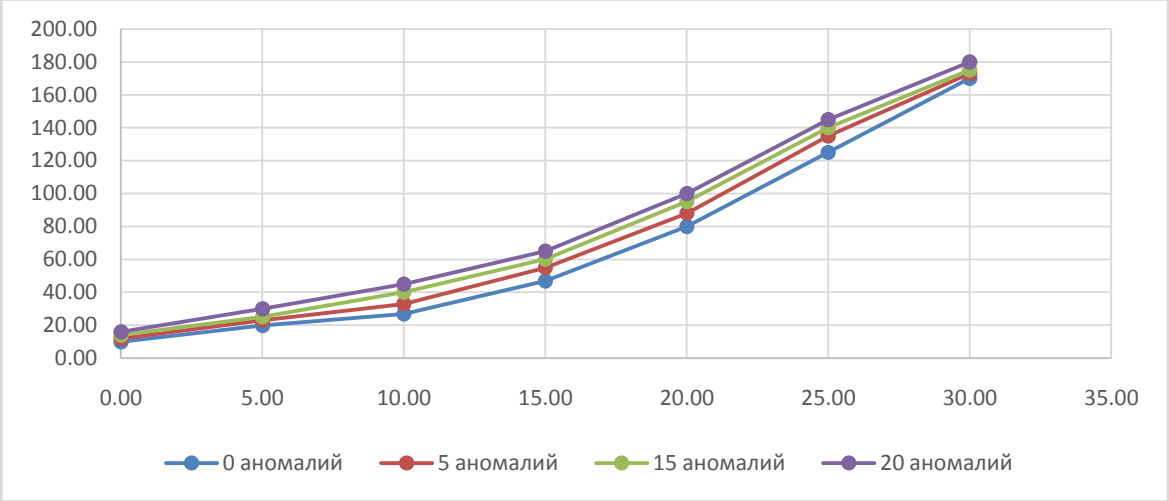

Figure 4 a - Results of experiments detecting traffic filtering anomalies

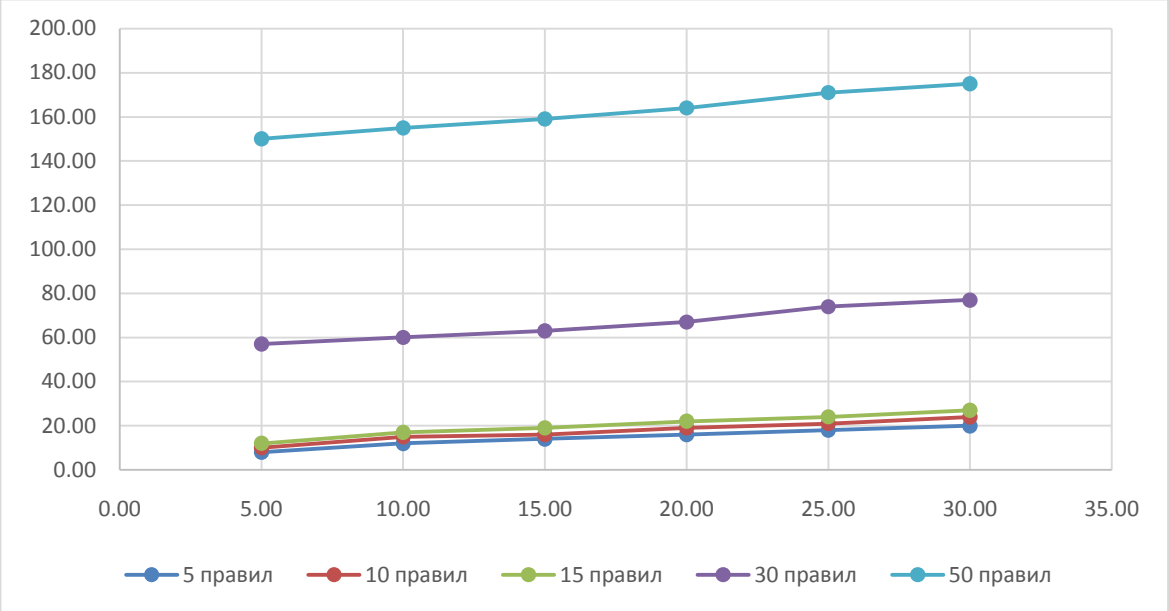

Figure 4 b - Results of experiments detecting traffic filtering anomalies

IV. CONCLUSION AND FUTURE WORK

According to the data obtained, the search time for anomalies, depending on the number of rules, grows exponentially and a linear dependence of the search time on the number of anomalies in the rules is revealed. Experiments have shown that the proposed method allows you to identify all the anomalies of filtering rules, but can be effectively used up to a certain number of rules. The introduction of temporal characteristics into the filtering rules did not significantly change the verification time.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 6 , June 2019

This work on the subject of the grant ËOT-Атех-2018-168“Improving methods and means of detecting attacks in computer networks”.

REFERENCES

[1] M.M. Karimov, Sh.R. Gulomov, B.K. Yusupov, "Approach development accelerate of process special traffic filtering", Journal of Computerand Communications, vol. 3, no. 9, pp. 68-82, September 2015.

[2]Kotenko I. Agent-Based Modelling and Simulation of Network Cyber-Attacks and Cooperative Defence Mechanisms // Discrete Event Simulations. Sciyo, In-teh, 2010. P.223-246.

[3] Kotenko I., Konovalov A., Shorov A. Agent-based Modeling and Simulation of Botnets and Botnet Defense // Conference on Cyber Conflict. CCD COE Publications. Tallinn, Estonia, 2010. P.21-44.

[4] Philip R. et al. Enabling Distributed Security in Cyberspace. Departament of Homeland Security, 2011. P.56-60.

[5] GulomovSherzodRajaboevich, NasrullayevNurbekBakhtiyorovich. Method for security monitoring and special filtering traffic mode in info communication systems // 2016 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent University of Information Technologies. Tashkent, Uzbekistan. Applications, Trends and Opportunities 2nd, 3rd and 4th of November 2016.

AUTHOR’S BIOGRAPHY

GulomovSherzodRajaboevich. Assistant professor. was born February 26, 1983 year in Shakhrisabz city, Republic of Uzbekistan. In 2009 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 120 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Information Security» in Tashkent University of Information Technologies.

KadirovMirhusanMirpulatovich. Assistant professor.
was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan.
Has more than 90 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of “Information technologies” in Tashkent State Technical University.

KhoshimovaCharosSaidaminovna. Assistant professor.
was born 31.12.1972 year in Tashkent city, Republic of Uzbekistan. Has more than 20 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of “Information technologies” in Tashkent State Technical University.

YuldashevaNafisaSalimovna. Assistant**.**Was born July4, 1984 year in Tashkent city, Republic of Uzbekistan. Currently works at the department of “Information technologies” in Tashkent State Technical University.