Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements

Volodymyr Sokolov[1,*,†], Yuliia Kostiuk[1,†], Pavlo Skladannyi[1,†] and Nataliia Korshun[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine*

Abstract

The paper examines the challenges of ensuring information security in the context of growing traffic volumes and the complexity of topologies of distributed information and communication systems. The necessity of adapting the routing policy to the current cybersecurity requirements, considering the risks of targeted attacks and anomalous activity, is substantiated. The limitations of traditional technical security tools that are ineffective in a dynamic digital environment are analyzed A formalized approach to building an adaptive routing policy that integrates mathematical modeling, risk-based metrics, ISO/IEC 27033, 15408, and NIST SP 800-207 standards, as well as software-defined networking technologies and telemetry protocols (NetFlow, sFlow) is proposed. The architecture of an automated routing system that can adapt to real-time changes in the threat environment has been developed. The system provides context-dependent control of data flows, increases the level of cyber resilience of the network, and implements the principles of the Zero Trust Architecture (ZTA). The results obtained can be used to protect critical information systems in both the corporate and public sectors.

Keywords

adaptive routing, information security, network traffic, routing policy, risk-based methods, mathematical modeling, network resilience, automated security systems, Zero Trust Architecture, network telemetry

1. Introduction

In today's digital transformation environment, ensuring information security at the network level is critical to the reliability of enterprises and government information systems. The growing complexity of network topologies, threat dynamics, and scaling of digital services makes traditional routing and filtering methods ineffective. Most classical approaches do not consider the context of interaction, changes in the threat landscape, and the need for dynamic incident response. Modern information security standards (ISO/IEC 15408, 27033, NIST SP 800-207) emphasize the importance of proactive traffic management and context-sensitive access control in a constantly changing environment. Adapting network traffic routing policies to information security requirements using risk-based metrics, behavioral indicators, and automated solutions becomes particularly relevant. This study aims to substantiate the theoretical and applied foundations for building an adaptive traffic routing policy that provides dynamic flow control, considering the level of threats, criticality of resources, and network characteristics. A formalized mathematical model is proposed to achieve this goal, and algorithms and architecture of an automated system that implements the principles of ZTA and digital resilience in real-time are developed.

[1]*ICST-2025: Information Control Systems & Technologies, September 24–26, 2025, Odesa, Ukraine*

* Corresponding author.

† These authors contributed equally.

v.sokolov@kubg.edu.ua (V. Sokolov); y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladannyi); n.korshun@kubg.edu.ua (N. Korshun)

0000-0002-9349-7946 (V. Sokolov); 0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0003-2908-970X (N. Korshun)

2. Source review

Adapting network traffic routing to information security requirements is a key task in protecting information systems, driven by complex architectures, growing threats, and the need for proactive network-level security. Modern approaches combine classical routing with dynamic traffic management, machine learning, and risk-based methods.

Studies by Sert and Yazici [1] and Touati [2] show that fuzzy logic and genetic algorithms enable dynamic routing adaptation, efficient load balancing, and improved resilience under uncertainty—critical for secure communication channels. Al-Karaki and Kamal [3] provide a foundational review of routing methods, while ISO/IEC 27033 and NIST SP 800-207 [4, 5] highlight the role of context- and trust-based dynamic access control. Overall, adaptive routing enhances attack resilience, reduces data leakage risks, and supports proactive cyber defense in modern communication systems.

3. Research methods

The work is based on formal methods of set theory, combinatorial analysis, and mathematical optimization, which are applied to the problems of modeling communication structures in networks in the context of information security. These methods allow for formalizing the set of possible data transmission routes, modeling the relationships between nodes and communication channels about security constraints, and finding optimal solutions by specified criteria. Particular attention is paid to constructing mathematical models that provide dynamic adaptation of traffic routes, considering changes in the topology structure, interaction context, and risk level. This approach contributes to the formation of attack-resistant routing policies in complex information systems.

4. Theoretical basis

The study examines modern approaches to building secure information networks, emphasizing adapting network traffic routing policies to meet information security requirements. Due to the increasing complexity of network topologies, the dynamics of digital services, and the scaling of cyber threats, traditional perimeter-oriented security tools are proving ineffective. The basic logic of classic firewalls, static access control lists, and traffic filtering cannot provide timely detection and blocking of attacks that exploit system vulnerabilities or configuration errors [1, 2, 4, 6, 7]. That is why there is a need to implement intelligent traffic management based on risk-based criteria. Risk-based criteria should be understood as indicators that consider the likelihood of threats, the level of potential damage to information resources, and the criticality of the objects to which traffic is directed. This approach allows you to adapt routing and filtering rules in real-time, focusing not only on formal parameters but also on the context of the threat environment.

The author analyzes the typical stages of network attacks, including: identifying network entry points, scanning security systems, exploiting vulnerabilities, accessing internal network segments, searching for and compromising target information, and deleting digital traces [6]. This sequential chain forms a model of attacker behavior that must be considered when developing a modern routing system. At the same time, it has been established that most successful attacks are associated with insufficient network policy flexibility, low contextual filtering level, and lack of centralized control over data flows.

The paper proposes the concept of proactive network protection, which is implemented by adapting the routing policy based on current threats. A key element of this concept is the automated formation of traffic routes in such a way as to minimize access to potentially vulnerable services from the external or internal environment [8–13]. We propose an architectural solution that integrates mathematical modeling, behavioral analytics, traffic telemetry (via protocols such as NetFlow/sFlow), and standardized security requirements by ISO/IEC 27033, 15408, and NIST SP

800-207 [4, 5]. Figure 1 shows an activity diagram that illustrates the stages of operation of a dynamic network traffic routing control system, considering the risks and current state of network security. To implement the proposed approach, a mathematical routing model has been developed that considers the set of valid routes, risk weights, trust in traffic sources and destinations, and the criticality of information resources [3]. The built model allows for automated decision-making regarding changing the route in real-time depending on changes in the security context [14]. Thus, the network becomes an adaptive environment that can independently respond to threats, localize potentially dangerous connections, and prevent intrusions even before their active phase [15]. Figure 2 shows the sequence of interaction between the main components of the adaptive traffic routing system, including the telemetry module, risk assessor, policy manager, and router, which provide dynamic traffic redirection based on the current level of threats.

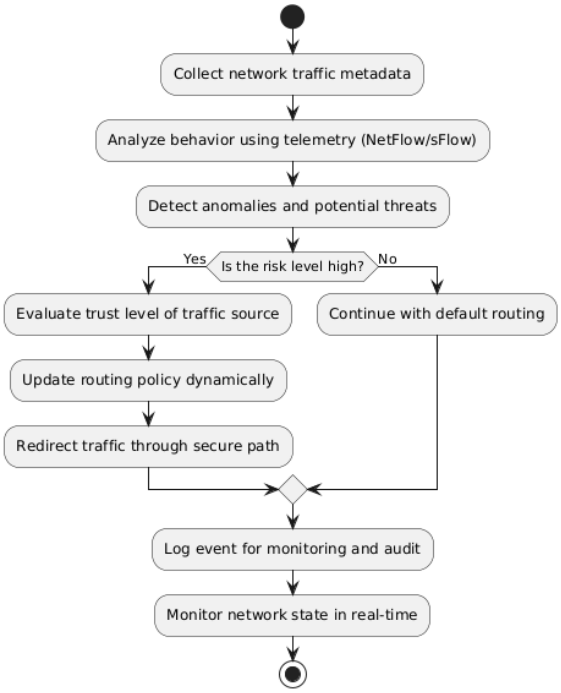

Figure 1: Diagram of adaptive traffic routing activity.

As part of the development of an adaptive traffic routing policy by information security requirements, a formalized approach is proposed that takes into account both the network topology and security priorities based on modern international standards, in particular ISO/IEC 15408 (common criteria), 27033, and NIST SP 800-207 [4, 7]. This approach allows for the dynamic redirection of network traffic based on the risks, vulnerabilities of communication channels, the level of trust, and the criticality of information resources [6].

The model is based on key parameter sets. The set of access channels to information resources that are potentially vulnerable to security is denoted as $S = (S_1, S_2, ..., S_p)$. Network nodes through which traffic is transmitted to protected objects are represented by the set $N = (n_1, n_2, ..., n_k)$. For each channel S_i, a security factor $X = (X_1, X_2, ..., X_p)$ is determined, which is a discrete normalized value (for example, on a scale from 1 to 10) and reflects the current level of security determined based on behavioral analysis, identified vulnerabilities, and the presence of active threats [16]. The model also takes into account the set of current threats $M = (M_1, M_2, ..., M_p)$, potentially implemented through the appropriate channels, and the set $NP = (NP_1, NP_2, ..., NP_k)$, which contains routing priorities formed based on non-functional characteristics of routes (e.g., delay, throughput, or topological proximity), without taking into account security factors [9, 10, 17]. The constraints in the form of the maximum allowable risk level are set through the set $K = (K_1, K_2, ..., K_r)$, which includes all the essential network security requirements classified according to ISO/IEC 15408.

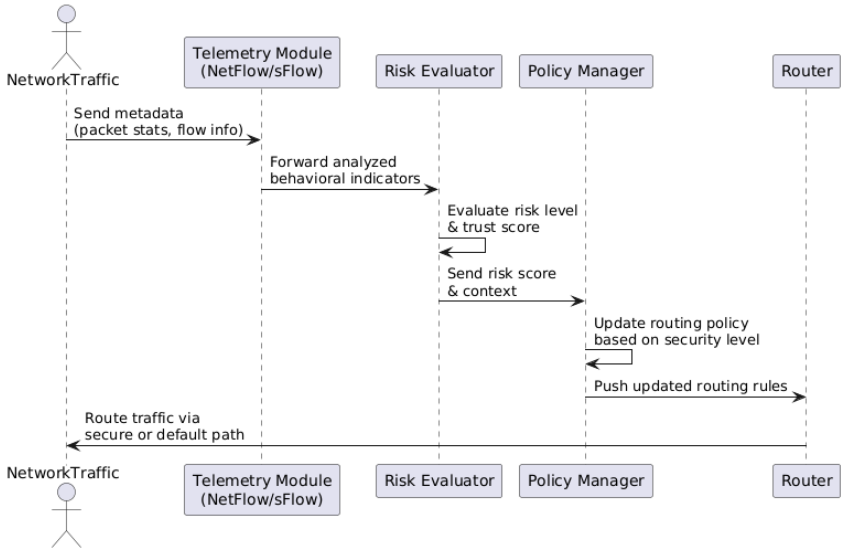

Figure 2: Sequence diagram of interaction between components of the adaptive routing system.

For each channel S_i, a matrix of security requirements is constructed, in which information resources R_k, are placed in the columns, and requirements are placed in the rows K_j. The element of the matrix W_{ijk} represents the weight of the importance of a particular requirement K_j to the resource R_k, available through the channel S_i and is set by an expert on a scale from 0 to 10. The integral security factor of each channel S_i is calculated by the formula:

$$X_i = \sum_{j=1}^{r} \sum_{k=1}^{m} W_{ijk}, \tag{1}$$

where X_i is the total security assessment of the channel, W_{ijk} is the weight of the security requirement K_j to the resource R_k, r is the number of security requirements, m is the number of information resources served by the channel S_i. To include a channel in the list of acceptable routes, the condition $X_i \geq L_i$, $\forall i \in [1,p]$, must be met, i.e., the actual security of the channel must be at least as high as the established threshold level [3, 8].

The final routing priority is formed using a combined metric:

$$P_i = \alpha \cdot NP_i + \beta \cdot X_i, \tag{2}$$

where P_i is the integral priority of the route through the channel S_i, NP_i is the initial (technical) priority of the route, X_i is the safety factor, $\alpha, \beta \in [0,1]$ is the weighting factor that determines which component is dominant. For example, $\alpha = 0.4$ and $\beta = 0.6$ if safety is given preference.

Figure 3 shows a data flow diagram that reflects the sequence of information processing in the adaptive traffic routing system. The key input data is traffic telemetry, information about threats and security requirements, as well as the stages of calculating channel security coefficients X_i, checking their compliance with the boundary values L_i and forming the integrated route priority P_i are presented [18, 19]. Traffic telemetry means a set of automatically collected real-time network flow parameters, including volume, delay, packet transmission frequency, protocol types, and anomaly frequency. These are used to analyze the network status and decide its protection. As a result, the system selects the most secure routing channel.

The proposed model generates an adaptive routing policy that dynamically considers the risk context, traffic characteristics, and security constraints [4, 5]. Unlike static schemes, the approach increases resistance to attacks, isolates vulnerable channels, and routes traffic through the most secure routes, focusing on the topology and the current security state, which aligns with the principles of ZTA [7] and cyber resilience. The formalized model considers the network topology, criticality of nodes, security thresholds, and routing priorities [1, 5], based on the oriented structure of links and the calculation of security factors for each channel.

The limit value of the safety factor L_i for each channel C_i is determined as the sum of the values of the elements of the constraint matrix formed based on the requirements of ISO/IEC 15408 standards and expert risk assessment [12]:

$$L_i = \sum_{j=1}^{r} \sum_{k=1}^{m} W_{ijk}^{\max}, \tag{3}$$

where $W_{ijk}^{\max}$ is the maximum criticality weight of the requirement K_j for the resource R_k through the channel C_i, r is the number of security requirements, m is the number of information resources the channel serves.

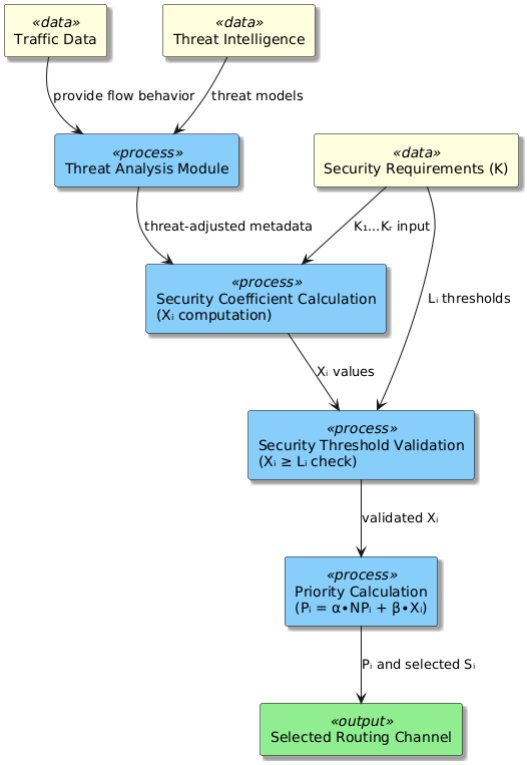

Figure 3: Data flow diagram of data processing in the adaptive traffic routing system.

The set of routing priorities for nodes $NP = (NP_1, NP_2, ..., NP_k)$ is formed based on expert evaluation and considers delays, throughput, reliability, and topological proximity to critical resources. Each $n_i \in N$ node is assigned a routing priority $NP(n_i)$, which reflects its importance in the overall network structure. This priority is determined independently of information security requirements and is formed based on a matrix of node relationships.

To model the real network structure, we use the oriented link model $G = (N, D)$, where N is a set of nodes, and $D \subseteq N \times N$ is a set of ordered links between them. The ordering of $d = (n_i, n_j)$ pair is determined according to priorities: the node with the highest $NP(n_i)$ value is considered as the source of the communication direction. Thus, a directed routing structure is created, in which nodes correspond to routers, directed connections to communication channels, and priorities define the topological route in the network. If there are no start or end points in such a structure (nodes without incoming or outgoing connections), artificial elements, a conditional source S, and a conditional receiver T are introduced, which are connected to the corresponding nodes via auxiliary channels. As a result, a specialized directed network structure is formed, which serves as a modeling environment for routing analysis.

The next step is to calculate the maximum safe flow using the modified Ford-Fulkerson algorithm, a classical method of flow theory in networks used to find the maximum possible flow from source to sink in a directed network with finite bandwidth. The sink is the final destination

node to which the information flow from the source arrives. The idea of the algorithm is to gradually increase the flow along the so-called permissible (unexhausted) paths in the network until the limit is reached, beyond which further increase becomes impossible. In the context of information security, the algorithm is modified to take into account channel security constraints: the optimal flows $f = (x, y)$ for each connection $(x, y) \in D$ are interpreted as security coefficients of the corresponding communication channels, which allows us to estimate the probability of their safe use in the routing process:

$$X_i = (x, y), C_i \leftrightarrow (x, y), \tag{4}$$

where X_i values must satisfy the conditions $X_i \le L_i$, $\forall i \in [1, ..., p]$, i.e., not exceed the security limits set for each channel.

The optimization function determines the best secure routing configuration according to maximizing the security coefficients on all channels. Let $O(n)$ denote the set of all channels leading to the node n. Then the channel with the maximum security factor is selected for each node:

$$C_n^* = \arg \min_{C_i \in O(n)} X_i, \tag{5}$$

where C_n^* is the channel with the highest security to access the node n.

If the risk profile changes (e.g., an increase in attacks or new vulnerabilities), the system recalculates X_i and P_i, adapting routes in real-time:

$$X_i(t) = f\,(ThreatLevel_i(t), Anomalies_i(t), Vulnerabilities_i(t)). \tag{6}$$

This allows us to dynamically adapt routing to the context of threats, which is the basis of ZTA and the principles of digital resilience. Therefore, the risk deficit formula looks like this:

$$X_i = \max\left\{0, \frac{L_i - X_i}{L_i}\right\}. \tag{7}$$

The above formula determines the relative security deficit for the channel S_i. If X_i (the actual security level) is less than L_i (the threshold level), then R_i reflects the degree of failure to reach this threshold, which can be used to adjust the routing parameters further.

Normalization of safety requirements weights [12]:

$$\widetilde{W_{ijk}} = \frac{W_{ijk}}{\max\{W_{ijk} \mid \forall i, j, k\}}, \tag{8}$$

where the above expression normalizes the weight values of W_{ijk} to the interval [0,1], which allows comparing them regardless of the initial scale, which simplifies further calculations of the integral security factor X_i.

Updating the weights of security requirements using the exponential smoothing method:

$$W_{ijk}(t + 1) = \gamma \cdot W_{ijk}(t) + (1 - \gamma) \cdot \Delta W_{ijk}(t), \tag{9}$$

where $\gamma \in [0,1]$ is the smoothing factor, $\Delta W_{ijk}(t)$ is a new expert assessment or weight adjustment at the current stage, which allows the weight values to be adapted to changes in the threat environment over time. Dynamic adjustment of the integrated route priority:

$$P_i(t) = \alpha \cdot NP_i + \beta \cdot X_i(t) - \delta \cdot R_i(t). \tag{10}$$

The formula is a variant of the previously discussed expression for P_i, which additionally takes into account the penalty $\delta \cdot R_i(t)$, which is subtracted from the overall priority. The parameter δ determines the degree of influence of the risk deficit $R_i(t)$ on the final route priority, which allows for a more accurate consideration of high-risk situations.

Integral metric with adaptive weights:

$$P_i = \alpha(t) \cdot NP_i + \beta(t) \cdot X_i, \tag{11}$$

where $\alpha(t)$ and $\beta(t)$ are weighting factors that change over time depending on the situation (for example, when attacks increase $\beta(t) \uparrow$ and $\alpha(t) \downarrow$).

To avoid overloading, the Ld_i load factor of each channel is taken into account:

$$Ld_i = \frac{T_i^{used}}{T_i^{max}}, \tag{12}$$

where T_i^{used} is the amount of traffic that is already passing through the channel, T_i^{max} is the maximum allowable load on the channel. Using this coefficient allows you to exclude congested routes from consideration, regardless of their security.

Calculating the maximum bandwidth (maximum flow) of protected channels:

$$F_{max} = \sum_{(S,u) \in D} f(S,u). \quad (13)$$

The above expression is used to estimate the maximum throughput of a network (for example, in a simulated network), where $f(S, u)$ denotes the flow along the arcs (S, u) coming from the source S. The calculation of F_{max} helps determine how efficiently the network can handle traffic in the context of security. Route sustainability metric:

$$Resilience(Route) = \min_{C_i \in Route} \frac{X_i}{L_i}. \quad (14)$$

This metric defines route resilience as the ratio of the actual security level X_i to the threshold value L_i for the weakest link in the route. Values close to 1 indicate a high level of security, while lower values indicate potential vulnerabilities. The formula helps to identify a "weak spot" in the network path and apply measures to improve security. As a result, priority routing through the most secure channels is implemented, which minimizes the overload of vulnerable routes, ensures a balance between performance and security, and compliance with information security policies even in a distributed or hybrid environment [2, 3, 13, 18]. The built model supports context-sensitive routing, considering Quality of Service (QoS), predicted risks, threat structure, and resource criticality, ensuring the implementation of ZTA in the face of dynamic network activity [7]. In distributed networks, each node may have several alternative routes (access channels) to transmit traffic to protected information resources. To increase the efficiency of security-aware routing, these channels must be prioritized to reflect their integrated security. The security factors X_i are converted into route priorities by the principle: the higher the X_i, the higher the priority of the channel C_i for choosing a secure route [20]. Let us denote $PR = (PR_1, PR_2, ..., PR_n)$ the set of access channel priorities, X^0 the ordered (in ascending order) set of security coefficients

$$X^0 = \left(X_1^0, X_2^0, \ldots, X_n^0\right), \text{ where } X_1^0 \le X_2^0 \le \cdots \le X_n^0. \quad (15)$$

Each channel C_i with a security factor value of X_i is assigned a position in the ordered set X^0, which corresponds to its relative security among other channels. This lets you formalize the priority route selection, guaranteeing traffic is routed through the most secure network segments. Then the priority of the channel C_i, designated as PR_i, is determined by its X_i index in the ordered set X^0:

$$PR_i = \text{index}(X_i, X^0). \quad (16)$$

Thus, each channel receives an ordinal priority, according to which a route selection strategy is formed first of all, channels with the highest level of security are selected. The formula determines the rank (position) of the security factor X_i in the ordered list X^0, which reflects the relative security of the channel among others. As a result, each channel is assigned a unique priority, which allows the routing system to select the most secure paths for traffic transmission automatically.

For further processing and comparison of priorities in different nodes or contexts, it is crucial to ensure that priority values are normalized:

$$\widetilde{PR_i} = \frac{PR_i}{\max(PR)}, \forall i \in [1, n], \quad (17)$$

where $\widetilde{PR_i}$ is the normalized value of the channel priority C_i, $\max(PR)$ is the maximum value in the priority set. The formula ensures that the priorities are normalized to a unified scale in the range [0,1], which allows for a fair comparison of channels from different nodes. Normalization is essential for context-dependent analysis and decision-making in distributed networks with dynamically changing conditions. For the node n_j, the optimal channel C_j^* is selected as the one with the maximum normalized priority:

$$C_j^* = \arg \max_{C_i \in O(n_j)} \widetilde{PR_i}, \tag{18}$$

where $O(n_j)$ is the set of access channels to the node n_j. The formula allows you to choose the best route to the node, taking into account the normalized channel priorities. The channel with the highest priority guarantees an optimal balance between security and QoS, which is critical for adaptive routing in a changing threat environment.

The security of a route to a particular node can be assessed through an integral metric based on the average value of security factors across all channels in the route:

$$X_{\text{avg}}^{(j)} = \frac{1}{|O(n_j)|} \sum_{C_i \in O(n_j)} X_i, \tag{19}$$

where C_j^* is the average security factor of the route to the node n_j, $|O(n_j)|$ is the number of access channels to the node. This metric allows you to quantify a route's overall level of security to a particular node based on the average security factor of the channels leading to it. A higher average indicates a more reliable and secure route, which is an important criterion when choosing the direction of traffic in critical network segments. Taking into account the risk deficit R_i, which has already been described, the updated priority value can be adjusted using the following formula:

$$PR_i^{(t+1)} = \widetilde{PR_i} - \delta \cdot R_i, \tag{20}$$

where $\delta \in [0,1]$ is the parameter of risk influence on the final priority, the formula allows you to dynamically reduce the priority of routes with a high level of risk by adjusting their weight in the decision-making process. Thus, more risky channels automatically lose their preference when choosing routes, increasing the network infrastructure's overall security.

The risk factor for a channel can be formalized as:

$$R_i = \begin{cases} \dfrac{L_i - X_i}{L_i}, & \text{if } X_i < L_i, \\ 0, & \text{if } X_i \geq L_i. \end{cases} \tag{21}$$

This formula determines the degree of discrepancy between the actual security level of the channel X_i and its regulatory threshold L_i. If the level of security is less than the threshold, the coefficient R_i will be greater than zero, indicating a potential risk of using this channel. If the requirements of $X_i \geq L_i$ are met, the risk is considered absent. This indicator automatically de-prioritizes routes that do not meet security standards and can be integrated into dynamic routing policy adaptation.

Evaluation of route efficiency taking into account the criticality of the resource:

$$Eff_i = \frac{X_i \cdot CR_i}{Ld_i + 1}. \tag{22}$$

This metric allows you to quantify the effectiveness of the route in terms of information security and performance. $X_i \in [0,1]$ is the channel security level C_i, $CR_i \in [0,1]$ is the criticality of the resource served through the channel (determined by experts or based on data categories), Ld_i is the current load on the channel (in terms of traffic). The formula considers that high security and resource criticality increase route efficiency, while congestion reduces it. This gives automatic priority to less congested but secure channels, leading to essential information objects.

Route sensitivity index to attacks:

$$SI_i = \frac{Vuln_i \cdot (1 - X_i)}{P_i}. \tag{23}$$

This metric determines the relative susceptibility of a C_i channel to attacks based on three key parameters $Vuln_i \in [0,1]$ is the degree of vulnerability of the channel (determined based on known common vulnerabilities, exposures, etc.), X_i is the level of security (the lower the level of security, the greater the risk), P_i is the priority of the route in the system (the higher the priority, the more critical the channel). The formula shows that a channel with high vulnerability, low security, and

high priority is the most dangerous, as the likelihood of compromise is higher and the consequences are more significant. This index allows you to identify critical routing nodes that should be heavily protected or restricted. The metric of adaptive route weight depends on the risk:

$$W_i^{adapt} = \gamma \cdot X_i + (1-\gamma) \cdot (1-R_i). \quad (24)$$

The metric combines the level of channel security X_i and the inverse of risk R_i, which characterizes the current threat environment. The $\gamma \in [0,1]$ parameter regulates the balance between channel trust X_i and contextual risk assessment $(1 - R_i)$. The lower the risk R_i, the greater the share of security in the metric value, which allows you to dynamically change the route's weight by the network's current security situation. The likelihood of privacy violations on the route:

$$P_{conf}(i) = 1 - \frac{X_i}{L_i}. \quad (25)$$

The formula allows us to estimate the probability of privacy compromise on channel C_i by comparing the actual level of its security X_i with the regulatory threshold L_i. If $X_i < L_i$, then the value of $P_{conf}(i)$ increases, indicating an increased risk of information leakage. Thus, the formula allows you to identify critical channels where the current protection does not meet the established requirements and requires additional security enhancements. Confidence factor in the route:

$$Trust_i = \frac{X_i \cdot NP_i}{\sum_{j=1}^{n} X_j \cdot NP_j}. \quad (26)$$

The expression defines the relative confidence in the route i, which is calculated as the quotient between the product of the security level X_i and the initial (technical) priority NP_i to the total sum of the corresponding products for all routes. In other words, $Trust_i$ shows how reliable the route i is compared to other alternatives, taking into account not only its security but also its importance in terms of network topology. This coefficient can be used to rank routes or make decisions in routing systems that prioritize security and efficiency. A metric of dynamic traffic redistribution:

$$T_{new}^{(i)} = T_{curr}^{(i)} \cdot \left(1 - \frac{R_i}{\max(R)}\right). \quad (27)$$

This formula describes the change (decrease) in the volume of traffic passing through channel i depending on the risk R_i associated with it. Here, $T_{curr}^{(i)}$ is the current load on the channel, R_i is the risk index for this route (takes into account vulnerabilities, anomalies, and attack activity), and max(R) is the highest risk index among all channels used for normalization. If R_i is low (the channel is safe), then the $1 - \frac{R_i}{\max(R)}$ multiplier is close to 1, meaning that the traffic does not change. If R_i is high, the multiplier decreases, and less traffic is transmitted through the channel [6, 15, 19]. Thus, the formula implements a dynamic mechanism for redistributing traffic: the higher the risk, the less busy the channel becomes. This ensures a balance between system performance and information security. The risk of data leakage along the route:

$$Leak_i = \frac{1}{X_i \cdot QoS_i}. \quad (28)$$

The formula indicates that weak security and poor QoS increase the threat. Lower values of X_i (security factor) and QoS_i lead to a higher risk of data breaches. Such a metric can be used by security to rank routes when processing critical information flows.

Penalty function for violating the threshold:

$$Penalty_i = \begin{cases} 0, & \text{if } X_i \geq L_i \\ \lambda \cdot (L_i - X_i), & \text{if } X_i < L_i \end{cases}. \quad (29)$$

The formula determines the fine amount for non-compliance with the standard level of channel security. If the actual level of security X_i is sufficient (not lower than the threshold value L_i), no fine is charged. If the level of protection is lower than the regulatory threshold, the fine is calculated in proportion to the security deficit, taking into account the sensitivity factor λ. This allows you to quantify the degree of security breach and use this value to optimize the route policy.

A general metric of system security [16]:

$$S_{\text{total}} = \sum_{i=1}^{n} X_i \cdot \omega_i. \tag{30}$$

The formula determines the overall network security rating based on individual protections and channel weights (importance, load, etc.). The value X_i represents the security level of an individual channel, and the coefficient ω_i represents its weight in the overall system structure. Thus, the more important and better protected a channel is, the more it affects the overall security level of the network. The proposed formulas make it possible to form an adaptive, risk-based routing policy that takes into account the balance between performance, threats, and trust and is based on cybersecurity standards. Such a model operates on topological characteristics and the dynamic security context vulnerabilities, risk metrics, and resource criticality [6, 16, 20]. This ensures traffic redirection through the most secure channels, isolation of vulnerable areas, and proactive response to threats, which is the basis for implementing ZTA and digital resilience policies.

To support adaptive routing policy, security profiling based on the ISO/IEC 15408 standard is used [4, 5]. The so-called network security packages are formed, reflecting the current requirements for protecting channels in a distributed network. For each node of the system, a set of critical information objects $I = \{I_1, I_2, ..., I_n\}$, is considered to be where access is provided. For each of them, the current security requirements $K = \{K_1, K_2, ..., K_t\}$ are determined by ISO/IEC 15408 standards. As a result, a set of security packages $P = \{P_1, P_2, ..., P_g\}$ and a matrix of boundary values $M = \{M_1, M_2, ..., M_g\}$ for each channel is formed, and $U = \{U_1, U_2, ..., U_m\}$ is a set of network nodes (routers), $A = \{A_{U1}, A_{U2}, ..., A_{Um}\}$ is a set of connections between nodes, *SP* (Security Profile) is a general profile of information security requirements. In general, this model allows: the assessment of the level of channel security in a distributed network, forms adaptive security profiles, automates the selection of the optimal route, taking into account both performance and information security, to respond to dynamic changes in the threat environment in real-time [12]. Thus, the routing decision-making system receives a formalized logic that allows combining access policies, security criteria, and risk-based restrictions in a single structure of routed traffic management. This meets the modern requirements for building cyber-resistant information and communication systems and the ZTA policy.

5. Implementation of the method

The algorithm for generating security packets formalizes determining the current requirements for protecting information resources in the network based on traffic flow management. This approach makes it possible to create a flexible and adaptive routing policy that meets modern information security standards (in particular, ISO/IEC 15408, 27033, NIST SP 800-207) [4, 5] and takes into account both threats and criticality of resources in distributed network infrastructures. The essence of the algorithm is to select relevant security requirements for each access channel based on an analysis of potential risks and the type of resources accessed. For this purpose, a network channel security profile is formed as a package of security requirements.

Figure 4a shows a sequence of actions that includes network profile formation, asset identification and protection requirements, channel assessment, and security policy updates. This ensures flexible and adaptive routing management with information security in mind.

The scheme of forming the modeling structure is presented in Figure 4b as a flowchart showing a sequential algorithm for building the network topology for further security analysis. The process involves collecting topological information, identifying nodes and communication channels, setting

connection directions according to routing priorities, and, if necessary, adding a conditional source and receiver. After the integrity check, the structure is prepared to calculate security factors.

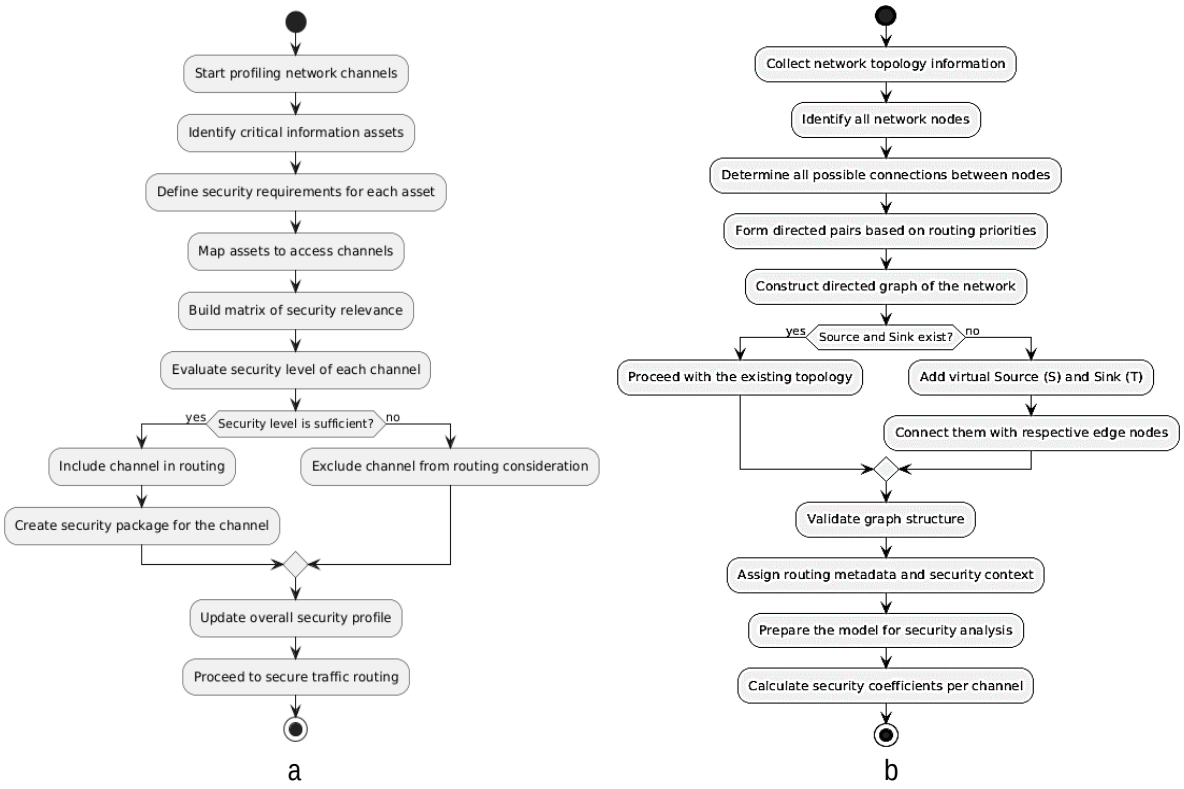

Figure 4: Block diagrams of (a) an algorithm for generating security packets in adaptive network traffic routing and (b) a modeling network for routing analysis.

The flowchart formalizes creating a functional model of the routing environment, which is the basis for building a secure, adaptive traffic management system. Such a system automatically selects optimal routes based on the level of threats, channel status, and access policies, dynamically responds to changes in the network, and maintains the integrity, confidentiality, and availability of traffic by information security requirements. Figure 5 shows a data flow diagram that reflects the logic of transforming the security factors of communication channels X_i into route priorities PR_i. The input data comes from the router as a request to the security factor database.

Next, the X_i values are sorted in descending order in the priority assignment module, after which each channel is assigned a positional priority. The resulting PR_i values are recorded in the priority database and returned to the router to decide on the selection of the safest routes. This decision is the automated comparison of available routes based on the assigned priorities, where the router selects channels with the highest security factors that meet the specified access policies, bandwidth requirements, and current network status. This ensures traffic is routed through the least risky routes, minimizing the likelihood of data being intercepted, lost, or modified. The diagram emphasizes the importance of a formalized mechanism for calculating priorities in adaptive routing systems, taking into account the level of channel security, which is especially important in ZTA.

Considering information security requirements, the adaptive routing policy for network traffic is implemented through dynamic routing protocols of the third level of the ISO/OSI open systems interaction model. Such protocols include, in particular, Open Shortest Path First, Intermediate System to Intermediate System, and Border Gateway Protocol ver. 4 (BGP v4). The main idea of the proposed approach is to use the attributes of routes (length, weight, cost) to change the direction of traffic by the level of risk and security of network channels. In this way, routing is provided not only based on the technical characteristics of the network but also taking into account the

calculated security factors, which allows for priority routing through the most secure channels. To automate this approach, we propose creating an automated system for building a traffic flow management policy that implements the whole cycle from data collection and model building to generating configuration code for routers. This system is structured in interconnected modules, each performing separate functions, providing scalability, speed, and adaptation to changes in the network environment.

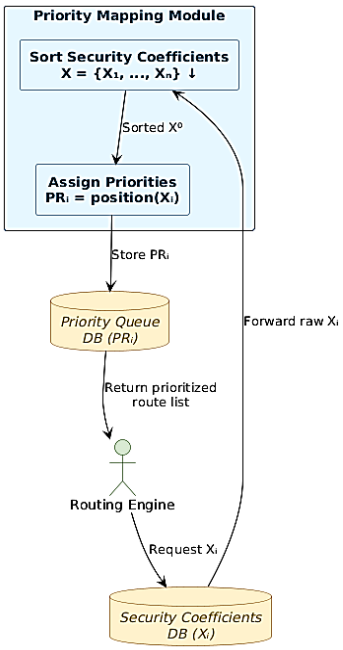

Figure 5: Converting safety factors into route priorities.

The data preprocessing module is responsible for entering and saving network parameters via a web interface. Next, the modeling structure is formed, a directed model of node and channel connections by ISO/IEC 15408, which allows you to analyze the security of routes in various scenarios. The module for calculating security factors determines the channel security level, considering the criticality of resources, security requirements, and behavioral analysis of traffic. The results are transferred to the module to generate technical specifications, which generate router settings (for example, BGP) in the appropriate format. A separate monitoring module detects changes in the state of the network, new vulnerabilities, attacks, and topology, and initiates routing policy updates without user intervention. This ensures that the system constantly adapts to the current level of threats.

The diagram (Figure 6) shows the logical structure of deploying the system's key components for adapting the routing policy to information security requirements. The system includes modules for processing user requests (web interface), calculating security coefficients (security coefficients computation), generating a routing policy, interacting with the software-defined networking controller, router configuration database, and router cluster, as well as a monitoring subsystem and integration with the security information and event management system. The model reflects the data exchange between components in the face of dynamic threat changes, allowing for context-sensitive, flexible, and cyber-resilient traffic routing [4, 5].

To ensure the cyber resilience of an information system, it is critical to minimize its response time to changes in the network environment. This parameter should be less than the period of route information update, which reduces the likelihood of network compromise due to a delayed response. The response time can be evaluated using standard diagnostic utilities (*ping*, *time*) by analyzing the moment the response appears after a new route is added to the routing table.

A command script is used to initiate the calculation of channel security coefficients and generate technical specifications to evaluate the routing policy's effectiveness. The time of

propagation of changes is recorded using the command interface of the equipment (in particular, Cisco or Juniper), which provides control over the updating of routing parameters.

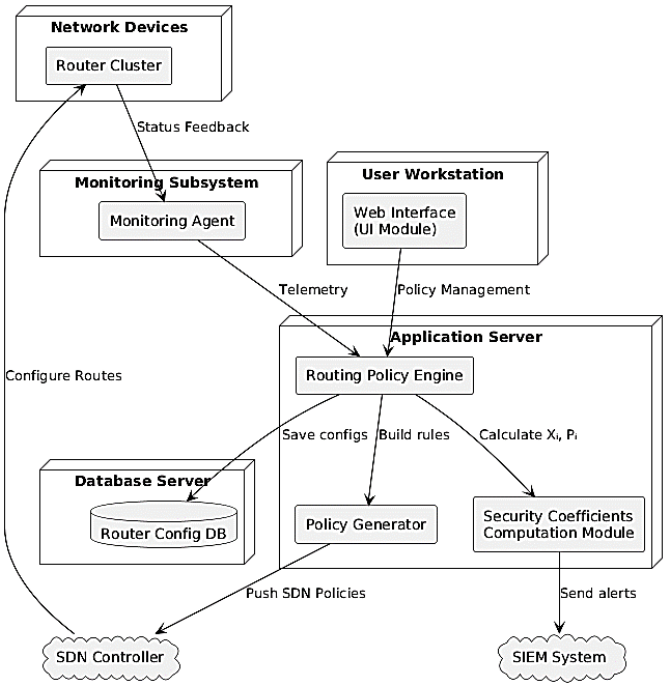

Figure 6: Deployment diagram of the adaptive network of the traffic routing system.

The possibility of parallel execution of individual system modules is checked using system process monitoring utilities, making it possible to evaluate the solution's performance under scalability and high load conditions. The proposed system is tested in a simulation environment built based on Cisco 7500 and Juniper M20 routers using the BGP v4 protocol. It is advisable to use Sun Microsystems Enterprise 220R as a server platform with the Sun Solaris 8 operating system. The test results confirm the possibility of effective operation of the system in real-time and demonstrate its adaptability to changes in the threat environment.

Figure 7 shows a deployment diagram that models the physical environment of the adaptive traffic routing system with respect to information security requirements.

The system is implemented on a Sun Microsystems Enterprise 220R server running Sun Solaris 8, where the main software modules calculate security factors and generate routing policies. The deployed policies are transferred to Cisco 7500 and Juniper M20 routers, which implement traffic management via BGP v4. A separate monitoring module measures system response time and controls parallel execution of processes, improving the solution's performance and scalability in a dynamic threat environment.

The test results obtained during simulation and pilot deployment demonstrate that the system ensures stable real-time operation and promptly adapts to changes in the threat environment. During testing, the system consistently maintained secure and efficient routing, automatically reconfiguring traffic flows when the risk profile or network topology changed. The architecture's modular design allowed it to respond predictably to dynamic security conditions without noticeable degradation in network service quality. The proposed architecture integrates formalized mathematical modeling, risk-based prioritization, and standards compliance, ensuring a balanced combination of security and performance in diverse network conditions. To summarize, the system allows you to form an adaptive routing policy based on the current level of risk, the degree of criticality of information resources, and security priorities. The built architecture fully complies with the requirements of modern international standards such as ISO/IEC 15408, 27033, and NIST SP 800-207. It supports the key principles of ZTA, ensuring a high level of security and cyber resilience of distributed information systems.

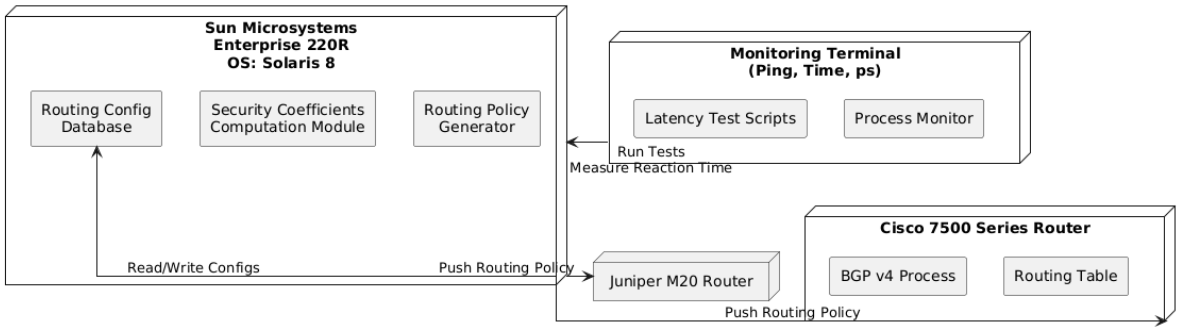

Figure 7: Deployment diagram of the physical environment of the traffic routing system.

Conclusions

The study proposes a formalized model for adapting network traffic routing to information security requirements, integrating risk-based metrics, trust parameters, behavioral characteristics, and standards (ISO/IEC 15408, 27033; NIST SP 800-207). Mathematical models account for technical parameters, threats, resource criticality, and risk dynamics, enabling automatic updates of routing priorities based on security factors. New metrics (risk deficit, route stability, attack sensitivity, integral efficiency) and a modified Ford–Fulkerson algorithm support secure flow construction. The adaptive routing system combines topology, risk-oriented metrics, behavioral parameters, and contextual constraints, forming routing priorities by access channel security level. It integrates telemetry, risk assessment, traffic analytics, and dynamic routing protocols, enhancing resilience against real-time threats, isolating vulnerabilities, and supporting Zero Trust Architecture. Applicable in critical state and corporate systems, the approach unites proactive cybersecurity, flexible traffic management, and standardized security models into an integrated next-generation routing solution that meets international protection standards and minimizes data leakage or modification risks. Future research could integrate quantum networking to enhance the adaptive routing system's predictive capabilities, quantum-resistant security, and edge compatibility. Additionally, scalability for large-scale networks, cross-domain interoperability, advanced persistent threats resilience, and real-world validation could ensure broader applicability and robustness.

Declaration on Generative AI

Authors have not employed any Generative AI tools.

References

[1] S. A. Sert, A. Yazici, Optimizing the Performance of Rule-based Fuzzy Routing Algorithms in Wireless Sensor Networks, in: IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019, pp. 1–6. doi:10.1109/FUZZ-IEEE.2019.8858920.

[2] Y. Touati, Fuzzy Logic-based Evolutionary Approach for Load Balancing in Large-Scale Wireless Sensor Networks, in: 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, pp. 520-525. doi:10.1109/UEMCON.2018.8796811.

[3] J. N. Al-Karaki, A. E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey, IEEE Wireless Communications 11 6 (2004) 6–28. doi:10.1109/MWC.2004.1368893.

[4] National Institute of Standards and Technology, Zero Trust Architecture. NIST Special Publication 800-207, 2020. doi:10.6028/NIST.SP.800-207.

[5] International Organization for Standardization, ISO/IEC 27033-1:2015. Information Technology—Security Techniques—Network Security. Part 1: Overview and Concepts, Ed. 2, 2015. https://www.iso.org/standard/63461.html

[6] A. Alshamrani, S. Myneni, A. Chowdhary, D. Huang, A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities, IEEE Communications Surveys & Tutorials 21 2 (2019) 1851–1877. doi:10.1109/COMST.2019.2891891.

[7] L. Zhou, H. Yin, H. Zhao, J. Wei, D. Hu, V. C. M. Leung, A Comprehensive Survey of Artificial Intelligence Applications in UAV-Enabled Wireless Networks. Digital Communications and Networks (2024). doi:10.1016/j.dcan.2024.11.005.

[8] T. Maitra, R. Amin, D. Giri, P. D. Srivastava, An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card, International Journal of Network Security 18 3 (2016) 553–564. http://ijns.jalaxy.com.tw/contents/ijns-v18-n3/ijns-2016-v18-n3-p553-564.pdf

[9] Q. Zhang, L. T. Yang, Z. Yan, Z. Chen, P. Li, An Efficient Deep Learning Model to Predict Cloud Workload for Industry Informatics, IEEE Transactions on Industrial Informatics 14 7 (2018) 4334–4343. doi:10.1109/TII.2018.2808910.

[10] O. Kryvoruchko, Y. Kostiuk, A. Desiatko, K. Stepashkina, D. Tyshchenko, T. Franchuk, D. Hnatchenko, R. Zakharov, R. Brzhanov, Analysis of technical indicators of efficiency and quality of intelligent systems, Journal of Theoretical and Applied Information Technology 101 24 (2023) 127–139. https://www.jatit.org/volumes/Vol101No24/16Vol101No24.pdf

[11] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, M. Liyanage, A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions, IEEE Communications Surveys & Tutorials 26 1 (2024) 534-570. doi:10.1109/COMST.2023.3312349.

[12] S. Rzaieva, D. Rzaiev, Y. Kostyuk, H. Hulak, O. Shcheblanin, Methods of Modeling Database System Security, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, pp. 384–390. https://ceur-ws.org/Vol-3654/short5.pdf

[13] P. Nayak, A. Devulapalli, A Fuzzy Logic-based Clustering Algorithm for WSN to Extend the Network Lifetime, IEEE Sensors Journal 16 1 (2016) 137–144, doi:10.1109/JSEN.2015.2472970.

[14] M. Adnan, L. Yang, T. Ahmad, Y. Tao, An Unequally Clustered Multi-Hop Routing Protocol based on Fuzzy Logic for Wireless Sensor Networks, IEEE Access 9 (2021) 38531–38545, doi:10.1109/ACCESS.2021.3063097.

[15] T. Shafique, A.-H. Soliman, A. Amjad, Data Traffic Based Shape Independent Adaptive Unequal Clustering for Heterogeneous Wireless Sensor Networks, IEEE Access 12 (2024) 46422–46443. doi:10.1109/ACCESS.2024.3381520.

[16] Y. Kostiuk, P. Skladannyi, Y. Samoilenko, K. Khorolska, B. Bebeshko, V. Sokolov, A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: Cyber Hygiene & Conflict Management in Global Information Networks, vol. 3925, 2025, pp. 249–264. https://ceur-ws.org/Vol-3925/paper21.pdf

[17] Y. Kostiuk, P. Skladannyi, N. Korshun, B. Bebeshko, K. Khorolska, Integrated Protection Strategies and Adaptive Resource Distribution for Secure Video Streaming over a Bluetooth Network, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, pp. 129–138. https://ceur-ws.org/Vol-3826/paper12.pdf

[18] H. Taheri, P. Neamatollahi, O. M. Younis, S. Naghibzadeh, M. H. Yaghmaee, An Energy-Aware Distributed Clustering Protocol in Wireless Sensor Networks using Fuzzy Logic, Ad Hoc Networks 10 7 (2012) 1469–1481. doi:10.1016/j.adhoc.2012.04.004.

[19] N. A. Torghabeh, M. R. A. Totonchi, M. H. Y. Moghaddam, Cluster Head Selection using a Two-Level Fuzzy Logic in Wireless Sensor Networks, in: 2nd International Conference on Computer Engineering and Technology, 2010, pp. V2-357–V2-361. doi:10.1109/ICCET.2010.5485483.

[20] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, in: 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, vol. 2, 2000, pp. 10. doi:10.1109/HICSS.2000.926982.