РАДІОЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

RADIO ELECTRONICS AND TELECOMMUNICATIONS

UDC 621.396.946

FUZZY-LOGIC ALGORITHM FOR RISK ASSESSMENT IN WI-FI NETWORKS

Antipov I. – Doctor of sciences, Professor of the Department of Computer Radio Engineering and Technical Information Protection Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. ROR: https://ror.org/01ctj1b90. ORCID: https://orcid.org/0000-0002-9754-4412.

Vasylenko T. – PhD, Senior Lecturer of the Department of Computer Radio Engineering and Technical Information Protection Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine. ROR: https://ror.org/01ctj1b90. ORCID: https://orcid.org/0000-0003-1291-8065.

ABSTRACT

Context. With the increasing use of Wi-Fi wireless networks, the risk of attacks specific to them is also rising. Traditional protection methods, which usually rely on precise thresholds, do not reflect the actual uncertainty of the conditions in which wireless networks operate. Due to the openness of the radio channel, its instability, dispersion, and the presence of noise, a promising direction is the use of fuzzy logic algorithms, which allow for taking into account the incompleteness and ambiguity of data when assessing the risks of Wi-Fi wireless networks.

Objective. Develop a fuzzy logic algorithm for assessing the state of Wi-Fi networks, which allows adaptively determining the level of risk by analyzing wireless network parameters and making decisions regarding security system actions.

Method. A fuzzy-logic-based algorithm for analyzing the operational state of a wireless Wi-Fi network is proposed. The algorithm is based on the integrated analysis of six network parameters using elements of fuzzy logic. It includes the construction of membership functions for the input variables, the formation of a fuzzy IF–THEN rule base, and a defuzzification mechanism that provides a continuous numerical assessment of the network risk level. To evaluate the effectiveness of the proposed approach, a comparative simulation study was conducted against the classical threshold-based decision-making method. The study was carried out in the MathCAD and MATLAB environments to enable cross-validation of the algorithm's functionality. Three network operation scenarios were considered, with 100 network states simulated for each scenario.

Results. The simulation results obtained in the MathCAD and MATLAB environments coincide up to the third decimal place, confirming the correctness of the software implementation of the algorithm. Comparative analysis showed that the threshold-based method produces binary decisions and is highly sensitive to random fluctuations in network parameters, which leads to an increased number of false alarms. The proposed fuzzy-logic-based algorithm provides a continuous risk assessment, demonstrates lower result variance, and exhibits a stable response to changes in network conditions. Under unstable network operating conditions, the algorithm enables discrimination between noise and interference effects and the initial phases of attacks, while also ensuring a gradual increase in the risk level without abrupt transitions between linguistic levels. The obtained results confirm a reduction in Type I errors and an improvement in decision-making informativeness.

Conclusions. The fuzzy logic-based Wi-Fi network state analysis algorithm proposed in this work enables more adequate decision-making regarding the network's condition. The use of fuzzy logic allows adjusting decisions depending on changes in network operating conditions in real time and can be integrated into intrusion detection systems or advanced wireless network cybersecurity tools.

KEYWORDS: Cybersecurity, Wi-Fi, intrusion detection systems, fuzzy logic, risk assessment.

ABBREVIATIONS

Auth_Fails is a number of failed authentications per minute;

Clients is a number of connected subscribers;

Com_Rule is a comprehensive assessment according to all rules;

ETX is an Expected Transmission Count;

IDS is an intrusion Detection System;

IEEE is an Institute of Electrical and Electronics Engineers;

IIoT is an Industrial Internet of Things;

Probe_Rate is a frequency of probe requests;

ROC is a Receiver Operating Characteristic;

RSSI_Var is a signal level variance;

S 1, 2, 3 is a scenario 1, 2, 3;

Traffic_Anomaly is a percentage of anomalous traffic;

Wi-Fi is a wireless fidelity;

WPA is a Wi-Fi Protected Access.

DOI 10.15588/1607-3274-2026-1-1

NOMENCLATURE

a is a the first point of the trapezoid;
A_{ik} is a fuzzy sets of the corresponding terms;
b is a the second point of the trapezoid;
B_k is a fuzzy sets of the corresponding terms;
c is a the third point of the trapezoid;
d is a the fourth point of the trapezoid;
j is a number of the linguistic term;
x_i is an input parameter;
y is an output parameter;
μ_{ij} is a membership function.

INTRODUCTION

In the modern world, wireless networks are extremely relevant and play an important role in people's lives. Many companies successfully use wireless local area networks to manage production processes, while hospitals deploy wireless networks to improve operational efficiency and convenience. The basic standard for wireless local area networks is the IEEE 802.11 standard, various versions of which regulate data transmission in the 2.4 and 5 GHz bands, as detailed in [1–4]. In practice, the actual communication range usually does not exceed 200 meters.

Since 802.11 standard devices communicate with each other over the radio spectrum, any other station operating in this band can also receive this data. To ensure at least a minimal level of wireless network security, encryption mechanisms based on WPA and WPA2 algorithms [5, 6] are used, as well as intrusion detection systems (IDS) [7].

This work considers an algorithm for analyzing the state of a wireless Wi-Fi network using elements of fuzzy logic. This algorithm allows making decisions regarding the presence of potential security threats, taking into account various or rapidly changing conditions that traditional intrusion detection systems (IDS) [8] do not consider.

The object of study is the operation process of a wireless Wi-Fi network and its functional parameters, which characterize the security state during subscriber access and data transmission.

The subject of study is methods and models of fuzzy logic assessment of risk levels in Wi-Fi networks based on the analysis of technical parameters (signal level, number of connected clients, number of failed authentications, traffic anomalies, signal level variance, and frequency of probe requests).

The purpose of the work is to develop and investigate a fuzzy logic algorithm for assessing the security risk level of a Wi-Fi network based on a set of its technical indicators. The algorithm should provide automated interpretation of traffic characteristics, connection states, and client behavior, generating both quantitative and linguistic risk assessments in real time.

1 PROBLEM STATEMENT

The input data are represented by a vector of observed parameters: $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$, where x_1=RSSI, dBm [–90,–30]; x_2=Auth_Fails [0,20]; x_3=Traffic_Anomaly [0, 100]; x_4=Clients [0, 50]; x_5= RSSI_Var[0, 25]; x_6 = Probe_Rate [0, 20].

It is necessary to construct fuzzy membership functions for each variable: $\mu_{ij}(x_i): X_i \to [0,1]$.

The output variable is the network state risk level: $y = Risk\_Level \in [0,1]$, which is also described by a set of linguistic terms: $\{no\_risk, low\_risk, medium\_risk, high\_risk\}$.

A Mamdani-type fuzzy rule base should be formed: $R_k : IFx_1 \in A_{1k} AND...ANDx_6 \in A_{6k} THENy \in B_k$.

Quality criteria include:

– correctness of the fuzzy interpretation of network states;

– consistency of results in MathCAD and MATLAB environments;

– the ability of the algorithm to generate values of corresponding to expected scenarios (“no risk,” “low,” “medium,” “high”);

– stability of results under variations of input parameters.

Additional constraints: all input parameters must belong to their allowed intervals; membership functions must provide full coverage of the respective universes; the rule base must be minimally sufficient yet adequate to account for all typical network states.

2 REVIEW OF THE LITERATURE

Fuzzy logic is not merely a theoretical tool; it is actively used in practice for ensuring security and assessing risk in various types of wireless networks, as evidenced by a large number of published works on this topic.

In [9], the authors propose a model for analyzing information security risks in IIoT. They developed several fuzzy inference systems for assessing overall risk. The model reflects real conditions of attacks and threats, but it is tailored to IIoT systems rather than traditional Wi-Fi networks, which have their own specific characteristics.

The study in [10] demonstrated the use of fuzzy logic to detect jamming attacks in wireless mesh IoT networks. The authors used ETX metrics, the number of retransmissions, undelivered packets, and packet delivery ratio as input parameters. The system was evaluated using standard metrics (accuracy, precision, recall, ROC). This work demonstrates that the fuzzy approach can be effective even in complex attack scenarios at the physical and data link layers. Despite the high effectiveness of this method against jamming attacks, it may be less suitable for typical Wi-Fi attacks, as it relies on a limited set of parameters that are not fundamental for Wi-Fi networks.

The work in [11] is devoted to improving the accuracy of IDS. To achieve this, the authors combine fuzzy

DOI 10.15588/1607-3274-2026-1-1

logic, neural networks, and a genetic algorithm. This study demonstrates that fuzzy logic can be successfully integrated with modern machine learning methods to achieve higher efficiency. However, such a method is complex to implement and requires significant resources, which may be critical for a real Wi-Fi network.

The publication [12] investigates IDS based on fuzzy logic. The authors showed that using fuzzy models with classical membership functions can significantly outperform traditional threshold-based approaches in terms of accuracy, especially when dealing with limited or noisy data. Since this model uses triangular membership functions and lacks a learning mechanism, it limits the flexibility of the wireless network under dynamic network conditions, when monitoring is most necessary.

Few studies consider the combination of risk assessment with security at the Wi-Fi level. Most research focuses on IoT/IIoT, where network structures and characteristics differ significantly.

Therefore, the development of fuzzy logic algorithms for risk assessment in Wi-Fi networks remains a relevant and timely task.

3 MATERIALS AND METHODS

The main element of using fuzzy logic is the membership functions. They determine the degree of belonging of an output variable to a linguistic term. Most often, triangular membership functions are used because they are simple to compute and clearly illustrate the process of fuzzy evaluation of wireless system parameters. However, in real systems, they are not sufficiently informative.

In this work, trapezoidal membership functions are used to describe fuzzy linguistic variables, which are well suited for changes in real Wi-Fi network parameters such as signal strength, the number of connected clients, the frequency of failed authentications, and the traffic anomaly index. Membership functions of this type simplify the construction of fuzzy logic rules for wireless networks.

The work describes membership functions for working hours in a secured enterprise. Analogous membership functions should be created for different scenarios (working hours, vacation periods, nighttime). For instance, during nighttime, when only stationary devices (e.g., cameras) operate in the enterprise, if the system detects that 30 subscribers are connected to the network, this is considered an anomaly, unlike during working hours.

The general formula for a trapezoidal membership function is as follows:

$$\mu_{ij} = \begin{cases} 0, x \le a, \\ \dfrac{x-a}{b-a}, a < x \le b, \\ 1, b < x \le c, \\ \dfrac{d-x}{d-c}, c < x \le d, \\ 0, x \ge d. \end{cases} \quad (1)$$

To determine the signal level, we use three linguistic terms: “weak” with trapezoid points [–90;–80;–70], “medium” [–80;–70;–60;–50], and “strong” [–60;–50;–40;–30].

The membership functions for the signal level are shown in Fig. 1.

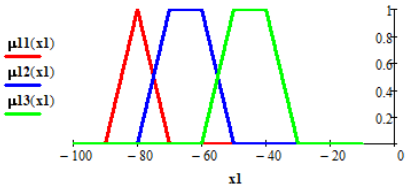


Figure 1 – Signal level membership functions

To determine the number of failed authentications, we use three linguistic terms: “low level” [0;0;1;3], “medium level” [2;5;8;12], and “high level” [10;15;20;20]. The membership functions for the number of failed authentications are shown in Fig. 2.

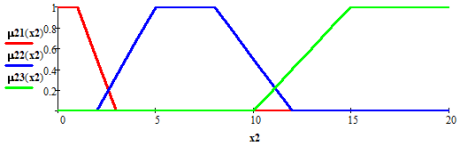


Figure 2 – Membership functions of the number of failed authentications

When determining the percentage of anomalous traffic, three linguistic terms were used: “normal” [0;0;10;30], “suspicious” [20;40;60;80], and “critical” [70;85;100;100]. The membership functions for the percentage of anomalous traffic are shown in Fig. 3.

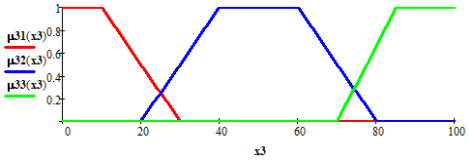


Figure 3 – Membership functions of the percentage of anomalous traffic

When determining the number of connected subscribers, three linguistic terms are used: “few” [0;0;5;15], “normal” [10;20;30;40], and “many” [30;40;50;50]. The membership functions for the number of connected clients are shown in Fig. 4.

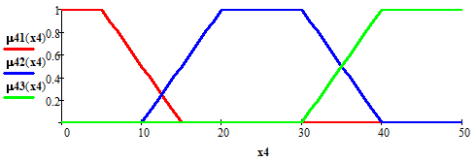


Figure 4 – Membership functions of the number of connected clients

To determine the signal level variance over a short interval, three linguistic terms are used: “stable signal”

DOI 10.15588/1607-3274-2026-1-1

[0;0;2;4], “moderate instability” [4;6;10;12] , and “high signal instability” [10;14;25;25]. The membership functions for the signal level variance over a short interval are shown in Fig. 5.

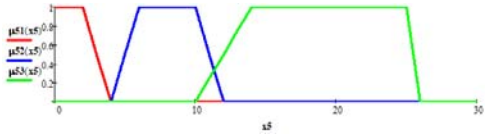


Figure 5 – Membership functions of the signal level dispersion over a short interval

To determine the frequency of probe requests, three linguistic terms are used: “low frequency” [0;0;10;20], “moderate frequency” [20;30;50;60], and “high frequency” [50;70;120;120]. The membership functions for the frequency of probe requests are shown in Fig. 6.

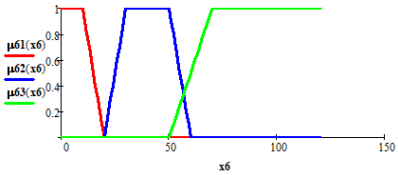


Figure 6 – Probe frequency membership functions

The output variable of the fuzzy system in this work is the “Risk Level.” It represents a generalized assessment of the state of the wireless network and is used for decision-making. The variable is formed based on a combination of the system’s input parameters. Each of these parameters can partially correspond to different linguistic states, so the risk assessment result is also expressed as degrees of membership to the corresponding linguistic terms. For the output variable, four linguistic terms have been defined to represent the level of threat: “no risk” [0;0;0;0.3], “low risk” [0.2;0.3;0.5;0.6], “medium risk” [0.4;0.5;0.8;0.9], and “high risk” [0.7;0.8;1;1]. The membership functions of the output variable are shown in Fig. 7.

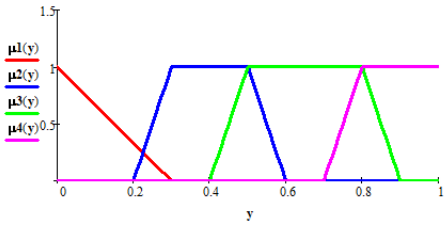


Figure 7 – Membership functions of the output variable

This representation helps to avoid abrupt jumps in decision-making and ensures smooth changes in the system’s response with small variations in network parameters.

To create a security system for a wireless Wi-Fi network, six input parameters and one output parameter were used. Considering all possible combinations would require 729 rules. To prevent overloading the system while still demonstrating its effectiveness, a simplified rule base was developed in this work, where the system’s response is determined by the factors that most significantly influence network risks. For example, if the system indicates that traffic is anomalous, the number of users or the signal level becomes almost irrelevant – the risk will still be high. Similarly, if the number of failed authentications is high and there is simultaneously a large number of probe requests, this almost always indicates the presence of an attack.

Algorithm processing procedure:

1. At the first stage, data is collected. In real time, the security system receives data from the access point or through specialized software that analyzes the data transmission environment.

2. At the second stage, membership functions consisting of linguistic terms are assigned to all six input parameters and the single output parameter. In our case, trapezoidal functions are used, which evaluate each parameter from 0 to 1.

3. The third stage involves creating the rule base. In this work, rules were developed using several experts and statistical analysis of medium-sized wireless Wi-Fi networks. The resulting rule base contains 20 rules in an “IF–THEN” format.

4. At the fourth stage, all rules are evaluated to determine how well they correspond to the current state of the wireless network. Computation is carried out using fuzzy logic by calculating the minima of the membership functions, as this method is classical for the Mamdani-type system used in this work.

5. After transforming features into fuzzy linguistic variables and computing them, a comprehensive assessment of all parameters is performed. This stage involves combining all rule sets that are above zero into a single function that characterizes the network risk level using the maximum operation. If several rules indicate a high security risk at different levels, they are aggregated. Aggregation is performed by taking the highest values at each point. As a result, a curve is obtained that characterizes the current state of the wireless network.

6. After the comprehensive evaluation of all parameters, the defuzzification process is performed to convert the linguistic variable into a numerical value.

7. Based on the number obtained after defuzzification, the system determines the security state of the wireless network according to the corresponding risk level:

– 0–0.299 – no risk (normal operation),
– 0.3–0.599 – low risk (enhanced monitoring),
– 0.6–0.799 – medium risk (event logging),
– >8 – high risk (automatic blocking or administrator notification).

8. At the final stage, the resulting security decision of the system is made.

9. As an additional but very important function, implemented after decision-making, feedback allows the security system to learn responses to attacks it has already encountered, adjust membership functions, or modify the system’s response to specific activities.

The structural diagram of the algorithm implementing network analysis functions using fuzzy logic is shown in Fig. 8.

DOI 10.15588/1607-3274-2026-1-1

4 EXPERIMENTS

The purpose of the experiment is to verify the functionality of the proposed wireless network protection model. To simulate the operation of the proposed security system, which uses elements of fuzzy logic, two software environments were employed: MathCAD and MATLAB.

Using two independent software environments allowed verification of the correctness of the proposed algorithm and detection of possible errors. MathCAD enables step-by-step implementation with mathematical descriptions and graphical visualization, but errors may occur during algorithm development. Therefore, MATLAB was also used, which performs all calculations automatically and provides only graphical visualization of the algorithm.

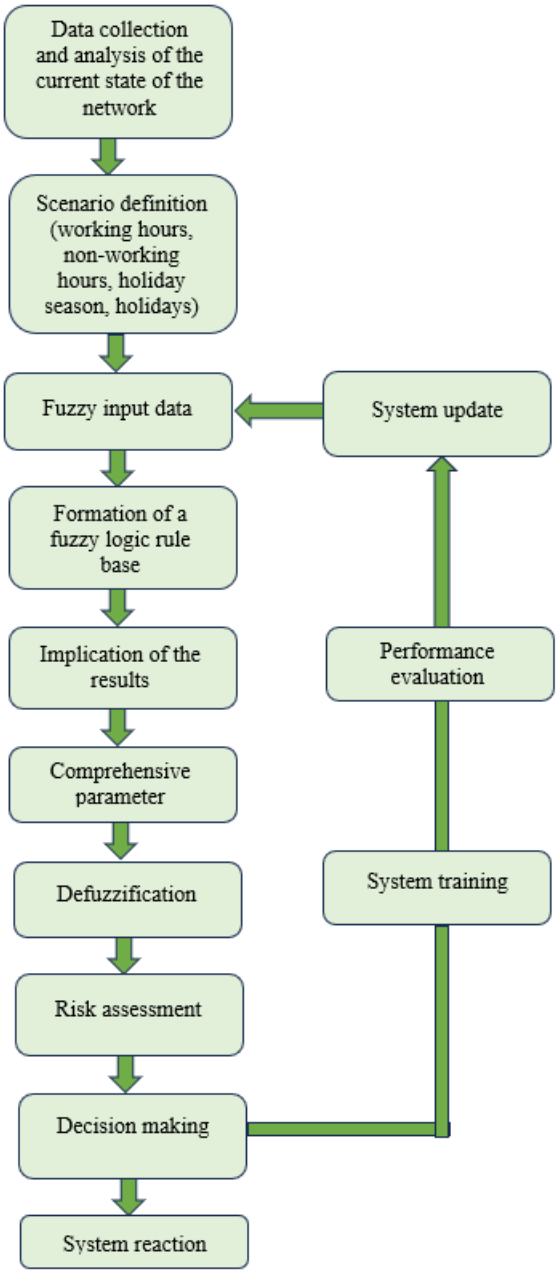


Figure 8 – Block diagram of an algorithm that implements network analysis functions using fuzzy logic

During the implementation of the algorithm in both software environments, identical operating conditions were applied (the same six input parameters, the same membership functions, the same rule base with 20 rules, the same defuzzification method – center of gravity, and identical test input combinations).

According to (1), in both software environments, the rules were implemented prior to the realization of the trapezoidal membership functions for the input and output parameters.

For implementing the relationships within the rules, the Mamdani model was used with the t-norm as the minimum operator. The rules implemented in the MathCAD environment are shown in Fig. 9

1. R1 := μ33(x3)
2. R2 := min(μ32(x3), μ22(x2))
3. R3 := min(μ32(x3), μ43(x4))
4. R4 := min(μ31(x3), μ41(x4))
5. R5 := min(μ23(x2), μ63(x6))
6. R6 := min(μ22(x2), μ62(x6))
7. R7 := min(μ21(x2), μ31(x3))
8. R8 := min(μ11(x1), μ53(x5))
9. R9 := min(μ11(x1), μ52(x5))
10. R10 := min(μ13(x1), μ51(x5))
11. R11 := min(μ43(x4), μ32(x3))
12. R12 := min(μ43(x4), μ23(x2))
13. R13 := min(μ42(x4), μ31(x3))
14. R14 := min(μ53(x5), μ63(x6))
15. R15 := min(μ53(x5), μ32(x3))
16. R16 := min(μ51(x5), μ61(x6))
17. R17 := min(μ31(x3), μ21(x2))
18. R18 := min(μ31(x3), μ51(x5))
19. R19 := min(μ31(x3), μ61(x6))
20. R20 := min(μ31(x3), μ41(x4))

Figure 9 – Rule base

For horizontal truncation, the MIN implication was used.

To perform a comprehensive evaluation of the parameters across all rules, the S-norm function using the maximum value was applied:

$$Com\_Rule = \max(Rule1(y), Rule2(y)...Rule20(y)).$$

To obtain a result, the system must convert the set of values into a single number. For this purpose, defuzzification is used, employing the center of gravity method:

$$Risk = \frac{\sum_{y}(y \cdot Com\_Rule(y))}{\sum_{y}(Com\_Rule(y))}.$$

To compare the classical threshold method of analyzing a wireless Wi-Fi network and the proposed algorithm that analyzes the network using elements of fuzzy logic, a comparative experimental study was conducted using the MathCAD software environment. Three scenarios were considered. S 1 – normal network operation; S 2 – unstable conditions (large signal dispersion, fluctuations in traffic parameters caused by noise, interference and dynamic changes in the communication channel, without active attacks); S 3 – the initial phase of the attack (high level of unsuccessful authentications, high frequency of probe requests). For each scenario, a sequence of 100 network states was generated and processed, the same for both network analysis methods.

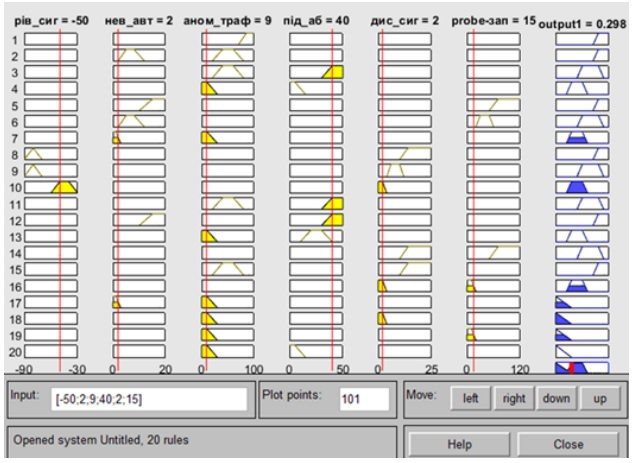
DOI 10.15588/1607-3274-2026-1-1

5 RESULTS

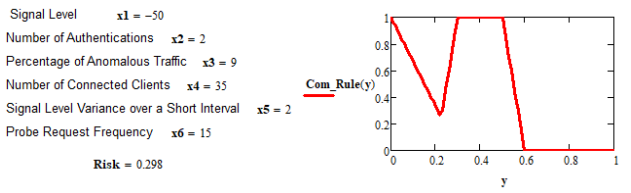
To demonstrate the operation of the security system, modeled input parameters were fed into the model. As an example, the network state "No Risk" is shown. Input data: $x_1 = -50$; $x_2 = 2$; $x_3 = 9$; $x_4 = 35$; $x_5 = 2$; $x_6 = 15$. The results are shown in Fig. 10a, implemented in MATLAB, and Fig. 10b, implemented in MathCAD.

In Fig. 10a, all 20 rules are shown, indicating which rules are activated and to what extent, with implication applied. For each rule, the resulting membership function is displayed, and at the very bottom, the aggregated membership function after the comprehensive evaluation, consisting of all activated rules, is shown. Additionally, the numeric result is shown above the resulting membership functions.

In Fig. 10b, the input data and the resulting value are demonstrated, matching the MATLAB results up to the third decimal place. The resulting membership function is also shown, which completely coincides with the one obtained in MATLAB.



a



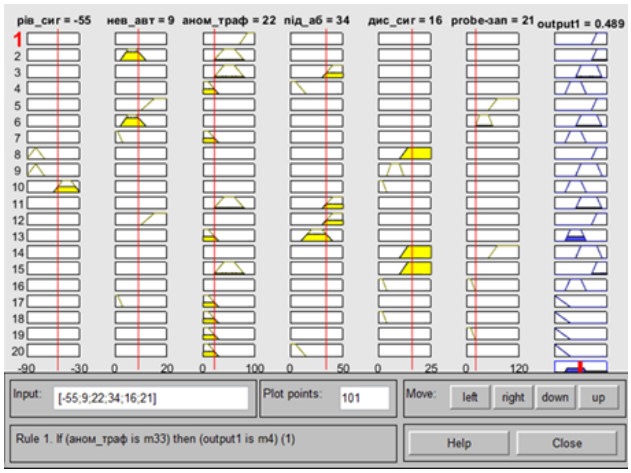
b

Figure 10 – In the network under study, the status is "No risk" : a – implementation in MATLAB; b – implementation in MathCAD

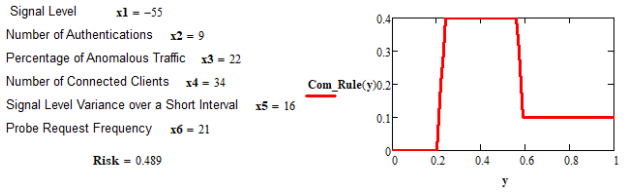
For the network state "Low Risk," the results are shown in Fig. 11. Input data: $x_1 = -55$; $x_2 = 9$; $x_3 = 22$; $x_4 = 34$; $x_5 = 16$; $x_6 = 21$.

For the network state "Medium Risk," the results are shown in Fig. 12. Input data: $x_1 = -60$; $x_2 = 3$; $x_3 = 15$; $x_4 = 24$; $x_5 = 5$; $x_6 = 25$.

For the network state "High Risk," the results are shown in Fig. 13. Input data: $x_1 = -75$; $x_2 = 15$; $x_3 = 85$; $x_4 = 45$; $x_5 = 19$; $x_6 = 44$.

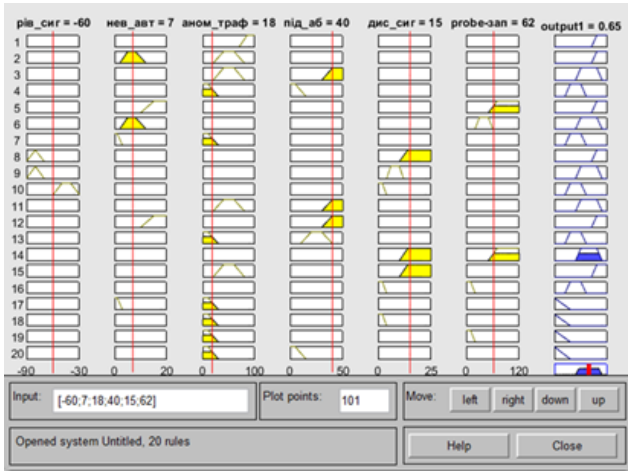


a

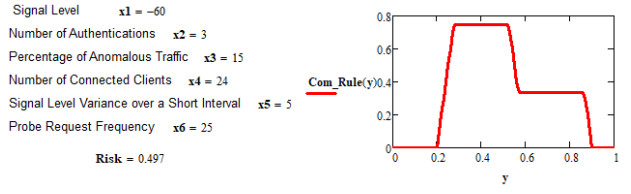


b

Figure 11 – In the network under study, the status is "Risk is low" : a – implementation in MATLAB; b – implementation in MathCAD



a

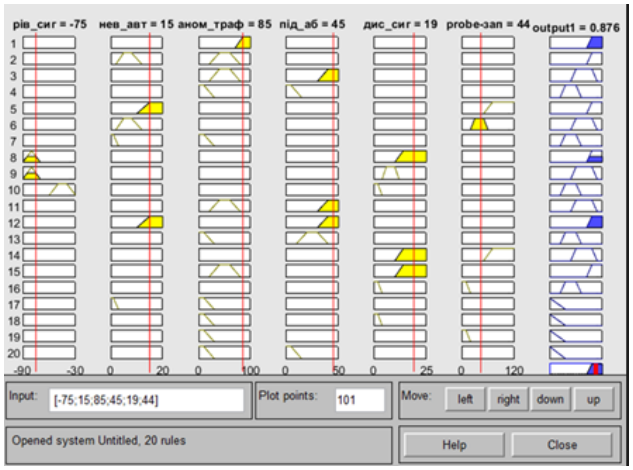


b

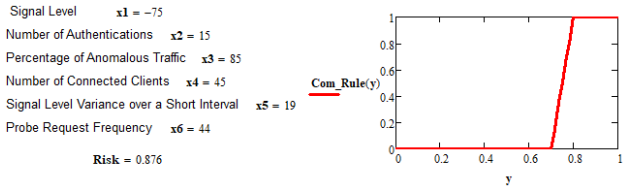
Figure 12 – In the network under study, the status is "Risk Medium" : a – implementation in MATLAB; b – implementation in MathCAD

For S1–3, 100 consecutive network states were generated. The values presented in Tables 1 and 2 correspond to statistical characteristics (mean and standard deviation) calculated over these 100 simulations. Table 3 presents representative risk values illustrating the transition dynamics during the initial attack phase.

DOI 10.15588/1607-3274-2026-1-1



a



b

Figure 13 – In the network under study, the status is “Risk is high” : a – implementation in MATLAB; b – implementation in MathCAD

The threshold-based method produces binary decisions for each network state (attack / no attack). Therefore, the values presented in Tables 1–3 represent the alarm frequency calculated over 100 simulated network states rather than a continuous risk level. In contrast, the proposed fuzzy-logic algorithm provides a smooth risk assessment that reflects gradual changes in network conditions.

Table 1 – Risk assessment results for different Wi-Fi network scenarios

Scenario	Alarm frequency based on threshold value	Fuzzy-logic risk
S1	5%	0.18
S2	62%	0.46
S3	88%	0.82

Table 2 – Stability of methods

Method	Mean alarm frequency	Standard deviation
Alarm frequency based on threshold value	0.62	0.31
Fuzzy-logic risk	0.47	0.08

Table 3 – Risk evolution during the initial phase of the attack

Network state index	Threshold-based decision	Fuzzy-logic algorithm
1	0	0.32
20	0	0.48
40	1	0.66
60	1	0.78
80	1	0.86

6 DISCUSSION

As can be seen from Figs. 10–13, the results are identical across different software environments, as also demonstrated in Table 4.

Table 4 – Comparison of Results

Network State	MathCAD Result	MATLAB Result	Difference
No Risk	0.298	0.298	0
Low Risk	0.489	0.489	0
Medium Risk	0.65	0.65	0
High Risk	0.876	0.876	0

Thus, the proposed algorithm correctly determines the risk levels. The results obtained in both software environments match with an accuracy of 10^{-3} (the same precision used during calculations), which confirms the correctness of the implementation of the fuzzy-logic-based wireless network protection system. The dual implementation of the algorithm demonstrated consistent results, indicating the reliability of the proposed approach to network risk assessment. The actions of the fuzzy-logic algorithm depend on the risk level determined by the system at a given moment.

When the system determines the result “Low Risk,” it means that the network is operating in normal mode without any suspicious activity, i.e., all network parameters are within acceptable limits. In this case, the system continues its regular operation and periodically logs the network status (RSSI, number of clients, traffic). No additional actions are taken so as not to overload the security system.

For example, the signal level is stable, the number of clients corresponds to the expected value for the given time and day of the week, failed authentications are rare, and the traffic shows no anomalies.

With “Medium Risk,” the wireless security system detects certain deviations in the analyzed indicators, but these deviations are not significant. In such a situation, occasional network malfunctions, repeated authentications, or signal instability may occur. This indicates that the likelihood of an attack is not high, but the network still requires increased monitoring. In this case, the system begins enhanced monitoring of the network: it collects data more frequently (for instance, if under normal conditions data is received every minute, it may start receiving updates every 10 seconds); it begins recording an extended list of parameters in the log (probe requests, traffic anomalies); it analyzes nearby access points (in case a rogue access point attack is being attempted). The system may also limit data transfer rates for certain suspicious clients or request re-authentication from them. At this risk level, the administrator receives a notification about the network status

For example, if the security system detects a decrease in signal strength for several clients and a slight increase in the number of probe requests, but without any loss of connection.

When a “High Risk” level is identified, it means that the wireless security system has detected signs of an on-

DOI 10.15588/1607-3274-2026-1-1

going attack (a suspicious client, password-guessing attempts, or atypical traffic). In this situation, an entry is made in the security log, recording the time, MAC address, and other signal parameters. The system sends a notification to the administrator marked "WARNING", may block suspicious clients, and also forwards a signal to the intrusion detection system to compare signatures with a database of known attacks.

For example, if a client or several clients exhibit suspicious activity – changes in signal strength, authentication errors, and traffic that is not typical for the user – this is highly likely to indicate the beginning of a man-in-the-middle attack.

In the case of "Critical Risk," the network exhibits activity that clearly indicates an active attack on the Wi-Fi wireless network: eavesdropping on communication channels, rogue access points, mass authentication requests, or a sharp increase in probe requests. During such aggressive activity, the security system responds immediately, blocking the malicious activity. This may include complete traffic blockage in a specific segment, after which the administrator is notified of the threat. A security log entry is also created, containing all current parameters.

For example, if the traffic is abnormal, there is a high number of authentications, and the signal strength drops sharply, this may indicate a DoS attack, an access point spoofing attack, or network client scanning.

Traditional algorithms use fixed thresholds. If a low threshold is set, a high percentage of Type I errors (missed attacks) will occur. Conversely, if the threshold is set too high, a large number of Type II errors (false positives) will occur. Both cases negatively affect the operation of the wireless network. Choosing the "golden middle" is practically impossible.

The experimental results (Tables 1–3) demonstrate a fundamental difference between the classical threshold-based approach and the proposed fuzzy-logic-based risk assessment algorithm when applied to Wi-Fi network monitoring.

First, the results presented in Table 1 show that under normal operating conditions (S1), the threshold-based method generates a nonzero alarm rate (5%), indicating the presence of false positives caused by random fluctuations in network parameters. In contrast, the fuzzy logic algorithm produces a low continuous risk value (0.18), which reflects a more adequate interpretation of minor deviations and helps to avoid unnecessary alarm triggering.

Under unstable but benign conditions (S2), characterized by increased signal variance and traffic fluctuations, the limitations of the threshold-based approach become more evident. The alarm rate increases to 62%, which complicates reliable decision-making and may lead to excessive security responses. At the same time, the fuzzy logic algorithm assigns a moderate risk level (0.46), indicating a degradation in network conditions without explicitly classifying it as an attack. This behavior confirms the ability of the proposed algorithm to distinguish between channel-induced instability and malicious activity.

During the initial phase of an attack (S3), both methods detect anomalous behavior. However, their results differ significantly in terms of interpretability. The threshold-based method rapidly switches to a high alarm rate (88%), providing only binary information. In contrast, the fuzzy logic algorithm generates a high but unsaturated risk value (0.82), enabling the system to track the progression of the attack and to provide adaptive security responses.

The robustness of both methods is further illustrated in Table 2. The standard deviation of the fuzzy logic risk values is significantly lower than that of the threshold-based alarm rate (0.08 versus 0.31). This indicates that the proposed algorithm provides a more stable assessment under varying network conditions and is less sensitive to random noise and short-term parameter fluctuations.

The temporal evolution of risk during the initial attack phase, shown in Table 3, highlights an important advantage of the fuzzy logic approach. While the threshold-based method produces abrupt transitions from "no attack" to "attack," the fuzzy logic algorithm reflects a gradual increase in risk as network conditions deteriorate. This property is particularly important for early attack detection and proactive security management in wireless networks.

The proposed fuzzy logic algorithm does not merely replicate threshold-based decisions but extends them by providing a continuous, interpretable, and noise-resilient risk assessment. This makes the approach more suitable for real Wi-Fi network environments, which are inherently characterized by parameter variability, channel noise, and transient states.

The proposed algorithm, which uses elements of fuzzy logic, introduces four output terms, allowing the reduction of both Type I and Type II errors.

The developed algorithm for network state decision-making is recommended for implementation within an intrusion detection system in companies, offices, and other environments using IEEE 802.11 wireless networks. Such network protection is particularly advisable in locations where valuable information is stored and there is a risk of unauthorized network access. The proposed model is relevant because it does not require significant resources, is user-friendly, and significantly enhances the security of the wireless network. Moreover, a fuzzy-logic-based decision-making model can detect attacks whose signatures are unknown.

In combination with the methodologies discussed in [13, 14], this algorithm can serve as a reliable protection system for Wi-Fi wireless networks.

CONCLUSIONS

The problem of improving decision-making reliability in Wi-Fi network state analysis under conditions of uncertainty is addressed in this work.

The scientific novelty of the obtained results consists in the development of a fuzzy-logic-based algorithm for

DOI 10.15588/1607-3274-2026-1-1

Wi-Fi network state assessment that enables adaptive interpretation of network parameters using fuzzy rules and membership functions. The proposed approach allows smoother transitions between network states and reduces the impact of abrupt parameter changes, which improves the adequacy of anomaly detection compared to threshold-based methods.

The obtained results enable more stable identification of abnormal network conditions and contribute to reducing false alarms in dynamically changing environments.

The practical significance of the results lies in the possibility of using the developed algorithm in Wi-Fi monitoring and security systems operating in automatic or expert-assisted modes. The results of modeling confirm the applicability of the proposed approach for practical network state analysis tasks.

Prospects for further research include extending the set of analyzed parameters and conducting quantitative evaluation of detection efficiency in real-world wireless environments.

ACKNOWLEDGEMENTS

We thank the Department of Computer Radio Engineering and Technical Information Protection Systems of the Kharkiv National University of Radio Electronics for the opportunity to conduct scientific research.

SOFTWARE AVAILABILITY

MATLAB R2018b (MathWorks Inc., Natick, MA, USA) was used for numerical simulations and data processing. The software was used under a valid professional license.

DECLARATIONS

Conflict of interest: The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship, or otherwise, that could affect the research and its results presented in this paper.

Authors' contributions: Ivan Antipov: a method for analyzing the state of functioning of a Wi-Fi wireless network, which analyzes network parameters using fuzzy logic elements; Tetiana Vasylenko: experimental study of a method for analyzing the state of functioning of a Wi-Fi wireless network, which analyzes network parameters using fuzzy logic elements and analysis of the results obtained.

Data availability: The manuscript has no related data in the repository.

Software availability: The manuscript has no associated software.

Use of artificial intelligence tools: The authors confirm that they did not use artificial intelligence technologies in creating the submitted work.

REFERENCES

1. Natkaniec P., Bieńkowski P. Analysis of the Mixed IEEE 802.11ax Wireless Networks in the 5 GHz Band, *Sensors,* 2023, Vol. 23, № 10, P. 4964. DOI: 10.3390/s23104964.
2. Forenbacher I., Husnjak S., Jovović I. et al. Throughput of an IEEE 802.11 Wireless Network in the Presence of Wireless Audio Transmission: A Laboratory Analysis, *Sensors,* 2021, Vol. 21, № 8, P. 2620. DOI: 10.3390/s21082620
3. Wang K., Psounis K. Efficient scheduling and resource allocation in 802.11ax multiuser transmissions, *Computer Communications,* 2020, Vol. 152, pp. 171–186. DOI: 10.1016/j.comcom.2020.01.010
4. Natkaniec M., Kras M. An Optimization of Network Performance in IEEE 802.11ax Dense Networks , *International Journal of Electronics and Telecommunications,* 2023, Vol. 69, pp. 169–176. DOI: 10.24425/ijet.2023.144347
5. Faíscas D. (In)Security in Wi-Fi networks: a systematic review, *Advanced Research on Information Systems Security*, 2022, Vol. 2, № 2, pp. 17–23. DOI: 10.56394/aris2.v2i2.18
6. Lee B. Stateless Re-Association in WPA3 Using Paired Token, *Electronics*, 2021, Vol. 10, № 2, P. 215. DOI: 10.3390/electronics10020215
7. Kumar Y. A., Kumar V. Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications, *Wireless Personal Communications,* 2023, Vol. 123, № 1, pp. 395–452. DOI: 10.1007/s11277-023-10773-x
8. Dimakis D. A., Michael K. Survey of Wireless Intrusion Detection Systems: Threats, Swarm Intelligence and Machine Learning-Based Solutions, *Wireless Networks,* 2022, Vol. 23, № 10, P. 4964. DOI: 10.1007/s11276-022-02933-3
9. Kerimkhulle S., Dildebayeva Z., Tokhmetov A. et al. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things, *Symmetry,* 2023, Vol. 15, № 10, P. 1958. DOI: 10.3390/sym15101958
10. Savva M., Ioannou I., Vassiliou V. Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks, *Mediterranean Communication and Computer Networking Conference (MedComNet), Paphos, 1–3 June 2022: proceedings.* Paphos, IEEE, 2022, pp. 54–63. DOI: 10.48550/arXiv.2205.03797
11. Ishaque M., Khatibi A., Yamin M.et al. A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system, *Sensors*, 2023, Vol. 30, P. 100933. DOI: 10.1016/j.measen.2023.100933
12. Iantorno M. S., Beladda K. Fuzzy Logic for Cybersecurity: Intrusion Detection and Privacy Preservation with Synthetic Data, *Agents and Artificial Intelligence : 17th International Conference (ICAART), Porto, 26–28 February 2025: proceedings*. Porto, SCITEPRESS, 2025, Vol. 3, pp. 376–382. DOI: 10.5220/0013137300003890
13. Antipov I., Vasylenko T. Identification of mobile devices by correlation features of their signal spectra, *Radio Electronics, Computer Science, Control,* 2024, № 4, pp. 6–12. DOI: 10.15588/1607-3274-2024-4-1
14. Antipov I., Vasilenko T. Improving the model of decision making about abnormal network state using a positioning system, *Eastern-European Journal of Enterprise Technologies,* 2019, Vol. 1, № 9 (97), pp. 6–11. DOI: 10.15587/1729-4061.2019.157001

Received 30.12.2025.
Accepted 11.02.2026.
Published 27.03.2026.

DOI 10.15588/1607-3274-2026-1-1

УДК 621.396.946

НЕЧІТКО-ЛОГІЧНИЙ АЛГОРИТМ ОЦІНЮВАННЯ РИЗИКУ У WI-FI МЕРЕЖАХ

Антіпов І. Є. – д-р техн. наук, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, м. Харків, Україна. ROR: https://ror.org/01ctj1b90. ORCID: https://orcid.org/0000-0002-9754-4412.

Василенко Т. О. – канд. техн. наук, старший викладач кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, м. Харків, Україна. ROR: https://ror.org/01ctj1b90. ORCID: https://orcid.org/0000-0003-1291-8065.

АНОТАЦІЯ

Актуальність. Зі зростанням використання безпровідних мереж Wi-Fi підвищується ризик атак, специфічних саме для них. Традиційні методи захисту які зазвичай використовують чіткі пороги, не відображають реальної невизначеності умов в яких функціонують безпровідні мережі. Через відкритість радіоканалу, нестабільність, розсіюваність та наявність шуму, перспективним напрямком є використання нечітко-логічних алгоритмів, що дозволяють враховувати неповноту та неоднозначність даних при оцінюванні ризиків безпровідних мереж Wi-Fi.

Мета. Розробити нечітко-логічний алгоритм оцінювання стану Wi-Fi мереж, який дозволяє адаптивно визначати рівень ризику, аналізуючи параметри безпровідної мережі та приймати рішення щодо дій системи безпеки.

Метод. Запропоновано нечітко-логічний алгоритм аналізу стану функціонування безпровідної Wi-Fi мережі, що базується на комплексному аналізі шести мережевих параметрів із використанням елементів нечіткої логіки. Алгоритм включає побудову функцій належності для вхідних змінних, формування бази нечітких правил типу IF–THEN та механізм дефазифікації, що забезпечує отримання безперервної числової оцінки рівня ризику мережі. Для оцінювання ефективності запропонованого підходу проведено порівняльне імітаційне моделювання з класичним пороговим методом прийняття рішень. Дослідження виконано у середовищах MathCAD та MATLAB для взаємної перевірки працездатності алгоритму. Розглянуто три сценарії функціонування мережі, для кожного з яких змодельовано 100 станів мережі.

Результати. Результати імітаційного моделювання збігаються з точністю до третього знаку в двох програмних середовищах MathCAD та MATLAB. Запропонований алгоритм коректно реагує на збільшення кількості невдалих спроб автентифікації та на аномальні зміни трафіку. Використання елементів нечіткої логіки дозволяє уникнути різких стрибків між рівнями ризику «низький», «середній», «високий», що зменшує кількість хибних тривог та мінімізує помилки першого роду. Модель успішно розрізняє нормальні зміни рівня сигналу та небезпечні. Запропонований алгоритм здатен сам реагувати на потенційні загрози: моніторинг, посилене логування, обмеження доступу, блокування клієнта та сповіщати адміністратору.

Висновки. Запропонований у роботі нечітко-логічний алгоритм аналізу стану Wi-Fi мережі на основі нечіткої логіки дає змогу більш адекватно ухвалювати рішення щодо стану мережі. Використання нечіткої логіки дозволяє коригувати рішення залежно від зміни умов функціонування мережі у режимі реального часу та може бути інтегрована у системи виявлення вторгнень або розширені засоби кіберзахисту безпровідних мереж.

КЛЮЧОВІ СЛОВА: кібербезпека, Wi-Fi, системи виявлення вторгнень, нечітка логіка, оцінка ризику.

ЛІТЕРАТУРА

1. Natkaniec P. Analysis of the Mixed IEEE 802.11ax Wireless Networks in the 5 GHz Band / P. Natkaniec, P. Bieńkowski // Sensors. – 2023. – Vol. 23, № 10. – P. 4964. DOI: 10.3390/s23104964.
2. Throughput of an IEEE 802.11 Wireless Network in the Presence of Wireless Audio Transmission: A Laboratory Analysis / [I. Forenbacher, S. Husnjak, I. Jovović et al.] // Sensors. – 2021. – Vol. 21, № 8. – P. 2620. DOI: 10.3390/s21082620
3. Wang K. Efficient scheduling and resource allocation in 802.11ax multi-user transmissions / K. Wang, K. Psounis // Computer Communications. – 2020. – Vol. 152. – P. 171–186. DOI: 10.1016/j.comcom.2020.01.010
4. Natkaniec M. An Optimization of Network Performance in IEEE 802.11ax Dense Networks / M. Natkaniec, M. Kras // International Journal of Electronics and Telecommunications. – 2023. – Vol. 69. – P. 169–176. DOI: 10.24425/ijet.2023.144347
5. Faíscas D. (In)Security in Wi-Fi networks: a systematic review / D. Faíscas // Advanced Research on Information Systems Security. – 2022. – Vol. 2, № 2. – P. 17–23. DOI: 10.56394/aris2.v2i2.18
6. Lee B. Stateless Re-Association in WPA3 Using Paired Token / B. Lee // Electronics. – 2021. – Vol. 10, № 2. – P. 215. DOI: 10.3390/electronics10020215
7. Kumar Y. A. Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications / Y. Kumar, V. Kumar // Wireless Personal Communications. – 2023. – Vol. 123, № 1. – P. 395–452. DOI: 10.1007/s11277-023-10773-x
8. Dimakis D. A. Survey of Wireless Intrusion Detection Systems: Threats, Swarm Intelligence and Machine Learning-Based Solutions / D. Dimakis, K. Michael // Wireless Networks. – 2022. – Vol. 23, № 10. – P. 4964. DOI: 10.1007/s11276-022-02933-3
9. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things / [S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov et al.] // Symmetry. – 2023. – Vol. 15, № 10. – P. 1958. DOI: 10.3390/sym15101958
10. Savva M. Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks / M. Savva, I. Ioannou, V. Vassiliou // Mediterranean Communication and Computer Networking Conference (MedComNet), Paphos, 1–3 June 2022: proceedings. – Paphos: IEEE, 2022. – P. 54–63. DOI: 10.48550/arXiv.2205.03797
11. A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system / [M. Ishaque, A. Khatibi, M. Yamin et al.] // Sensors. – 2023. – Vol. 30. – P. 100933. DOI: 10.1016/j.measen.2023.100933
12. Fuzzy Logic for Cybersecurity: Intrusion Detection and Privacy Preservation with Synthetic Data / [M. S. Iantorno, K. Beladda] // Agents and Artificial Intelligence : 17th International Conference (ICAART), Porto, 26–28 February 2025: proceedings. – Porto: SCITEPRESS, 2025. – Vol. 3. – P. 376–382. DOI: 10.5220/0013137300003890
13. Antipov I. Identification of mobile devices by correlation features of their signal spectra / I. Antipov, T. Vasylenko // Radio Electronics, Computer Science, Control. – 2024. – № 4. – P. 6–12. DOI: 10.15588/1607-3274-2024-4-1
14. Antipov I. Improving the model of decision making about abnormal network state using a positioning system / I. Antipov, T. Vasilenko // Eastern-European Journal of Enterprise Technologies. – 2019. – Vol. 1, № 9 (97). – P. 6–11. DOI: 10.15587/1729-4061.2019.157001

DOI 10.15588/1607-3274-2026-1-1