veral methods for this problem solution, with their application. Applying special programming means for the business model is as well described.

The business model is designed universally, which enables it to extend the result within the whole class of analogous models without alternating the algorithm of solution. So the object of the investigation is a business model of a multimodal logistics company and the focus is on methods of its solution. Its objective is to determine various methods to solve multicriteria optimization problems in transportation logistics. The paper demonstrates the most effective of all methods suggested and signifies the algorithm to solve the two-criteria multimodal logistics problem. To illustrate the algorithm, both real and model data are provided.

Key words: *business model, multimodal transport problem, multicriteria optimization, transport enterprise.*

Отримано: 19.10.2021

UDC 004.056
DOI: 10.32626/2308-5916.2021-22.58-66

Sherzod Gulyamov*, D-r of Tech. Science, Professor,
Fotima Sagatova**

*Tashkent University of Information Technologies named after Al – Khorezmi, Tashkent, Republic of Uzbekistan,
**Tashkent State Technical University
named after Islam Karimov, Tashkent, Republic of Uzbekistan

METHOD OF RISK DETECTION MODEL IN PACKET FILTERING

This article describes Petri net diagrams for fuzzy knowledge and reasoning. A mathematical model of fuzzy Petri nets to detect risks in rules by packet filtering is formed. A model of a two-level fuzzy packet filtering system that provides packet filtering performance is presented. This model uses fuzzy Petri net as a graphical method to describe the fuzzy logical control of the movement of packets through the firewall and allows it to determine the level of threat embedded in packets from the Internet and to change the order of ACLs by determining the rating of acceptance and rejection of packets. In the proposed model, the packet is represented by a token in place of fuzzy Petri nets, and the operation of the packet is illustrated by the transition of fuzzy Petri net, which is responsible for moving the packet from one place to another.

Key words: *tokens, Petri net, Access Control List (ACL), packet filtering, SYN-Flood, risks, Fuzzy logic, membership degree function.*

Introduction. With the advent of the Internet, there have been many changes in people's lives. These changes also affected firms. Most employees in modern companies do not use the Internet connection for its intended purpose. User's «choke» the channel using torrents, watching videos on the Internet, downloading files or playing online games. Social networks, entertainment portals and other sites, where thousands of new pages are infected every day and new modifications of well-known threats appear, have been and remain potential areas of risk for the spread of malware and causes of phishing attacks, causes of information leakage, theft of passwords and other spyware. To ensure the security and integrity of information, overlap channels of possible information leakage and improve network performance, it is necessary to control the traffic flow entering the local network. To filter Internet access, it is important to analyze network traffic that is generated by users. The solution to such uncontrolled traffic in any organization is filtering Internet requests.

The classical Petri net is a kind of directed graph consisting of points, transitions, directed arcs, markers. Directional arcs connect places with transitions or transitions with places. The transition is activated when each location in the transition precondition is fulfilled. The tokens that are located in the locations of the Petri net are used to determine the execution of the Petri net. The presence or absence of a token in a location may indicate whether the condition associated with that location is true or false and the number and position of tokens may change during the execution of the Petri net. In general, Petri net can be represented by a transition along with an entry point and an exit point. Petri net designations are shown in Figure 1.

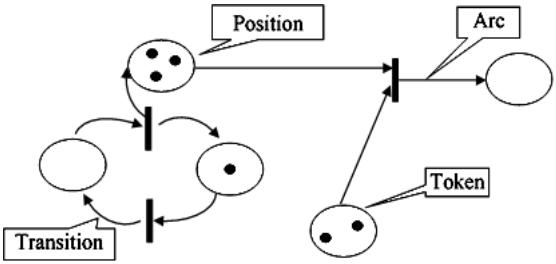

Fig. 1. *Petri net designations*

Risk Detection Model in Packet Filtering Rules Based on Fuzzy Petri Net. Fuzzy Petri Nets (FPNs) are a combination of fuzzy logic and Petri net. It is described as a Petri net that uses fuzzy logic rather than logic. FPNs are used to fuzzy knowledge and reasoning. The concept of fuzziness can be incorporated into Petri nets by applying a fuzzy reasoning mechanism to the structure of Petri net. Usually, FPN can model fuzzy production rules (like, if d_j, then d_k with confidence factor $(CF)\mu_i$.

Each location can contain a token associated with the truth value of a sentence, which is quantified by numbers in a unit interval [1-3]. Each transition is associated with a confidence factor that takes values from a unit interval. Formally, the FPN model is defined as a set of

$$N_f\left(P,T,D,I,\alpha,\beta\right),$$

where

$P \subset P_i$ for $\left(i=1, i \le n, i++\right)$ — a finite set of positions;

$T \subset T_i$ for $\left(i=1, i \le m, i++\right)$ — a finite set of transitions;

$D \subset D_i$ for $\left(i=1, i \le j, i++\right)$ — a finite set of sentences;

where

$P = \left\{T : (T,P) \in f\right\} \bigcup P = \left\{T : (P,T) \in f\right\}$ — this is the input mapping;

$T = \left\{P : (P,T) \in f\right\} \bigcup T = \left\{P : (P,T) \in f\right\}$ — this is the output mapping;

$f = \rightarrow [0,1]$ – displaying associations;

$\alpha : P \rightarrow [0,1]$; $\beta : P \rightarrow D$; $\mathrm{P} \bigcap T \bigcap D = \varphi, |P| = |D|$.

The value of the token at the position $p_i \in P$ is denoted by $\alpha(p_i) \in [0,1]$.

If $\alpha(p_i) = y_i$; $y_i \in [0,1]$ and $\beta(p_i) = d_i$; then this means that the degree of truth of the sentence d_i is equal to y_i. The transition t_i is allowed if for all $p_i \in I(t_i)$, $\alpha(p_i) \ge \lambda$, where λ is the threshold value in the unit interval. If this transition is triggered, then the token is removed from its entry locations and the token is placed in each of its exit locations. The truth value of the output tokens is usually calculated using some aggregation function τ.

$$y_k = \tau \prod_{j=1}^{n} y \prod_{i=1}^{m} \mu \text{ or } y_k = \tau\left(I\left(t_j\right), \mu_i\right), y_k \in \mathrm{O}\left(t_j\right).$$

In theory, Petri net and FPN have the same computational power, but FPN have much more modeling power because they have better structuring capabilities. Boolean expressions and functions can be constructed using fuzzy logic for all objects of the Petri net [4-7]. The FPN can efficiently analyze parallel systems, validating security rules and standards for transport operations and uses a graphical representation that is easy to understand and easy to modify due to its modularity.

Figure 2 shows a two-level fuzzy packet filtering model that provides filtering performance. The model uses FPN as a graphical method for describing fuzzy logic control over the movement of packets through a firewall. Two levels of fuzziness are applied to packets filtering:

- the first level, which allows it to determine the level of threat embedded in packets;
- the second level is used to change the order of the ACL by determining the acceptance and rejection ratings of packets.

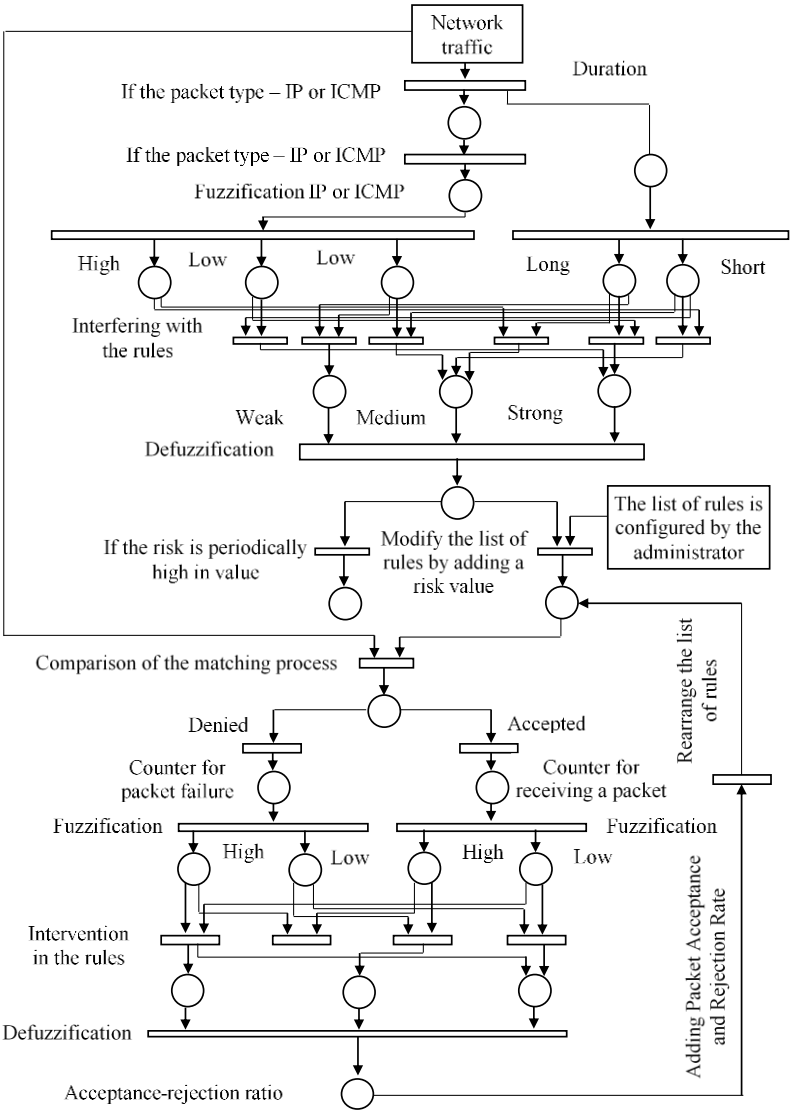

Fig. 2. *Two-level fuzzy packet filtering model*

First level: fuzzy filtering. This layer is based on capturing and classifying all incoming packets based on information associated with each packet, such as IP address, packet time and protocol type, to simulate and track packet movement [8; 9]. In the proposed model, the packet is represented by a token at the FPN location, and the packet operation is illustrated by the FPN transition, which is responsible for moving the packet from one location to another. Once the packet is captured by the gateway, it is moved to the position where it is checked and matched against the ACL, in addition, the snapshot of that packet is moved to the traffic analysis part to extract packet parameters such as the number of IP or ICMP packets arriving over a period of time. These two parameters are inputs to the fuzzy logic engine that is used to determine the level of risk. This level of risk represents the threats that result from moving packages from untrusted sources.

As it knows, the IP and ICMP protocols are used at many levels of an attacker's advance when hacking a system. In addition, the IP and ICMP protocols are used in some cases as a covert communication channel for attackers. This layer can also deal with attack methods using other protocols such as TCP SYN and UDP Flood. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams to slow down the victim to the point where they can no longer process valid connections. A distinctive feature of SYN-Flood attacks is that attackers send a large number of TCP SYN request packets with spoofed source IP addresses. This leads to the fact that the server side consumes a large number of resources to maintain a very large list of half-open connections, which ultimately leads to the fact that the server runs out of resources and becomes unable to provide normal services.

The rationale for choosing the number of ICMP echo request $p_{\text{echo}-\text{request}}$ packets and the p_{time} packet arrival time interval is that they are simple and suitable for most cases of protection against attacks, especially when it has a large number of whole packets. To satisfy the requirements of the membership degree function (MDF) used in the proposed fuzzy system, the measures for the feature vectors must be transformed into the range [0, 1] using the Gaussian normalization method. Fuzzy logic (FL) is probably the most efficient and flexible packet filtering method, allowing it to control a combination of measurements in terms of their degree of uncertainty. CL is a theory that allows natural linguistic descriptions of problems to be solved rather than using numerical values. The FL system consists of the following functions:

- fuzzifier that accepts input values and determines the degree of their belonging to each of the fuzzy sets through the MDF;

- a fuzzy inference system that defines a nonlinear mapping of an input data vector to scalar inference using fuzzy rules;
- defuzzifier that maps output fuzzy sets to a crisp number.

And so, here a fuzzy system with two inputs and one output is used, which is given by

$$f : U \subset \bigcup_{i=1}^{n} (R_n \cap V),$$

where $U = U_1 \times U_2$ — entrance space; R — filtering rules; V — outlet space.

Three fuzzy variables, including «Low», «Medium», and «High», are used to describe the $p_{\text{echo-request}}$ characteristic and two fuzzy variables, including Long and Short, are used to describe the p_{time} function. All membership function parameters are numerically specified based on experience to assess the level of risk arising through packet traffic. Once the system receives fuzzy descriptions of packet characteristics, a rule base can be built to infer that they are similar.

Fuzzy reasoning, which is formulated by a group of fuzzy If-Then rules, represents the degree of presence or absence of a connection or interaction between elements of two or more sets. Figure 3 shows packet filtering rules flowcharts (First level).

In general, the rules presented in Figure 3 imply weight assignment in the same way as humans. Fuzzy inference handles all cases in parallel, which makes the solution more reasonable [10]. The result of the fuzzy system is the risk level r_l, which characterizes the risk inherent in packet traffic.

Second level: fuzzy filtering. Typically, each firewall has two sets of packets associated with it: a set of packets that are accepted by the firewall and a set of packets that are discarded by the firewall. This model exploits this fact to improve packet filtering performance by applying Layer 2 fuzzy filtering to track the rate at which packets are accepted or rejected to minimize rule matching time. Here, an attempt is made to model the uncertainty in the rate of acceptance or rejection of packets using a fuzzy model. In this case, a fuzzy system with two inputs and one output is used. Two fuzzy variables including «Low» and «High» are used to describe both the receive rate counter A_r and the rejection rate R_r. The result of the fuzzy system is the computed rate C_r, which characterizes the rate of rejection and acceptance in packet traffic and is described by three fuzzy variables, including High Rejec-

tion, Equal, and High Accept [11]. Figure 4 shows packet filtering rules flowcharts (Second level).

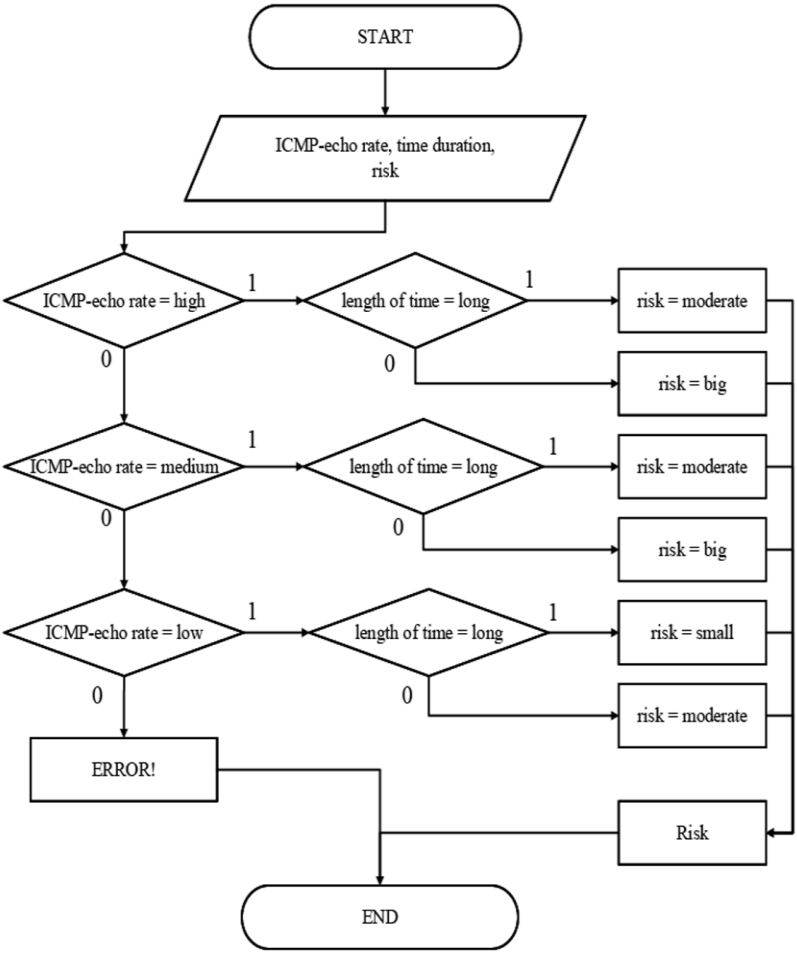

Fig. 3. *Packet Filtering Rules Flowcharts (First Level)*

The output fuzzy values are then defuzzied to generate a clear value for the variable. Here, if C_r = high acceptance, then all rules for which there is a permission action are reordered and moved to the top of the ACL with the highest priority to execute. Otherwise, if C_r = high rejection, then all rules that have a reject action are moved to the beginning of the ACL, taking the highest priority for execution and, as a consequence, rules that have an accept action stabilize at the end of the ACL.

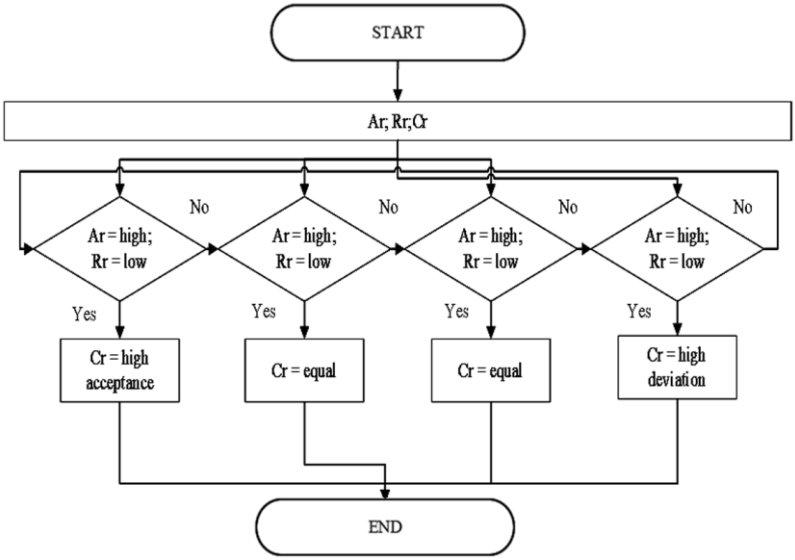

Fig. 4. *Packet Filtering Rules Flowcharts (Second Level)*

Conclusion. Thus, the proposed model has the ability to change the actions of the rules in two levels: at the first level, the action of the rule can be changed in accordance with the behavior of traffic based on the layer of risk; in the second level, the sequence of rules can be dynamically changed to reflect the highest priority of the rules based on the acceptance and rejection of packets.

References:

1. Thong W. J., Ameedeen M. A. A Survey of Petri Net Tools Advanced Computer and Communication Engineering Technology. *Lecture Notes in Electrical Engineering* / ed H. Sulaiman, M. Othman, M. Othman, Y. Rahim, N. Pee. 2015. Vol. 315. P. 537-551.
2. Zaitsev D. A. Toward the Minimal Universal Petri Net. *IEEE Transactions on Systems, Man, and Cybernetics: System.* 2013. P. 47-58.
3. Gulomov Sh., Ganiev A., Vaade V. Formalization of the business process security. *International conference on information science and communications technologies applications, trends and opportunities* (ICISCT). 4-6 November, 2019, Tashkent Uzbekistan.
4. Mirzaeva M. B., Suleymanov A. A. Communication network reliability evaluation using the simulation approach. *Technical Science and Innovation. Tashkent State Technical University named after Islam Karimov.* 2020. № 4 (06).
5. Karimov M. M., Gulomov Sh. R. IP-Traffic classification model based on machine learning ways. *Chemical Technology, Control and Management.* 2020. Vol. 2020. Is. 5 Special issue 5-6. P. 123-128.

6. Yusupov S. Y., Gulomov Sh. R. Improvement the schemes and models of detecting network traffic anomalies on computer systems. *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT).* Tashkent, Uzbekistan, 2020. P. 1-5.
7. Gulomov Sh. R., Yusupov S. Y. Improvement the schemes and models of detecting network traffic anomalies on computer systems. *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT).* Tashkent, Uzbekistan, 2020. P. 1-5.
8. Kodirov Z. Z., Karimov M. M., Tashev K. A., Gulomov Sh. R., Islomova M. X. Q. Artificial Intelligence, Ensuring Information Security in Virtual Robots And Extensive Use Of Smart Systems. *The American Journal of Engineering and Technology.* 2020 Vol. 02. Is. 08-04. P. 28-38.
9. Voronkov L. H., Iwaya L. A., Martucci S. Lindskog. Systematic Literature Review on Usability of Firewall Configuration. *ACM Computing Survey.* 2018. Vol. 50. № 6.
10. Gulomov Sh. R., Yusupov B. K., Kamilov Sh. Sh. ugli. Models and algorithms for solving problems associated with large amounts of data in the military sphere. *International Conference on Information Science and Communications Technologies, ICISCT 2020.* Tashkent; Uzbekistan.
11. Chao S., Yang S. J.-H. Towards a Usable Anomaly Diagnosis System among Internet Firewalls' Rules. *Journal of Internet Technology.* 2019. Vol. 20. № 3. P. 789-799.

МЕТОД МОДЕЛІ ВИЯВЛЕННЯ РИЗИКУ ПРИ ФІЛЬТРАЦІЇ ПАКЕТІВ

У цій статті описані діаграми мережі Петрі для нечітких знань і міркувань. Сформована математична модель нечітких мереж Петрі для виявлення ризиків в правилах за допомогою фільтрації пакетів. Представлена модель дворівневої системи нечіткої фільтрації пакетів, що забезпечує ефективність фільтрації пакетів. Ця модель використовує нечітку мережу Петрі в якості графічного методу для опису нечіткого логічного управління рухом пакетів через міжмережевий екран і дозволяє їй визначати рівень загрози, вбудованої в пакети з Інтернету, і змінювати порядок списків ACL шляхом визначення рейтингу. прийому і відхилення пакетів. У запропонованій моделі пакет представлений токеном замість нечітких мереж Петрі, а робота пакету ілюструється переходом нечіткої мережі Петрі, яка відповідає за переміщення пакета з одного місця в інше.

Ключові слова: *токени, мережа Петрі, список контролю доступу (ACL), фільтрація пакетів, SYN-Flood, ризики, нечітка логіка, функція ступеня приналежності.*

Отримано: 13.10.2021