Odesa Polytechnic National University, Kyiv National University, T. Shevchenko, Kharkiv National University of Radio Electronics, National Aviation University; Odesa National University, I.I. Mechnikov, Sumy State University, Admiral Makarov National University of Shipbuilding; Lodz Technical University, Azerbaijan State Oil Industry University, Anhalt University of Applied Sciences, Caten, Germany, CEUR-WS.

MATERIALS

OF THE XIII INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE «Information Control Systems and Technologies» (ICST- ODESA – 2025)

24th – 26th September, 2025

Львів-Торунь
Liha-Pres
2025

CONTENTS

computational effort, which makes it one of the most important stages of comprehensive optimization. This procedure reduced the objective function for the UAV's FCS by 27.5%. The final optimization stage, involving the tuning of FIE and the defuzzification operations, was found to have the least impact on overall system performance that can be omitted in a number of cases. It resulted in only a 5.6% improvement in performance.

References

1. Li, C., Han, S., Zeng, S., & Yang, S. (2024). *Intelligent optimization: Principles, algorithms and applications*. Singapore: Springer. https://doi.org/10.1007/978-981-97-3286-9

2. Kozlov, O., Ivanov, P., Petrenko, A., & Shevchenko, M. (2024). Swarm optimization of the drone's intelligent control system: Comparative analysis of hybrid techniques. In *CEUR Workshop Proceedings* (Vol. 3790, pp. 1–12). CEUR-WS. https://ceur-ws.org/Vol-3790/paper01.pdf

UDC 004.738:004.056

АДАПТИВНА ПОЛІТИКА МАРШРУТИЗАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ph.D. В. Соколов[0000-0002-9349-7946], **Ph.D. Ю. Костюк**[0000-0001-5423-0985], **Ph.D. П. Складанний** [0000-0002-7775-6039], **Dr.Sci. Н. Коршун** [0000-0003-2908-970X]
Київський столичний університет імені Бориса Грінченка, Україна
EMAIL: v.sokolov@kubg.edu.ua

ADAPTIVE ROUTING POLICY FOR NETWORK TRAFFIC IN INFORMATION SECURITY SYSTEMS

Ph.D. V. Sokolov, Ph.D. Y. Kostiuk, Ph.D. P. Skladannyi, Dr.Sci. N. Korshun
Borys Grinchenko Kyiv Metropolitan University, Ukraine

Анотація. *У статті розглядаються виклики забезпечення інформаційної безпеки в умовах зростання трафіку та складності топологій розподілених систем. Обґрунтовано адаптацію політики маршрутизації до вимог кібербезпеки з урахуванням ризиків атак. Запропоновано формалізований підхід з математичним моделюванням, метриками ризиків, стандартами ISO/IEC 27033, 15408, NIST SP 800-207 та технологіями програмно-конфігурованої мережі. Розроблено архітектуру системи для реального часу,*

що підвищує кіберстійкість за принципами zero trust. Результати застосовні для захисту критичних систем.

Ключові слова: *адаптивна маршрутизація, інформаційна безпека, мережевий трафік, політика маршрутизації,* zero trust.

Abstract. *The paper addresses information security challenges amid increasing traffic volumes and complex topologies in distributed systems. It justifies adapting routing policies to cybersecurity requirements, considering attack risks and anomalies. A formalized approach integrates mathematical modeling, risk metrics, ISO/IEC 27033, 15408, NIST SP 800-207 standards, software-defined networking technologies, and telemetry (NetFlow, sFlow). The developed system architecture adapts to threats in real-time, enhancing cyber resilience via Zero Trust principles. Results apply to critical corporate and public systems.*

Keywords: *adaptive routing, information security, network traffic, routing policy, zero trust.*

Adapting routing to security is a task driven by complex architectures and threats. Modern approaches combine classical routing with dynamic management, machine learning, and risk assessment. Research by Sert and Yazici [1] shows that fuzzy logic and genetic algorithms balance load and increase resilience. Al-Karaki and Kamal [2] review routing methods, while standards [3] emphasize dynamic access control. Adaptive routing reduces leakage risks and supports proactive defense.

The research is based on set theory, combinatorial analysis, and optimization for modeling networks under security constraints. Models dynamically adapt routes considering topology, context, and risks, forming resilient policies.

The concept of proactive defense is implemented through threat-based policy adaptation. Automated route generation minimizes access to vulnerable zones. The architectural solution integrates modeling, analytics, telemetry (NetFlow/sFlow), and ISO/IEC, NIST standards.

The mathematical model considers route sets, risk weights, trust, and criticality. It automates real-time routing decisions depending on security context. The interaction sequence of components—telemetry, risk evaluator, policy manager, router—ensures traffic redirection.

The model uses sets: channels $S = (S_1, ..., S_p)$, nodes $N = (N_1, ..., N_k)$, and security coefficients $X = (X_1, ..., X_p)$ are normalized values from 1 to 10 based on vulnerability and threat analysis. Sets of threats M, priorities NP, and constraints K per ISO/IEC 15408.

Requirements matrix: resources R_k in columns, requirements K_j in rows, weights W_{ijk} from 0 to 10. Integral coefficient:

$$X_i = \sum\sum W_{ijk}.$$

And security priority:

$$P_i = \alpha \cdot NP_i + \beta \cdot X_i$$

with $\alpha, \beta \in [0,1]$, e.g., $\alpha = 0.4$, $\beta = 0.6$, X_i is the safety factor.

The model adapts routing to security via risk metrics, trust parameters, behavior, and standards. Mathematics accounts for parameters, threats, criticality, and dynamics for automatic priority updates. New metrics (risk deficit, resilience, sensitivity, efficiency) and modified Ford-Fulkerson build secure flows.

The system combines topology, metrics, parameters, and constraints to form priorities by channel security level. It integrates telemetry, risk evaluation, analytics, and dynamic protocols for threat resilience, vulnerability isolation, and ZTA. Applicable to governmental and corporate systems, uniting proactive cyber defense, flexible traffic management, and standardized models.

References

1. Sert, S. A., & Yazici, A. (2019). Optimizing the performance of rule-based fuzzy routing algorithms in wireless sensor networks. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE. https://doi.org/10.1109/fuzz-ieee.2019.8858920

2. Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications, 11*(6), 6–28. https://doi.org/10.1109/mwc.2004.1368893

3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207