ABSTRACT AND REFERENCES
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2025.341735

IMPROVING A METHOD FOR DETERMINING THE COORDINATES OF A RECONNAISSANCE UNMANNED AERIAL VEHICLE BY A SMALL-BASED NETWORK OF TWO SOFTWARE-DEFINED RADIO RECEIVERS (p. 6–13)

Igor Ruban
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-4738-3286

Hennadii Khudov
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-3311-2848

Yelyzaveta Biernik
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID https://orcid.org/0009-0008-0349-6327

Oleksandr Makoveichuk
Higher Education Institution "Academician Yuriy Bugay International Scientific and Technical University", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-4425-016X

Volodymyr Maliuha
State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
ORCID: https://orcid.org/0000-0001-6227-1269

Serhii Yarovyi
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-6138-5774

Rostyslav Khudov
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-6209-209X

Vladyslav Khudov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-9863-4743

Leonid Poberezhnyi
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0009-0002-6648-512X

Olena Goncharenko
State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
ORCID: https://orcid.org/0000-0001-9479-9797

This study investigates the process for determining the coordinates of a reconnaissance unmanned aerial vehicle. The task addressed relates to determining the coordinates of a reconnaissance unmanned aerial vehicle using a small-scale network of mobile passive location devices.

A method for determining the coordinates of a reconnaissance unmanned aerial vehicle has been improved, which, unlike known ones, involves:

– determining bearings for a reconnaissance unmanned aerial vehicle;

– using the triangulation method.

The accuracy of determining the coordinates of a reconnaissance unmanned aerial vehicle by a small-scale network of two Software-Defined Radio receivers has been assessed. It has been established that the shape and orientation of the error ellipses depends on the position of the reconnaissance unmanned aerial vehicle relative to the Software-Defined Radio receivers. The accuracy of determining the coordinates significantly deteriorates in cases where the polar angle of observation from the center of the base approaches 0° or 180°. The highest accuracy of determining coordinates is achieved when the reconnaissance unmanned aerial vehicle is located on the traverse to the middle of the base.

It has been established that for small bases there is a more pronounced unevenness of the dependence of accuracy on the position of the reconnaissance unmanned aerial vehicle compared to larger bases. At long ranges, errors for small bases increase sharply. It has been established that with a decrease in the base length, the area of the error ellipses increases, which indicates a deterioration in the potential accuracy characteristics of the system and an increase in the average circular error. At the same time, the geometric features are preserved, the orientation of the ellipses and the nature of their location relative to the base line remain constant.

Keywords: unmanned aerial vehicle, small-base network, Software-Defined Radio receiver, bearing.

References

1. Goldstein, L., Waechter, N. (2023). Chinese Strategists Evaluate the Use of 'Kamikaze' Drones in the Russia-Ukraine War. Rand. Available at: https://www.rand.org/pubs/commentary/2023/11/chinese-strategists-evaluate-the-use-ofkamikaze-drones.html
2. Grigore, L., Cristescu, C. (2024). The Use of Drones in Tactical Military Operations in the Integrated and Cybernetic Battlefield. Land Forces Academy Review, 29 (2), 269–273. https://doi.org/10.2478/raft-2024-0029
3. Riabukha, V. P. (2020). Radar Surveillance of Unmanned Aerial Vehicles (Review). Radioelectronics and Communications Systems, 63 (11), 561–573. https://doi.org/10.3103/s0735272720110011
4. Hrudka, O. (2024). Russian drone manufacturer 'Orlan-10' ramps up production despite sanctions, Inform Napalm reports. Available at: https://euromaidanpress.com/2024/01/13/russian-drone-manufacturer-orlan-10-ramps-up-production-despite-sanctions-inform-napalm-reports/
5. British intelligence: Russian radar destroyed in missile attack on Belbek in Crimea (2024). Available at: https://mind.ua/en/news/20269399-british-intelligence-russian-radar-destroyed-in-missile-attack-on-belbek-in-crimea
6. Khudov, H., Makoveichuk, O., Kostyria, O., Butko, I., Poliakov, A., Kozhushko, Y. et al. (2024). Devising a method for determining the coordinates of an unmanned aerial vechicle via a network of portable spectrum analyzers. Eastern-European Journal of Enterprise Technologies, 6 (9 (132)), 97–107. https://doi.org/10.15587/1729-4061.2024.318551
7. Khudov, H., Kostianets, O., Kovalenko, O., Maslenko, O., Solomonenko, Y. (2023). Using Software-Defined radio receivers for determining the coordinates of low-visible aerial objects. Eastern-European Journal of Enterprise Technologies, 4 (9 (124)), 61–73. https://doi.org/10.15587/1729-4061.2023.286466
8. Boussel, P. (2024). The Golden Age of Drones: Military UAV Strategic Issues and Tactical Developments. Available at: https://trendsresearch.org/insight/the-golden-age-of-drones-military-uav-strategic-

issues-and-tactical-developments/?srsltid=AfmBOoptC41niCzbAJGHOTcUhRGJpWEW_y7hHLkJ_5hkabW_fIBS5sZ
9. Melvin, W. L., Scheer, J. (2012). Principles of Modern Radar: Advanced techniques. The Institution of Engineering and Technology. https://doi.org/10.1049/sbra020e
10. Melvin, W. L., Scheer, J. A. (2013). Principles of Modern Radar: Volume 3: Radar Applications. The Institution of Engineering and Technology. https://doi.org/10.1049/sbra503e
11. Lishchenko, V., Kalimulin, T., Khizhnyak, I., Khudov, H. (2018). The Method of the organization Coordinated Work for Air Surveillance in MIMO Radar. 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 1–4. https://doi.org/10.1109/ukrmico43733.2018.9047560
12. Neyt, X., Raout, J., Kubica, M., Kubica, V., Roques, S., Acheroy, M., Verly, J. G. (2006). Feasibility of STAP for Passive GSM-Based Radar. 2006 IEEE Conference on Radar, 546–551. https://doi.org/10.1109/radar.2006.1631853
13. Willis, N. J. (2004). Bistatic Radar. The Institution of Engineering and Technology. https://doi.org/10.1049/sbra003e
14. Semenov, S., Jian, Y., Jiang, H., Chernykh, O., Binkovska, A. (2025). Mathematical model of intelligent UAV flight path planning. Advanced Information Systems, 9 (1), 49–61. https://doi.org/10.20998/2522-9052.2025.1.06
15. Ruban, I., Khudov, H., Lishchenko, V., Pukhovyi, O., Popov, S., Kolos, R. et al. (2020). Assessing the detection zones of radar stations with the additional use of radiation from external sources. Eastern-European Journal of Enterprise Technologies, 6 (9 (108)), 6–17. https://doi.org/10.15587/1729-4061.2020.216118
16. Multilateration (MLAT). Concept of Use. Available at: https://www2023.icao.int/APAC/Documents/edocs/mlat_concept.pdf
17. Luo, D., Wen, G. (2024). Distributed Phased Multiple-Input Multiple-Output Radars for Early Warning: Observation Area Generation. Remote Sensing, 16 (16), 3052. https://doi.org/10.3390/rs16163052
18. Kalkan, Y. (2024). 20 Years of MIMO Radar. IEEE Aerospace and Electronic Systems Magazine, 39 (3), 28–35. https://doi.org/10.1109/maes.2023.3349228
19. Barabash, O., Kyrianov, A. (2023). Development of control laws of unmanned aerial vehicles for performing group flight at the straight-line horizontal flight stage. Advanced Information Systems, 7 (4), 13–20. https://doi.org/10.20998/2522-9052.2023.4.02
20. Khudov, H., Hryzo, A., Oleksenko, O., Repilo, I., Lisohorskyi, B., Poliakov, A. et al. (2025). Devising a method for determining the coordinates of an air object by a network of two SDR receivers. Eastern-European Journal of Enterprise Technologies, 1 (9 (133)), 62–68. https://doi.org/10.15587/1729-4061.2025.323336
21. Weber, C., Peter, M., Felhauer, T. (2015). Automatic modulation classification technique for radio monitoring. Electronics Letters, 51 (10), 794–796. https://doi.org/10.1049/el.2015.0610

DOI: 10.15587/1729-4061.2025.340918

DESIGN OF A SIMULATION TOOL FOR PLANNING UAV MISSION SUCCESS UNDER COMBAT CONSTRAINTS (p. 14–26)

Anton Tyshchenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0009-0001-9587-4274

Iryna Stopochkina
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-0346-0390

This study investigates unmanned aerial vehicle (UAV) networks operating under the influence of destructive and hostile factors. The study considers, among destructive factors, changes in signal power at the receiver side caused by distance and battery charge limitations. Among the hostile factors, cyber-physical threats have been examined, including those caused by electronic countermeasure (ECM) systems and malware-based attacks.

Algorithmic and software solutions have been developed to simulate the behavior of UAVs under such constraints. A special feature of the proposed model, in contrast to existing approaches, is that it integrates factors such as signal degradation caused by ECM systems and the dynamics of malware propagation within the network.

Scenarios include UAV behavior under jamming, the probabilistic spread of malware, and the switching of operational modes in response to threat exposure. The results were achieved by integrating a wide range of parameters, including device identifier, signal power, transmitter radius, transmission frequency, geolocation, task type, malware sensitivity, message handling queue, propagation delay, as well as movement speed. These features enable the model to realistically reproduce system behavior in uncertain and hostile environments, allowing both defensive and offensive security strategies to be explored. Devising appropriate operational scenarios is also possible.

The proposed software solution is characterized by the high level of detail in the simulation and the use of the Rust programming language, which ensures performance, modularity, and future extensibility. The solution reported here supports visualization of the behavior of up to 100 UAVs and more through both images and animations. It can be used for analyzing attack scenarios, designing robust UAV architectures, and prototyping offensive security tools. The source code is publicly available at GitHub repository, supporting practical usage and further research applications.

Keywords: UAV network simulation, cyber-physical security, malware, electronic countermeasures.

References

1. McNabb, M. (2025). Ukraine's Trojan Horse Drones: A New Frontier in Cyber Warfare. DroneLife. Available at: https://dronelife.com/2025/04/10/ukraines-trojan-horse-drones-a-new-frontier-in-cyber-warfare/
2. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218. https://doi.org/10.1016/j.iot.2020.100218
3. Hartmann, K., Giles, K. (2016). UAV Exploitation: A New Domain for Cyber Power. 6 8th International Conference on Cyber Conflict. Tallinn, 205–221. Available at: https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf
4. Abro, G., Zulkifli, S., Masood, R., Asirvadam, V., Laouiti, A. (2022). Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. Drones, 6 (10), 284. https://doi.org/10.3390/drones6100284
5. Riahi Manesh, M., Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future

research directions. Computers & Security, 85, 386–401. https://doi.org/10.1016/j.cose.2019.05.003
6. Drone Hacking: Exploitation and Vulnerabilities. Available at: https://spadok.org.ua/books/Drone+Hacking-+Exploitation++and+Vulnerabilities.pdf
7. Throwback Attack: Keylogging virus infects U.S. drone fleet (2022). Control Engineering. Available at: https://www.controleng.com/throwback-attack-keylogging-virus-infects-u-s-drone-fleet/
8. Zakharchenko, I., Tristan, A., Chornogor, N., Berdnik, P., Kalashnyk, G., Timochko, A. et al. (2022). Modeling of Object Monitoring Using 3D Cellular Automata. Problems of the Regional Energetics, 4 (56), 61–73. https://doi.org/10.52254/1857-0070.2022.4-56.06
9. Song, Z., Zhang, H., Zhang, X., Zhang, F. (2019). Unmanned Aerial Vehicle Coverage Path Planning Algorithm Based on Cellular Automata. 2019 15th International Conference on Computational Intelligence and Security (CIS), 123–126. https://doi.org/10.1109/cis.2019.00034
10. Ioannidis, K., Sirakoulis, G. Ch., Andreadis, I. (2011). A path planning method based on cellular automata for cooperative robots. Applied Artificial Intelligence, 25 (8), 721–745. https://doi.org/10.1080/08839514.2011.606767
11. Adamatzky, A. I. (1996). Computation of shortest path in cellular automata. Mathematical and Computer Modelling, 23 (4), 105–113. https://doi.org/10.1016/0895-7177(96)00006-4
12. Behring, C., Bracho, M., Castro, M., Moreno, J. A. (2001). An Algorithm for Robot Path Planning with Cellular Automata. Theory and Practical Issues on Cellular Automata, 11–19. https://doi.org/10.1007/978-1-4471-0709-5_2
13. Xie, J., Chen, J. (2022). Multiregional Coverage Path Planning for Multiple Energy Constrained UAVs. IEEE Transactions on Intelligent Transportation Systems, 23 (10), 17366–17381. https://doi.org/10.1109/tits.2022.3160402
14. Fedorova, A., Beliautsou, V., Zimmermann, A. (2022). Colored Petri Net Modelling and Evaluation of Drone Inspection Methods for Distribution Networks. Sensors, 22 (9), 3418. https://doi.org/10.3390/s22093418
15. Xu, D., Borse, P., Altenburg, K., Nygard, K. (2006). A Petri Net Simulator for Self-organizing Systems. Proceedings of the 5th WSEAS Int. Conf. on Artificial Intelligence, Knowledge Engineering and Data Bases. Madrid, 31–35. Available at: https://www.researchgate.net/publication/234805596
16. Gonçalves, P., Sobral, J., Ferreira, L. A. (2017). Unmanned aerial vehicle safety assessment modelling through petri Nets. Reliability Engineering & System Safety, 167, 383–393. https://doi.org/10.1016/j.ress.2017.06.021
17. Wang, X., Guo, Y., Lu, N., He, P. (2023). UAV Cluster Behavior Modeling Based on Spatial-Temporal Hybrid Petri Net. Applied Sciences, 13 (2), 762. https://doi.org/10.3390/app13020762
18. NS-3. Network Simulator. Available at: https://www.nsnam.org/
19. OMNeT++. Available at: https://omnetpp.org/
20. GAMA Platform. Available at: https://gama-platform.org/
21. Nikolaiev, M., Novotarskyi, M. (2024). Comparative Review of Drone Simulators. Information, Computing and Intelligent Systems, 4, 79–98. https://doi.org/10.20535/2786-8729.4.2024.300614
22. GPS Jamming, Spoofing and Hacking (2025). NorthStandard. Available at: https://north-standard.com/insights-and-resources/resources/articles/gps-jamming-spoofing-and-hacking
23. Stopochkina, I., Novikov, O., Voitsekhovskyi, A., Ilin, M., Ovcharuk, M. (2025). Simulation of UAV networks on the battlefield, taking into account cyber- physical influences that affect availability. Theoretical and Applied Cybersecurity, 6 (2). https://doi.org/10.20535/tacs.2664-29132024.2.318182
24. Pro zviazok vid Serhiya Flesh. Available at: https://t.me/s/serhii_flash
25. McNabb, M (2024). What Kind of Drones is Ukraine Buying? DroneLife. Available at: https://dronelife.com/2024/11/04/what-kind-of-drones-is-ukraine-buying/
26. Code and data for the paper: «Simulation of Unmanned Aerial Vehicles Networks under Electronic Warfare and Malware Propagation Conditions». Available at: https://github.com/KryvavyiPotii/drone-network

DOI: 10.15587/1729-4061.2025.341734

DEVELOPMENT OF A MODEL FOR THE ANALYSIS AND SEPARATION OF SERVICE AND USEFUL TRAFFIC IN CYBER-PHYSICAL SYSTEMS (p. 27–40)

Maksym Tolkachov
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-7853-5855

Nataliia Dzheniuk
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-0758-7935

Serhii Yevseiev
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1647-6444

Yevhen Melenti
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID https://orcid.org/0000-0003-2955-2469

Volodymyr Shulha
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-4356-7288

Serhii Mykus
National Defence University of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7103-4166

Ivan Opirskyy
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-8461-8996

Anton Smirnov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-4121-3902

Marharyta Melnyk
Science Entrepreneurship Technology University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-0619-7281

Mykhailo Zhyhalov
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0009-0000-7192-1382

The object of the study is the processes of formation, transmission and processing of service and useful traffic in cyber-physical systems of Smart Manufacturing Ecosystem multi-level architecture type, vulnerable to cyberattacks aimed at compromising control data, authentication and coordination. In modern computer networks, service traffic determines the stability and security of the infrastruc-

ture, since any distortion or interception of service traffic can lead to disruption of the system as a whole. In smart systems, industrial Internet of Things and critical infrastructure, the volume of service messages reaches significant scales, because it is they that support the synchronism of thousands of systems in real time.

The paper investigates the problem of protecting service traffic in Smart Manufacturing Ecosystem cyber-physical systems. A mathematical model of service and useful traffic segmentation is proposed, which takes into account the criteria of stability (access segmentation, integrity and authenticity control) and security (probability of compromise, channel criticality, level of trust in the transmission medium). To construct an integral risk indicator, the convolution method is used, which allows combining different types of parameters and determining the feasibility of dividing traffic for target analysis. The study was conducted using industrial protocols Modbus, DNP3, OPC UA, MQTT and HTTP, which are widely used in production networks. It was shown that the use of the model allows reducing the integral risk of attacks on service traffic by an average of 15–20% compared to approaches without segmentation. The developed model forms a scientific basis for creating methods and practical cyber protection solutions that ensure increased resilience of the Smart Manufacturing infrastructure and are able to withstand current and future challenges in the field of cybersecurity.

Keywords: service traffic, industrial protocols, cyber-physical system, cybersecurity, production pyramid, IoT networks.

References

1. 2024 Cybersecurity Statistics. Purplesec. Available at: https://purplesec.us/resources/cybersecurity-statistics/
2. ISO/IEC 27032:2023(en). Cybersecurity – Guidelines for Internet security. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en
3. X.1205 : Overview of cybersecurity (2008). ITU. Available at: https://www.itu.int/rec/t-rec-x.1205-200804-i
4. Zakharzhevskyy, A. G., Tolkachov, M. Yu., Dzhenyuk, N. V., Pogasii, S. S., Glukhov, S. I. (2024). The method of protecting information resources based on the semiotic model of cyberspace. Modern Information Security, 57 (1). https://doi.org/10.31673/2409-7292.2024.010007
5. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M. et al. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 53–74. https://doi.org/10.15587/1729-4061.2023.289467
6. Nadhir, A. M., Mounir, B., Abdelkader, L., Hammoudeh, M. (2025). Enhancing Cybersecurity in Healthcare IoT Systems Using Reinforcement Learning. Transportation Research Procedia, 84, 113–120. https://doi.org/10.1016/j.trpro.2025.03.053
7. Yin, C., Zhu, Y., Fei, J., He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/access.2017.2762418
8. Lu, Y., Morris, K., Frechette, S. (2016). Current Standards Landscape for Smart Manufacturing Systems. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8107
9. Hu, Y., Wendong, W., Xiangyang, G., Liu, C. H., Que, X., Cheng, S. (2014). Control traffic protection in software-defined networks. 2014 IEEE Global Communications Conference, 1878–1883. https://doi.org/10.1109/glocom.2014.7037082
10. Barbosa, R. R. R., Sadre, R., Pras, A. (2016). Exploiting traffic periodicity in industrial control networks. International Journal of Critical Infrastructure Protection, 13, 52–62. https://doi.org/10.1016/j.ijcip.2016.02.004
11. Kotsiopoulos, T., Radoglou-Grammatikis, P., Lekka, Z., Mladenov, V., Sarigiannidis, P. (2025). Defending industrial internet of things against Modbus/TCP threats: A combined AI-based detection and SDN-based mitigation solution. International Journal of Information Security, 24 (4). https://doi.org/10.1007/s10207-025-01076-2
12. Lin, C.-Y., Nadjm-Tehrani, S. (2023). Protocol study and anomaly detection for server-driven traffic in SCADA networks. International Journal of Critical Infrastructure Protection, 42, 100612. https://doi.org/10.1016/j.ijcip.2023.100612
13. Anwar, M., Lundberg, L., Borg, A. (2022). Improving anomaly detection in SCADA network communication with attribute extension. Energy Informatics, 5 (1). https://doi.org/10.1186/s42162-022-00252-1
14. Griffor, E. R., Greer, C., Wollman, D. A., Burns, M. J. (2017). Framework for cyber-physical systems: volume 1, overview. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.1500-201
15. Aposemat IoT-23. A labeled dataset with malicious and benign IoT network traffic. Available at: https://www.stratosphereips.org/datasets-iot23
16. Kamarei, M., Patooghy, A., Alsharif, A., AlQahtani, A. A. S. (2023). Securing IoT-Based Healthcare Systems Against Malicious and Benign Congestion. IEEE Internet of Things Journal, 10 (14), 12975–12984. https://doi.org/10.1109/jiot.2023.3257543
17. Ghadermazi, J., Shah, A., Bastian, N. D. (2025). Towards Real-Time Network Intrusion Detection With Image-Based Sequential Packets Representation. IEEE Transactions on Big Data, 11 (1), 157–173. https://doi.org/10.1109/tbdata.2024.3403394
18. Yu, L., Dong, J., Chen, L., Li, M., Xu, B., Li, Z. et al. (2021). PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection. Computer Networks, 194, 108117. https://doi.org/10.1016/j.comnet.2021.108117
19. Lazzaro, S., De Angelis, V., Mandalari, A. M., Buccafurri, F. (2024). Is Your Kettle Smarter Than a Hacker? A Scalable Tool for Assessing Replay Attack Vulnerabilities on Consumer IoT Devices. 2024 IEEE International Conference on Pervasive Computing and Communications (PerCom). https://doi.org/10.1109/percom59722.2024.10494466
20. IoT Security Risks: Stats and Trends to Know in 2025. JumpCloud. Available at: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025
21. Tran, B., Attorney, P. (2025). IoT Security Challenges: Device Vulnerability & Attack Stats. PatentPC. Available at: https://patentpc.com/blog/iot-security-challenges-device-vulnerability-attack-stats
22. Censys data reports over 145,000 exposed ICS services worldwide, highlights US vulnerabilities (2024). Industrial Cyber. Available at: https://industrialcyber.co/industrial-cyber-attacks/censys-data-reports-over-145000-exposed-ics-services-worldwide-highlights-us-vulnerabilities/
23. Cyberthreats to industrial IoT in the manufacturing sector (2005). PT Security. Available at: https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-industrial-iot/#Navigation-1
24. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I. et al. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 5 (9 (131)), 63–78. https://doi.org/10.15587/1729-4061.2024.313158

25. Tolkachov, M., Dzheniuk, N., Havrylova, A., Chechui, O., Hapon, A., Tiutiunyk, V. (2025). Cognitive Approach to Cybersecurity: Causality Analysis and Situational Learning. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), 1–4. https://doi.org/10.1109/ichora65333.2025.11017107
26. Hrischev, R. (2020). ERP systems and data security. IOP Conference Series: Materials Science and Engineering, 878 (1), 012009. https://doi.org/10.1088/1757-899x/878/1/012009
27. Silva, C., Cunha, V. A., Barraca, J. P., Aguiar, R. L. (2023). Analysis of the Cryptographic Algorithms in IoT Communications. Information Systems Frontiers, 26 (4), 1243–1260. https://doi.org/10.1007/s10796-023-10383-9
28. Kumar, A., Vishnoi, P., S. L., S. (2019). Smart Grid Security with Cryptographic Chip Integration. EAI Endorsed Transactions on Energy Web, 6 (23), 157037. https://doi.org/10.4108/eai.13-7-2018.157037
29. Sudyana, D., Yudha, F., Lin, Y.-D., Lai, C.-H., Lin, P.-C., Hwang, R.-H. (2025). From Flow to Packet: A Unified Machine Learning Approach for Advanced Intrusion Detection. Security and Communication Networks, 2025 (1). https://doi.org/10.1155/sec/5729035
30. Zhao, J., Jing, X., Yan, Z., Pedrycz, W. (2021). Network traffic classification for data fusion: A survey. Information Fusion, 72, 22–47. https://doi.org/10.1016/j.inffus.2021.02.009

DOI: 10.15587/1729-4061.2025.340917

DEVELOPMENT OF AN ALGORITHM WITH TEMPORARY CRYPTOGRAPHIC SECURITY FOR ENCRYPTING VIDEO STREAM FROM AN UNMANNED AERIAL VEHICLE (p. 41–53)

Liudmyla Kovalchuk
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-2874-7950

Anatolii Davydenko
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-6466-1690

Tatiana Klymenko
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
ORCID: https://orcid.org/0009-0003-4675-6428

Arina Nedashkivska
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0009-0003-2687-7011

Serhii Hilgurt
G. E. Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-1647-1790

This study considers the process that protects a video stream transmitted from the onboard video camera of an unmanned aerial vehicle (UAV) to a ground station in the front and near-front zones. The specificity of the task set is predetermined, on the one hand, by the limited computing resources of onboard equipment, which must encrypt an intensive data stream in real time, and, on the other hand, by the relatively short life span of UAV under combat conditions (especially for FPV kamikaze drones) ranging from 10 minutes to several days.

Most known works in this field consider algorithms focused on application in other settings, with the main efforts aimed at achieving maximal cryptographic security. Unlike the technological advancements highlighted in the available literature, this study has managed to solve the specified problem by taking into account its specific features and utilizing a certain trade-off between the speed and resource intensity of the algorithm, on the one hand, and its security, on the other.

The result was achieved through a detailed comparative analysis and categorization of the closest solutions in terms of characteristics, which is the largest part of the study. Based on its results, the PRESENT algorithm was chosen as the first approximation.

The proposed solution is based on the use of a modification of this algorithm reduced to 16 rounds in counter mode. Analysis of the resulting solution reveals that its cryptographic security requires more than 2 months of computational work when implementing the best attack, i.e., the security of the algorithm is reasonably acceptable.

For practical application of the theoretical results, it is necessary to carefully check the properties of the proposed solution implemented in the equipment under field conditions, as close as possible to combat operations, and, if necessary, to make the necessary adjustments.

Keywords: UAV, video data encryption, temporal cryptographic security, lightweight cryptographic algorithms, block ciphers, PRESENT.

References

1. Cox, J., Wong, K. (2019). Predictive feedback augmentation for manual control of an unmanned aerial vehicle with latency. International Journal of Micro Air Vehicles, 11. https://doi.org/10.1177/1756829319869645
2. Kamtam, S. B., Lu, Q., Bouali, F., Haas, O. C. L., Birrell, S. (2024). Network Latency in Teleoperation of Connected and Autonomous Vehicles: A Review of Trends, Challenges, and Mitigation Strategies. Sensors, 24 (12), 3957. https://doi.org/10.3390/s24123957
3. ECP5/ECP5-5G. Family Table. ECP5 and ECP5-5G Device Selection Guide. Lattice Semiconductor. Available at: https://www.latticesemi.com/Products/FPGAandCPLD/ECP5
4. 7 Series FPGAs Data Sheet: Overview. DS180 (v2.6.1) (2020). Product Specification. AMD XILINX. Available at: https://docs.amd.com/v/u/en-US/ds180_7Series_Overview
5. Ashrif, F. F., Sundararajan, E. A., Ahmad, R., Hasan, M. K., Yadegaridehkordi, E. (2024). Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. Journal of Network and Computer Applications, 221, 103759. https://doi.org/10.1016/j.jnca.2023.103759
6. Ismael, H. M., Al-Ta'i, Z. T. M. (2021). Authentication and Encryption Drone Communication by Using HIGHT Lightweight Algorithm. Turkish Journal of Computer and Mathematics Education, 12 (11), 5891–5908. Available at: https://www.researchgate.net/publication/392193717_Authentication_and_Encryption_Drone_Communication_by_Using_HIGHT_Lightweight_Algorithm
7. Cecchinato, N., Toma, A., Drioli, C., Oliva, G., Sechi, G., Foresti, G. L. (2022). A Secure Real-time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain. Procedia Computer Science, 205, 50–57. https://doi.org/10.1016/j.procs.2022.09.006
8. Rahiyanath, T. Y. (2015). A Novel Architecture for Lightweight Block Cipher, Piccolo. International Journal of Research in Engineering and Technology, 04 (09), 97–103. Available at: https://ijret.org/volumes/2015v04/i09/IJRET20150409017.pdf

9. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B. et al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems - CHES 2007, 450–466. https://doi.org/10.1007/978-3-540-74735-2_31
10. Safronov, T. (2024). AES-256: V Ukrspecsystems rozkryly detali shyfruvannia danykh BPLA Shark. Militarnyi. Available at: https://militarnyi.com/uk/news/zahyst-danyh-vid-bpla-shark-posylyly-shyfruvannyam-aes-256/
11. Belazi, A., Migallón, H. (2024). Drone-Captured Wildlife Data Encryption: A Hybrid 1D–2D Memory Cellular Automata Scheme with Chaotic Mapping and SHA-256. Mathematics, 12 (22), 3602. https://doi.org/10.3390/math12223602
12. Ozmen, M. O., Yavuz, A. A. (2018). Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones. MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM). https://doi.org/10.1109/milcom.2018.8599784
13. Eldeeb, H., Shehata, K., Shaker, N., Abdel Hafez, A. (2012). HANK-1, A new Efficient and Secure Block Cipher Algorithm for Limited Resources Devices. The International Conference on Electrical Engineering, 1–12. https://doi.org/10.21608/iceeng.2012.30662
14. Bassham, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B. et al. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-22r1a
15. Ramudu, S., Shanthi, G. (2015). Implementation of an Ultra-Lightweight Block Cipher. International Journal & Magazine of Engineering, Technology, Management and Research, 2 (2), 233–242. Available at: http://www.ijmetmr.com/olfebruary2015/SriRamudu-GShanthi-39.pdf
16. Yang, Y., Dong, H., Li, Z., Xiao, S. (2023). LWED: Lightweight white-box encryption communication system for drones over CARX algorithm. Journal of King Saud University - Computer and Information Sciences, 35 (9), 101727. https://doi.org/10.1016/j.jksuci.2023.101727
17. Yatao, Y., Ruoqing, Z., Hui, D., Yingjie, M., Xiaowei, Z. (2023). WBZUC: novel white-box ZUC-128 stream cipher. The Journal of China Universities of Posts and Telecommunications, 78 (11), 96–106. https://doi.org/10.19682/j.cnki.1005-8885.2022.0022
18. Hei, X., Song, B., Ling, C. (2017). SHIPHER: A new family of lightweight block ciphers based on dynamic operators. 2017 IEEE International Conference on Communications (ICC), 1–7. https://doi.org/10.1109/icc.2017.7996731
19. Lai, X., Massey, J. L. (1991). A Proposal for a New Block Encryption Standard. Advances in Cryptology – EUROCRYPT '90, 389–404. https://doi.org/10.1007/3-540-46877-3_35
20. Meleshko, Y., Maidanyk, O., Sobinov, O., Mynailenko, R. (2021). A Method of Encrypting the Traffic of Quadrocopters Through an A nalog Path During Monitoring of Agricultural Ground Objects. National Interagency Scientific and Technical Collection of Works. Design, Production and Exploitation of Agricultural Machines, 51, 216–226. https://doi.org/10.32515/2414-3820.2021.51.216-226
21. Myronchuk, K., Vatslavyk, O. (2017). Zabezpechennia peredachi danykh v BPLA. Available at: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/4474/1/Дроні-МИрончук-Вацлавик.pdf
22. Hell, M., Johansson, T. (2010). Security Evaluation of Stream Cipher Enocoro-128v2. CRYPTREC Technical Report. Available at: https://lup.lub.lu.se/search/files/5976181/2433492.pdf
23. Block Cipher Modes. Computer Security Resource Center. NIST. Available at: https://csrc.nist.gov/Projects/block-cipher-techniques/bcm
24. Blondeau, C., Gérard, B. (2011). Multiple Differential Cryptanalysis: Theory and Practice. Fast Software Encryption, 35–54. https://doi.org/10.1007/978-3-642-21702-9_3
25. Z'aba, M. R., Raddum, H., Henricksen, M., Dawson, E. (2008). Bit-Pattern Based Integral Attack. Fast Software Encryption, 363–381. https://doi.org/10.1007/978-3-540-71039-4_23
26. Wang, M. (2008). Differential Cryptanalysis of Reduced-Round PRESENT. Progress in Cryptology – AFRICACRYPT 2008, 40–49. https://doi.org/10.1007/978-3-540-68164-9_4

DOI: 10.15587/1729-4061.2025.339985

DEVELOPMENT OF ADAPTIVE CONGESTION CONTROL MECHANISM FOR REAL-TIME MULTIMEDIA STREAMING IN VARIABLE NETWORK CONDITION (p. 54–63)

Marvin Chandra Wijaya
Maranatha Christian University, Bandung, Indonesia
ORCID: https://orcid.org/0000-0001-5920-4348

This research focuses on real-time multimedia streaming using RTP and RTCP protocols. The main issue addressed is that standard RTP/RTCP congestion control is inadequately adapted to changing and unstable network conditions, resulting in increased packet loss, end-to-end latency, unstable bitrates, and poor video quality. A dynamic bandwidth-adaptive congestion control mechanism was developed for RTP streaming, which utilizes RTCP feedback to dynamically change the bitrate and framerate in real time during the streaming session. Controlled experiment results show that average packet loss decreases from 8.2% to 3.4%; end-to-end latency decreases from an average of 220 ms to 135 ms; and provides a more stable average bitrate than standard RTP/RTCP systems. Furthermore, this system also provides a more stable average framerate than standard RTP/RTCP systems and a higher average framerate under poor network conditions. This result can be attributed to the ability of the adaptive mechanism to continuously monitor packet loss, interference, and delays in addition to reacting immediately to conditions instead of waiting for RTCP reports to appear at fixed time intervals. A key point regarding the proposed design is the integration of bitrate and framerate to ensure smooth playback and user enjoyment with reduced risk of interruption and improved stability in dynamic and unpredictable network environments. This contribution can be practically applied in real-time applications, such as video conferencing, telemedicine, or live streaming while traversing mobile or wireless networks where conditions are always dynamic and unpredictable. The proposed method can be practically applied under unfavorable internet network conditions, which is an advantage of this method.

Keywords: adaptive system, multimedia, network congestion, real-time transport control protocol, video streaming.

References

1. Khoroshevska, I., Khoroshevskyi, O., Hrabovskyi, Y., Lukyanova, V., Zhytlova, I. (2024). Development of a multimedia training course for user self-development. Eastern-European Journal of Enterprise Technologies, 2 (2 (128)), 48–63. https://doi.org/10.15587/1729-4061.2024.302884
2. Hrabovskyi, Y., Brynza, N., Vilkhivska, O. (2020). Development of information visualization methods for use in multimedia ap-

plications. EUREKA: Physics and Engineering, 1, 3–17. https://doi.org/10.21303/2461-4262.2020.001103
3. Mohammed Jameel, S., Croock, M. S. (2020). Mobile learning architecture using fog computing and adaptive data streaming. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18 (5), 2454. https://doi.org/10.12928/telkomnika.v18i5.16712
4. Wijaya, M. C., Maksom, Z., Abdullah, M. H. L. (2022). Novel Framework for Translation Algorithms in Multimedia Authoring Tools. IAENG International Journal of Computer Science, 49 (3), 628–636. Available at: http://www.iaeng.org/IJCS/issues_v49/issue_3/IJCS_49_3_02.pdf
5. Tegou, T., Papadopoulos, A., Kalamaras, I., Votis, K., Tzovaras, D. (2019). Using Auditory Features for WiFi Channel State Information Activity Recognition. SN Computer Science, 1 (1). https://doi.org/10.1007/s42979-019-0003-2
6. Jin, F., Ma, L., Zhao, C., Liu, Q. (2024). State estimation in networked control systems with a real-time transport protocol. Systems Science & Control Engineering, 12 (1). https://doi.org/10.1080/21642583.2024.2347885
7. Muslim, A., Schmid, F., Recker, S. (2023). Latency Measurement Approach for Black Box Components in Edge Computing Environments. 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), 327–331. https://doi.org/10.1109/sist58284.2023.10223523
8. Wijaya, M. C., Maksom, Z., Abdullah, M. H. L. (2023). Auto-correction of multiple spatial conflicts in multimedia authoring tools. Bulletin of Electrical Engineering and Informatics, 12 (3), 1657–1665. https://doi.org/10.11591/eei.v12i3.4894
9. Sumtsov, D., Osiievskyi, S., Lebediev, V. (2018). Development of a method for the experimental estimation of multimedia data flow rate in a computer network. Eastern-European Journal of Enterprise Technologies, 2 (2 (92)), 56–64. https://doi.org/10.15587/1729-4061.2018.128045
10. Yermakova, I., Nikolaienko, A., Hrytsaiuk, O., Tadeieva, J., Kravchenko, P. (2024). Use a smartphone app for predicting human thermal responses in hot environment. Eastern-European Journal of Enterprise Technologies, 2 (2 (128)), 39–47. https://doi.org/10.15587/1729-4061.2024.300784
11. Wang, H., Li, J., Liu, H. (2024). Research of Technology About Video Control Based on Real-Time Transmission. 2024 IEEE 7th International Conference on Information Systems and Computer Aided Education (ICISCAE), 995–998. https://doi.org/10.1109/iciscae62304.2024.10761263
12. Zhang, S., Lei, W., Zhang, W., Guan, Y. (2019). Congestion Control for RTP Media: A Comparison on Simulated Environment. Simulation Tools and Techniques, 43–52. https://doi.org/10.1007/978-3-030-32216-8_4
13. Dai, T., Zhang, X., Zhang, Y., Guo, Z. (2020). Statistical Learning Based Congestion Control for Real-Time Video Communication. IEEE Transactions on Multimedia, 22 (10), 2672–2683. https://doi.org/10.1109/tmm.2019.2959448
14. Andrade-Zambrano, A. R., León, J. P. A., Morocho-Cayamcela, M. E., Cárdenas, L. L., de la Cruz Llopis, L. J. (2024). A Reinforcement Learning Congestion Control Algorithm for Smart Grid Networks. IEEE Access, 12, 75072–75092. https://doi.org/10.1109/access.2024.3405334
15. Perkins, C. (2023). Sending RTP Control Protocol (RTCP) Feedback for Congestion Control in Interactive Multimedia Conferences. RFC Editor. https://doi.org/10.17487/rfc9392
16. Shao, Y., Ozfatura, E., Perotti, A. G., Popović, B. M., Gündüz, D. (2023). AttentionCode: Ultra-Reliable Feedback Codes for Short-Packet Communications. IEEE Transactions on Communications, 71 (8), 4437–4452. https://doi.org/10.1109/tcomm.2023.3280563
17. Lin, Q., Han, L. (2023). Dynamic Recognition Method of Track and Field Posture Based on Mobile Monitoring Technology. Advanced Hybrid Information Processing, 336–348. https://doi.org/10.1007/978-3-031-28867-8_25
18. Rasanen, J., Altonen, A., Mercat, A., Vanne, J. (2021). Open-source RTP Library for End-to-End Encrypted Real-Time Video Streaming Applications. 2021 IEEE International Symposium on Multimedia (ISM), 92–96. https://doi.org/10.1109/ism52913.2021.00023
19. Wang, W., Li, Y., He, R. (2025). Design of real-time transmission system for underwater panoramic camera based on RTSP. PLOS ONE, 20 (3), e0320000. https://doi.org/10.1371/journal.pone.0320000
20. Pozueco, L., Pañeda, X. G., García, R., Melendi, D., Cabrero, S. (2013). Adaptable system based on Scalable Video Coding for high-quality video service. Computers & Electrical Engineering, 39 (3), 775–789. https://doi.org/10.1016/j.compeleceng.2013.01.015
21. Zubaydi, H. D., Jagmagji, A. S., Molnár, S. (2023). Experimental Analysis and Optimization Approach of Self-Clocked Rate Adaptation for Multimedia Congestion Control Algorithm in Emulated 5G Environment. Sensors, 23 (22), 9148. https://doi.org/10.3390/s23229148

DOI: 10.15587/1729-4061.2025.340994

DETERMINING THE EFFECT OF PHASE MODULATION AND OPTIMAL SIGNAL PROCESSING ON HF COMMUNICATION SYSTEM RELIABILITY AND RANGE (p. 64–81)

Yurii Honcharenko
Polissia National University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0002-2631-2956

Gennadii Golub
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
Vytautas Magnus University, Kaunas, Lithuania
ORCID: https://orcid.org/0000-0002-2388-0405

Nataliya Tsyvenkova
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-1703-4306

Ivan Poleshchuk
Polissia National University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0009-0000-6783-3013

Anatolii Denysiuk
Polissia National University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0003-4226-2394

Ivan Omarov
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9449-853X

Olena Sukmaniuk
Polissia National University, Zhytomyr, Ukraine
ORCID: https://orcid.org/0000-0003-2485-488X

This study considers analog high-frequency (HF) communication systems that use broadband signals modulated by the Barker code. The task addressed is to improve the efficiency of analog HF communication systems when transmitting broadband signals.

Patterns in the formation of a noise-resistant broadband signal with phase modulation by the Barker code and the operation of the

signal spectrum expansion and restoration unit have been investigated. It was established that phase modulation makes it possible to achieve such a spectral width, amplitude of the main peak of the autocorrelation function, and time resolution, which enable effective correlation separation of the usable signal and increases its noise immunity.

It has been shown that signal modulation with a five-bit code forms a spectrum with a width of 1 MHz, the amplitude of the main peak of the autocorrelation function is 9 units, and a time resolution of 1–2 μs, which provides an increase in noise immunity to 9 dB at S/N=1 dB compared to the base signal without modulation. The use of a thirteen-bit code allows this indicator to be increased to 13 dB at S/N=–3 dB.

The effectiveness of the module for expanding and restoring the spectrum of the modulated signal when transmitting it over a distance without loss of communication quality has been confirmed. Signal modulation with a 5- and 13-bit code, compared to unmodulated, increased the communication range by 9 and 25 times, respectively. The results are attributed to the optimal autocorrelation properties of Barker codes and hardware solutions that form a broadband signal without complicating the circuit. This is explained by the ability of Barker codes to form a narrow correlation pulse and expand the signal spectrum, which reduces sensitivity to narrowband interference.

The results are valuable for applications in analog RF communication systems as well as power grids, in particular at low S/N ratios.

Keywords: autocorrelation function, analog signal, Barker code, matched filter, phase modulation.

References

1. Giraneza, M., Abo-Al-Ez, K. (2022). Power line communication: A review on couplers and channel characterization. AIMS Electronics and Electrical Engineering, 6 (3), 265–284. https://doi.org/10.3934/electreng.2022016
2. Del Puerto-Flores, J. A., Naredo, J. L., Peña-Campos, F., Del-Valle-Soto, C., Valdivia, L. J., Parra-Michel, R. (2022). Channel Characterization and SC-FDM Modulation for PLC in High-Voltage Power Lines. Future Internet, 14 (5), 139. https://doi.org/10.3390/fi14050139
3. Girotto, M., Tonello, A. M. (2017). EMC Regulations and Spectral Constraints for Multicarrier Modulation in PLC. IEEE Access, 5, 4954–4966. https://doi.org/10.1109/access.2017.2676352
4. Fan, Z., Rudlin, J., Asfis, G., Meng, H. (2019). Convolution of Barker and Golay Codes for Low Voltage Ultrasonic Testing. Technologies, 7 (4), 72. https://doi.org/10.3390/technologies7040072
5. Ustun Ercan, S., Pena-Quintal, A., Thomas, D. (2023). The Effect of Spread Spectrum Modulation on Power Line Communications. Energies, 16 (13), 5197. https://doi.org/10.3390/en16135197
6. Hernandez Fernandez, J., Jarouf, A., Omri, A., Di Pietro, R. (2023). Inferring Power Grid Information with Power Line Communications: Review and Insights. arXiv. https://doi.org/10.48550/arXiv.2308.10598
7. Schmidt, K.-U., Willms, J. (2015). Barker sequences of odd length. Designs, Codes and Cryptography, 80 (2), 409–414. https://doi.org/10.1007/s10623-015-0104-4
8. Maksimov, V., Khrapovitsky, I. (2020). New composite barker codes in the synchronization system of broadband signals. Information and Telecommunication Sciences, 2, 24–30. https://doi.org/10.20535/2411-2976.22020.24-30
9. Maksymov, V., Noskov, V., Khrapovytsky, I. (2022). New Barker's composite codes as modulation signals in broadband communication systems. Information and Telecommunication Sciences, 2, 15–20. https://doi.org/10.20535/2411-2976.22022.15-20
10. Maksymov, V., Gatturov, V., Khrapovytsky, I. (2022). New composite Barker codes, gold codes and kasamisequences in broadband signal synchronization systems. Information and Telecommunication Sciences, 1, 14–21. https://doi.org/10.20535/2411-2976.12022.14-21
11. Abdel-Rahman, M. A. A. (2018). Generation and Digital Correlation of Barker Code for Radars and Communication Systems. IJIREEICE, 6 (9), 1–6. https://doi.org/10.17148/ijireeice.2018.691
12. Tsmots, I. G., Riznyk, O. Ya., Balych, B. I., Lvovskij, Ch. Z. (2021). The method and simulation model for the synthesis of barker-like code sequences. Ukrainian Journal of Information Technology, 3 (2), 45–50. https://doi.org/10.23939/ujit2021.02.045
13. Siebert, W. M. (1988). The early history of pulse compression radar-the development of AN/FPS-17 coded-pulse radar at Lincoln Laboratory. IEEE Transactions on Aerospace and Electronic Systems, 24 (6), 833–837. https://doi.org/10.1109/7.18655
14. Blunt, S. D., Mokole, E. L. (2016). Overview of radar waveform diversity. IEEE Aerospace and Electronic Systems Magazine, 31 (11), 2–42. https://doi.org/10.1109/maes.2016.160071
15. Zhang, Y.-X., Liu, Q.-F., Hong, R.-J., Pan, P.-P., Deng, Z.-M. (2016). A Novel Monopulse Angle Estimation Method for Wideband LFM Radars. Sensors, 16 (6), 817. https://doi.org/10.3390/s16060817
16. Seleym, A. (2016). Complementary phase coded LFM waveform for SAR. 2016 Integrated Communications Navigation and Surveillance (ICNS), 4C3-1-4C3-5. https://doi.org/10.1109/icnsurv.2016.7486346
17. Levanon, N., Cohen, I., Itkin, P. (2017). Complementary pair radar waveforms–evaluating and mitigating some drawbacks. IEEE Aerospace and Electronic Systems Magazine, 32 (3), 40–50. https://doi.org/10.1109/maes.2017.160113
18. Azouz, A., Abosekeen, A., Nassar, S., Hanafy, M. (2021). Design and Implementation of an Enhanced Matched Filter for Sidelobe Reduction of Pulsed Linear Frequency Modulation Radar. Sensors, 21 (11), 3835. https://doi.org/10.3390/s21113835
19. Liu, M., Li, Z., Liu, L. (2018). A Novel Sidelobe Reduction Algorithm Based on Two-Dimensional Sidelobe Correction Using D-SVA for Squint SAR Images. Sensors, 18 (3), 783. https://doi.org/10.3390/s18030783
20. Azouz, A. (2020). Novel Sidelobe cancellation for Compound-Barker Combined with LFM or Polyphase Waveform. 2020 12th International Conference on Electrical Engineering (ICEENG), 268–276. https://doi.org/10.1109/iceeng45378.2020.9171777
21. Saari, V. (2011). Continuous-time low-pass filters for integrated wideband radio receivers. Aalto University. Available at: https://core.ac.uk/download/pdf/80703915.pdf
22. Kiranmai, B., Rajesh Kumar, P. (2015). Performance Evaluation of Compound Barker Codes using Cascaded Mismatched Filter Technique. International Journal of Computer Applications, 121 (19), 31–34. https://doi.org/10.5120/21649-4844
23. El-Tokhy, M. A., Mansour, H. A. K. (2008). A 2.3-mW 16.7-MHZ Analog Matched Filter Circuit For DS-CDMA Wireless Applications. Progress In Electromagnetics Research B, 5, 253–264. https://doi.org/10.2528/pierb08022406
24. Haji Ali, S. M., Shaker, M. M., Salih, T. (2018). Design and implementation of a dynamic analog matched filter using FPAA technology. World Academy of Science, Engineering and Technology, 206–210. Available at: https://www.researchgate.net/publication/322683048_Design_and_Implementation_of_a_Dynamic_Analog_Matched_Filter_Using_FPAA_Technology

25. Lari, M. (2023). Matched-filter design to improve self-interference cancellation in full-duplex communication systems. Wireless Networks, 29 (7), 3137–3150. https://doi.org/10.1007/s11276-023-03352-2
26. Hahm, M. D., Friedman, E. G., Titlebaum, E. L. (1997). A comparison of analog and digital circuit implementations of low power matched filters for use in portable wireless communication terminals. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 44 (6), 498–506. https://doi.org/10.1109/82.592584
27. Angarita Malaver, E. F., Barrera Lombana, N., Moreno Rubio, J. J. (2024). Smith Chart-Based Design of High-Frequency Broadband Power Amplifiers. Electronics, 13 (20), 4096. https://doi.org/10.3390/electronics13204096
28. Chen, S., Sun, H., Weng, M., Wen, S., Li, L., Liu, B. (2023). Design and Research of Channel Circuit Based on Broadband Power Line Carrier. Journal of Physics: Conference Series, 2433 (1), 012017. https://doi.org/10.1088/1742-6596/2433/1/012017
29. Thakur, S., Singh, R., Sharma, S. (2015). Dynamic Capacity Scheduling in Hadoop. International Journal of Computer Applications, 125 (15), 25–28. https://doi.org/10.5120/ijca2015906178
30. Qian, N., Zhou, D., Shu, H., Zhang, M., Wang, X., Dai, D. et al. (2025). Analog parallel processor for broadband multifunctional integrated system based on silicon photonic platform. Light: Science & Applications, 14 (1). https://doi.org/10.1038/s41377-025-01753-w
31. Oluwajobi, F., Wasiu, L. (2014). Multisim Design and Simulation of 2.2GHz LNA for Wireless Communication. International Journal of VLSI Design & Communication Systems, 5 (4), 65–74. https://doi.org/10.5121/vlsic.2014.5405
32. Li, Z., Li, X., Jiang, D., Bao, X., He, Y. (2020). Application of Multisim Simulation Software in Teaching of Analog Electronic Technology. Journal of Physics: Conference Series, 1544 (1), 012063. https://doi.org/10.1088/1742-6596/1544/1/012063
33. Berkman, L. N., Varfolomeieva, O. H., Hrushevska, V. P. (2015). Typovi syhnaly ta zavady v elektrozviazku. Kyiv: DUT NNITI, 92.
34. Galli, S., Logvinov, O. (2008). Recent Developments in the Standardization of Power Line Communications within the IEEE. IEEE Communications Magazine, 46 (7), 64–71. https://doi.org/10.1109/mcom.2008.4557044
35. Ndjiongue, A. R., Ferreira, H. C. (2019). Power line communications (PLC) technology: More than 20 years of intense research. Transactions on Emerging Telecommunications Technologies, 30 (7). https://doi.org/10.1002/ett.3575
36. Ustun Ercan, S. (2024). Power line Communication: Revolutionizing data transfer over electrical distribution networks. Engineering Science and Technology, an International Journal, 52, 101680. https://doi.org/10.1016/j.jestch.2024.101680
37. Balashov, V. O., Vorobienko, P. P., Liakhovetskyi, L. M., Pediash, V. V. (2012). Systemy peredavannia shyrokosmuhovymy syhnalamy. Odesa: Vyd. tsentr ONAZ im. O.S. Popova, 336. Available at: https://duikt.edu.ua/uploads/l_412_70653078.pdf

DOI: 10.15587/1729-4061.2025.340990

DEVELOPMENT OF A STRATOSPHERIC AIRSHIP-BASED NETWORK ARCHITECTURE FOR TELECOMMUNICATION IN REMOTE AREAS (p. 82–92)

Mukhit Abdullayev
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0002-3349-1881

Ainur Kuttybayeva
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-7281-3690

Kalmukhamed Tazhen
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0004-5890-5328

Anar Khabay
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0409-1531

Nurzhamal Ospanova
International IT University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1170-4794

Yerlan Tashtay
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0809-537X

Arnur Sabyrbayev
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0007-6768-2412

Iliyas Samat
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-9441-3783

Rimma Abdykadyrqyzy
Ministry of Science and Higher Education of the Republic of Kazakhstan, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0009-1935-2536

Daria Zhumakhanova
Shakarim University, Semey, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-2459-4822

The object of this study is a stratospheric airship-based telecommunication platform, employed as a high-altitude platform station (HAPS), designed to operate at altitudes of 20–30 km and provide broadband connectivity in regions with limited terrestrial infrastructure such as rural and remote areas of the Republic of Kazakhstan. The key research problem is to ensure stable connectivity of HAPS-based telecommunication platforms under strong stratospheric winds, with limited payload capacity and energy resources, while developing a scalable network architecture for multi-airship coordination.

This paper proposes a network concept based on modular nano-airships, which reduces drag, enhances maintainability, and ensures continuous service. Calculations of lifting capacity, aerodynamic drag of different envelope shapes, energy balance, and the coverage radius of a single station were performed. Experimental tests of a prototype confirmed the feasibility of using the sub-GHz band (433 MHz) to provide long-range communication under ground test conditions, where signal attenuation was found to be minimal compared to higher frequencies.

Due to the obtained characteristics, the hypothesis of employing a group of smaller airships instead of a single large carrier was confirmed. This is explained by their reduced sensitivity to wind loads, flexibility in network configuration, and lower operational risks. Unlike traditional satellite systems, which are expensive to launch and maintain, stratospheric airships can be recovered, repaired, and redeployed at relatively low cost, offering an economically viable solution for developing regions.

The results can be applied in the creation of national communication networks for remote and sparsely populated areas of the Republic of Kazakhstan, in emergency response operations, and as a comple-

mentary layer to satellite constellations. The proposed concept demonstrates that modular HAPS networks are a realistic and scalable alternative, capable of providing broadband access under real-world atmospheric and geographic constraints.

Keywords: high-altitude platform stations (HAPS), stratospheric airship, telecommunication network, LoRa technology, sub-GHz frequency.

References

1. Abdullaev, M., Esnazarov, E. (2012). Organization of Broadband Communication Based on Stratospheric High-Altitude Platforms in the Territory of Kazakhstan. Information and Telecommunication Technologies: Education, Science, Practice, 232–236.
2. Abdykadyrov, A., Abdullayev, M., Kuttybayeva, A., Tazhen, K., Kystaubayev, N., Ermekbayev, M. et al. (2025). Development and evaluation of radio frequency management approaches for stratospheric communication systems. Eastern-European Journal of Enterprise Technologies, 3 (5 (135)), 17–29. https://doi.org/10.15587/1729-4061.2025.331607
3. Widiawan, A. K., Tafazolli, R. (2006). High Altitude Platform Station (HAPS): A Review of New Infrastructure Development for Future Wireless Communications. Wireless Personal Communications, 42 (3), 387–404. https://doi.org/10.1007/s11277-006-9184-9
4. D'Oliveira, F. A., Melo, F. C. L. de, Devezas, T. C. (2016). High-Altitude Platforms - Present Situation and Technology Trends. Journal of Aerospace Technology and Management, 8 (3), 249–262. https://doi.org/10.5028/jatm.v8i3.699
5. Karapantazis, S., Pavlidou, F. (2005). Broadband communications via high-altitude platforms: A survey. IEEE Communications Surveys & Tutorials, 7 (1), 2–31. https://doi.org/10.1109/comst.2005.1423332
6. Alexandre, L. C., Linhares, A., Neto, G., Sodre, A. C. (2021). High-Altitude Platform Stations as IMT Base Stations: Connectivity from the Stratosphere. IEEE Communications Magazine, 59 (12), 30–35. https://doi.org/10.1109/mcom.001.2100477
7. Abbasi, O., Yadav, A., Yanikomeroglu, H., Đào, N.-D., Senarath, G., Zhu, P. (2024). HAPS for 6G Networks: Potential Use Cases, Open Challenges, and Possible Solutions. IEEE Wireless Communications, 31 (3), 324–331. https://doi.org/10.1109/mwc.012.2200365
8. Lou, Z., Youcef Belmekki, B. E., Alouini, M.-S. (2023). HAPS in the Non-Terrestrial Network Nexus: Prospective Architectures and Performance Insights. IEEE Wireless Communications, 30 (6), 52–58. https://doi.org/10.1109/mwc.004.2300198
9. Arum, S. C., Grace, D., Mitchell, P. D. (2020). A review of wireless communication using high-altitude platforms for extended coverage and capacity. Computer Communications, 157, 232–256. https://doi.org/10.1016/j.comcom.2020.04.020
10. Tang, J., Xie, W., Zhou, P., Yang, H., Zhang, T., Wang, Q. (2023). Multidisciplinary Optimization and Analysis of Stratospheric Airships Powered by Solar Arrays. Aerospace, 10 (1), 43. https://doi.org/10.3390/aerospace10010043
11. Dumas, A., Pancaldi, F., Anzillotti, F., Trancossi, M. (2009). High Altitude Platforms for Telecommunications: Design Methodology. SAE Technical Paper Series, 1. https://doi.org/10.4271/2009-01-3159
12. Trancossi, M. (2020). High Altitude Platform System Airship for Telecommunication and Border Monitoring Design and Physical Model. SAE Technical Paper Series. https://doi.org/10.4271/2020-01-0044
13. Gong, W., Zhang, Y., Zhu, M., Chen, T., Zheng, Z. (2025). Dynamic control of multiple stratospheric airships in time-varying wind fields for communication coverage missions. Aerospace Science and Technology, 166, 110514. https://doi.org/10.1016/j.ast.2025.110514
14. Luo, Q., Sun, K., Chen, T., Zhang, Y., Zheng, Z. (2024). Trajectory planning of stratospheric airship for station-keeping mission based on improved rapidly exploring random tree. Advances in Space Research, 73 (1), 992–1005. https://doi.org/10.1016/j.asr.2023.10.002
15. Song, K., Li, Z., Zhang, Y., Wang, X., Xu, G., Zhang, X. (2023). Power Generation Calculation Model and Validation of Solar Array on Stratospheric Airships. Energies, 16 (20), 7106. https://doi.org/10.3390/en16207106
16. Ning, X., Liu, P., Pan, Z. (2021). The Mechanical Characteristics and Experimental Study of the Stratospheric Airship. Journal of Applied Mathematics and Physics, 09 (01), 183–196. https://doi.org/10.4236/jamp.2021.91013
17. Ilcev, St. D. (2011). Stratospheric communication platforms as an alternative for space program. Aircraft Engineering and Aerospace Technology, 83 (2), 105–111. https://doi.org/10.1108/00022661111120999
18. Ilcev, D. S. (2016). Development of Airships Stratospheric Platform Systems (SPS). 2016 UBT International Conference, 65–75. https://doi.org/10.33107/ubt-ic.2016.54
19. Bagarić, T., Rezo, Z., Steiner, S. (2025). High-Altitude Pseudo-Satellite platforms as support to air traffic management. Transportation Research Procedia, 83, 593–600. https://doi.org/10.1016/j.trpro.2025.03.030
20. Chen, Z., Miao, M., Wu, H. (2025). Operational Effectiveness Evaluation of Stratospheric Airship Anti-stealth Penetration. Mechanical Design and Simulation: Exploring Innovations for the Future, 1283–1292. https://doi.org/10.1007/978-981-97-7887-4_113
21. Chu, Y., Donaldson, R., Kumar, R., Grace, D. (2021). Feasibility of quantum key distribution from high altitude platforms. Quantum Science and Technology, 6 (3), 035009. https://doi.org/10.1088/2058-9565/abf9ae
22. Hokazono, Y., Kishiyama, Y., Asai, T. (2022). Studies toward Practical Application of HAPS in the Space RAN. NTT Technical Review, 20 (12), 28–35. https://doi.org/10.53829/ntr202212fa3
23. Zhou, D., Gao, S., Liu, R., Gao, F., Guizani, M. (2020). Overview of development and regulatory aspects of high altitude platform system. Intelligent and Converged Networks, 1 (1), 58–78. https://doi.org/10.23919/icn.2020.0004
24. Skalski, P. (2021). Design and Energy Systems of Stratospheric Airships. 2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace), 13–18. https://doi.org/10.1109/metroaerospace51421.2021.9511752
25. Holis, J., Pechac, P. (2008). Elevation Dependent Shadowing Model for Mobile Communications via High Altitude Platforms in Built-Up Areas. IEEE Transactions on Antennas and Propagation, 56 (4), 1078–1084. https://doi.org/10.1109/tap.2008.919209
26. Dovis, F., Lo Presti, L., Mulassano, P. (2005). Support infrastructures based on high altitude platforms for navigation satellite systems. IEEE Wireless Communications, 12 (5), 106–112. https://doi.org/10.1109/mwc.2005.1522113
27. Taissariyeva, K. N., Ilipbaeva, L., Dzhobalaeva, G. (2016). Researching the method of providing harmonicity to multi-level inverter. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2016, 10031, 1003123. https://doi.org/10.1117/12.2249145

DOI: 10.15587/1729-4061.2025.340833

PREDICTING ROBOTIC PLATFORM MISSIONS USING A KERNEL ACTIVATION NETWORK WITH AN ASYMMETRIC KERNEL (p. 93–103)

Oleksandr Laktionov
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0002-5230-524X

Alina Yanko
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0003-2876-9316

Bohdan Boriak
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0000-0002-8114-7930

Oleksii Mykhailichenko
National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
ORCID: https://orcid.org/0009-0009-3512-0030

This study considers those processes predicting the functional efficiency of robotic platforms that affect the optimization of their mission planning. Given the growing demand for autonomous mobile systems, a critical task is to ensure high efficiency of their dynamics under different loads, terrains, and speeds, which requires reliable tools for decision-making even before physical launch.

To solve the task, a method based on a customized Kernel Activation Network (KAN) was devised and programmatically implemented to predict the functional efficiency of the platform. The results demonstrate a significant increase in accuracy: KAN achieves an MSE of 0.00055727 on synthetic data and 0.00041720 on the experimental sample, while other architectures demonstrate 0.00105989 and higher.

The key innovation of KAN is the use of an asymmetric chi-square kernel in parallel with the Gaussian kernel, as well as the integration of input estimates that take into account the triple interaction of factors. This explains the network's ability to effectively capture complex nonlinear dependences between numerous platform parameters (rolling resistance, aerodynamic drag, climbing force, etc.) and environmental conditions. The use of an asymmetric kernel significantly simplifies the network architecture, allowing for high accuracy at lower computational complexity.

In practice, the results serve as an additional tool for optimizing mission planning of robotic platforms. This makes it possible to optimize equipment selection, construct strategic logistics routes, and increase the safety and reliability of autonomous systems under actual conditions. The achieved Technology Readiness Level is 4.

Keywords: functional prediction, factor interaction, asymmetric kernel, neural network, robotic platform.

References

1. Yanko, A., Pedchenko, N., Kruk, O. (2024). Enhancing the protection of automated ground robotic platforms in the conditions of radio electronic warfare. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 6, 136–142. https://doi.org/10.33271/nvngu/2024-6/136
2. Papadopoulos, C., Mitridis, D., Yakinthos, K. (2022). Conceptual Design of a Novel Unmanned Ground Effect Vehicle (UGEV) and Flow Control Integration Study. Drones, 6 (1), 25. https://doi.org/10.3390/drones6010025
3. Yanko, A., Krasnobayev, V., Martynenko, A. (2023). Influence of the number system in residual classes on the fault tolerance of the computer system. Radioelectronic and Computer Systems, 3, 159–172. https://doi.org/10.32620/reks.2023.3.13
4. Krasnobayev, V., Yanko, A., Kovalchuk, D. (2023). Control, Diagnostics and Error Correction in the Modular Number System. Computer Modeling and Intelligent Systems, 3392, 199–213. https://doi.org/10.32782/cmis/3392-17
5. Trujillo, J.-C., Munguia, R., Grau, A. (2021). Aerial Cooperative SLAM for Ground Mobile Robot Path Planning. The 8th International Symposium on Sensor Science, 65. https://doi.org/10.3390/i3s2021dresden-10164
6. Asiminari, G., Moysiadis, V., Kateris, D., Busato, P., Wu, C., Achillas, C. et al. (2024). Integrated Route-Planning System for Agricultural Robots. AgriEngineering, 6 (1), 657–677. https://doi.org/10.3390/agriengineering6010039
7. Yu, S., Hirche, M., Huang, Y., Chen, H., Allgöwer, F. (2021). Model predictive control for autonomous ground vehicles: a review. Autonomous Intelligent Systems, 1 (1). https://doi.org/10.1007/s43684-021-00005-z
8. Macaulay, M. O., Shafiee, M. (2022). Machine learning techniques for robotic and autonomous inspection of mechanical systems and civil infrastructure. Autonomous Intelligent Systems, 2 (1). https://doi.org/10.1007/s43684-022-00025-3
9. Rybczak, M., Popowniak, N., Lazarowska, A. (2024). A Survey of Machine Learning Approaches for Mobile Robot Control. Robotics, 13 (1), 12. https://doi.org/10.3390/robotics13010012
10. Golub, V., Bisyk, S., Golub, G., Tsyvenkova, N., Sedov, S., Nadykto, V. et al. (2025). Devising a method for categorizing combat wheeled vehicles using fuzzy cluster analysis. Eastern-European Journal of Enterprise Technologies, 2 (1 (134)), 13–21. https://doi.org/10.15587/1729-4061.2025.324546
11. Laktionov, O., Yanko, A., Pedchenko, N. (2024). Identification of air targets using a hybrid clustering algorithm. Eastern-European Journal of Enterprise Technologies, 5 (4 (131)), 89–95. https://doi.org/10.15587/1729-4061.2024.314289
12. Barus, E. S., Zarlis, M., Nasution, Z., Sutarman, S. (2025). Development of machine learning for forecasting optimization implemented in morphology plant growth. Eastern-European Journal of Enterprise Technologies, 3 (2 (135)), 42–53. https://doi.org/10.15587/1729-4061.2025.331745
13. Harumy, H. F., Ginting, D. S., Manik, F. Y., Yel, M. B. (2025). Dominant disaster detection and prediction in coastal areas using neural network system to optimize disaster management in coastal areas. Eastern-European Journal of Enterprise Technologies, 2 (2 (134)), 6–16. https://doi.org/10.15587/1729-4061.2025.321966
14. Laktionov, A. (2021). Improving the methods for determining the index of quality of subsystem element interaction. Eastern-European Journal of Enterprise Technologies, 6 (3 (114)), 72–82. https://doi.org/10.15587/1729-4061.2021.244929
15. Bai, Y. (2022). RELU-Function and Derived Function Review. SHS Web of Conferences, 144, 02006. https://doi.org/10.1051/shsconf/202214402006
16. Bolohin, A., Bolohina, Y., Tymchuk, Y. (2025). Ranking of the technical condition of aircraft according to the diagnostic data of the glider design. System Research and Information Technologies, 2, 98–105. https://doi.org/10.20535/srit.2308-8893.2025.2.06

17. Hryshchuk, O., Zagorodnyuk, S. (2025). Managing energy consumption in FPGA-based edge computing systems with soft-core CPUs. Journal of Edge Computing, 4 (1), 57–72. https://doi.org/10.55056/jec.717
18. Kumar Malik, M., Joshi, H., Swaroop, A. (2025). An Effective Hybrid HBA-MAO for Task Scheduling with a Hybrid Fault-Tolerant Approach in Cloud Environment. International Journal of Image, Graphics and Signal Processing, 17 (4), 68–86. https://doi.org/10.5815/ijigsp.2025.04.05
19. Sveshnikov, S., Bocharnikov, V., Mudrak, Y. (2024). Evaluation and choice of an anti-aircraft missile system under uncertain conditions based on fuzzy-integral calculus and hierarchical cluster analysis. Operations Research and Decisions, 34 (2). https://doi.org/10.37190/ord240209
20. Lutsyk, Y., Parkhomenko, P., Demeniev, O., Alimov, D. (2023). Analysis of the defense planning system based on the capabilities taking into account the leading experience of NATO member states. Modern Economics, 41, 73–78. https://doi.org/10.31521/modecon.v41(2023)-11
21. Manziuk, E. (2022). Intelligent information technology for obtaining trust decisions based on the ontology of trust in a human-centered approach. Computer Systems and Information Technologies, 1, 83–88. https://doi.org/10.31891/csit-2022-1-11
22. Volkov, V., Taran, I., Volkova, T., Pavlenko, O., Berezhnaja, N. (2020). Determining the efficient management system for a specialized transport enterprise. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 4, 185–191. https://doi.org/10.33271/nvngu/2020-4/185
23. Bazarnyi, S., Husak, Y., Voitko, T., Aliew, F., Yevseiev, S. (2025). Mathematical model of multi-domain interaction based on game theory. Advanced Information Systems, 9 (3), 22–31. https://doi.org/10.20998/2522-9052.2025.3.03
24. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko, E. (2018). Influence of diagnostics errors on safety: Indicators and requirements. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 53–57. https://doi.org/10.1109/dessert.2018.8409098
25. Yanko, A., Hlushko, A., Onyshchenko, S., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and Cyber Security, 30–58. https://doi.org/10.15587/978-617-7319-98-5.ch2
26. Jarema, R. (2018). 10 Steps to Choosing the Right Motors for Your Robotic Project. Husarion Blog, Medium. Available at: https://medium.com/husarion-blog/10-steps-to-choosing-the-right-motors-for-your-robotic-project-bf5c4b997407
27. Larminie, J., Lowry, J. (2012). Electric Vehicle Technology Explained. John Wiley & Sons. https://doi.org/10.1002/9781118361146
28. MinMaxScaler. Scikit-learn developers. Available at: https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.MinMaxScaler.html
29. StandardScaler. Scikit-learn developers. Available at: https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.StandardScaler.html
30. Berrar, D. (2019). Cross-Validation. Encyclopedia of Bioinformatics and Computational Biology, 542–545. https://doi.org/10.1016/b978-0-12-809633-8.20349-x
31. BRouter-Web. BRouter. Available at: https://brouter.de/brouter-web
32. torch. PyPI. Available at: https://pypi.org/project/torch/
33. Netron. Netron developers. Available at: https://netron.app/
34. Onyshchenko, S., Zhyvylo, Y., Hlushko, A., Bilko, S. (2024). Cyber risk management technology to strengthen the information security of the national economy. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 5, 136–142. https://doi.org/10.33271/nvngu/2024-5/136

DOI: 10.15587/1729-4061.2025.340033

DESIGN AND IMPLEMENTATION OF DISK-BASED GRAPH FEATURE PREPROCESSOR FOR TERRORIST FINANCING DETECTION (p. 104–116)

Aigerim Bolshibayeva
International IT University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1191-4249

Sabina Rakhmetulayeva
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-4678-7964

Aliya Kulbayeva
International IT University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0002-7245-8312

Ansar-Ul-Haque Yasar
Hasselt University, Diepenbeek, Belgium
ORCID: https://orcid.org/0000-0002-1542-2658

The object of the study is streaming payment transactions modeled as directed multigraphs. This study investigates terrorism-financing detection in payment transaction networks using disk-based graph processing and anomaly detection. The key problem addressed is the high memory consumption of graph-based detectors, which prevents analysis on systems with limited Random Access Memory, typical of small and mid-sized financial institutions.

A disk-based graph feature preprocessor (DGFP) was made to get around this problem. During stream processing, DGFP dynamically labels connected components and identifies eight graph patterns characteristic of terrorist financing, including fan-in/fan-out stars and multi-hop chains. The system persists component descriptors to a columnar store on an SSD and uses an LRU-managed hot cache to serve the features, enabling real-time transaction scoring with sub-second latency.

On a two-million-transaction AMLSim stream, the system integrates with a lightweight Isolation Forest and achieves an F1-score of 0.76 while reducing peak RAM from 18.3 GB to 9.8 GB and maintaining 410 ± 15 ms mean latency for 10 000 transactions. Per-motif computation remains ≤ 28.4 ms (median < 24 ms), supporting real-time scoring on commodity hardware.

DGFP produces model-agnostic graph features that interoperate with standard anomaly detectors without retraining GNNs.

Contributions of this research include an external memory architecture for streaming graph feature extraction; a motif-aware feature labeling scheme stored on SSD and cached by LRU; and an empirical evaluation demonstrating real-time performance and memory efficiency improvements on anti-money laundering data.

Keywords: terrorism-financing, graph processing, external-memory algorithms, anomaly detection, compliance.

References

1. Money Laundering. Terrorist Financing. United Nations Office on Drugs and Crime. Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html
2. Crowdfunding for terrorism financing (2023). Financial Action Task Force. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/

reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf
3. U.S. Department of the Treasury. Available at: https://home.treasury.gov/
4. Opportunities and Challenges of New Technologies for AML/CFT (2021). Financial Action Task Force. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf
5. Anti-money laundering and countering the financing of terrorism at EU level. European Commission. Available at: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en
6. Thakkar, H., Datta, S., Bhadra, P., Dabhade, S. B., Barot, H., Junare, S. O. (2024). Mapping the Knowledge Landscape of Money Laundering for Terrorism Financing: A Bibliometric Analysis. Journal of Risk and Financial Management, 17 (10), 428. https://doi.org/10.3390/jrfm17100428
7. Altman, J., Blanuša, J., von Niederhäusern, L., Egressy, B., Anghel, A., Atasu, K. (2023). Realistic Synthetic Financial Transactions for Anti-Money Laundering Models. arXiv. https://doi.org/10.48550/arXiv.2306.16424
8. Alarab, I., Prakoonwit, S., Nacer, M. I. (2020). Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain. Proceedings of the 2020 5th International Conference on Machine Learning Technologies, 23–27. https://doi.org/10.1145/3409073.3409080
9. Cardoso, M., Saleiro, P., Bizarro, P. (2022). LaundroGraph: Self-Supervised Graph Representation Learning for Anti-Money Laundering. Proceedings of the Third ACM International Conference on AI in Finance, 130–138. https://doi.org/10.1145/3533271.3561727
10. Deprez, B., Vanderschueren, T., Baesens, B., Verdonck, T., Verbeke, W. (2024). Network Analytics for Anti-Money Laundering -- A Systematic Literature Review and Experimental Evaluation. arXiv. https://doi.org/10.48550/arXiv.2405.19383
11. Egressy, B., Von Niederhäusern, L., Blanuša, J., Altman, E., Wattenhofer, R., Atasu, K. (2024). Provably Powerful Graph Neural Networks for Directed Multigraphs. Proceedings of the AAAI Conference on Artificial Intelligence, 38 (10), 11838–11846. https://doi.org/10.1609/aaai.v38i10.29069
12. Mohan, A., P. V., K., Sankar, P., Maya Manohar, K., Peter, A. (2022). Improving anti-money laundering in bitcoin using evolving graph convolutions and deep neural decision forest. Data Technologies and Applications, 57 (3), 313–329. https://doi.org/10.1108/dta-06-2021-0167
13. Lo, W. W., Kulatilleke, G. K., Sarhan, M., Layeghy, S., Portmann, M. (2023). Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin. Applied Intelligence, 53 (16), 19406–19417. https://doi.org/10.1007/s10489-023-04504-9
14. Motie, S., Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. Expert Systems with Applications, 240, 122156. https://doi.org/10.1016/j.eswa.2023.122156
15. Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv. https://doi.org/10.48550/arXiv.1908.02591
16. Asiri, A., Somasundaram, K. (2025). Graph convolution network for fraud detection in bitcoin transactions. Scientific Reports, 15 (1). https://doi.org/10.1038/s41598-025-95672-w
17. Soria Quijaite, J. J., Segura Peña, L. V., Loayza Abal, R. I. (2024). Machine Learning Models for Money Laundering Detection in Financial Institutions. A Systematic Literature Review. Proceedings of the 22nd LACCEI International Multi-Conference for Engineering, Education and Technology (LACCEI 2024): "Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0." https://doi.org/10.18687/laccei2024.1.1.1682
18. Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. The Innovation, 2 (4), 100176. https://doi.org/10.1016/j.xinn.2021.100176
19. Anti-money laundering and combating financing of terrorism framework (2020). European Investment Bank. https://doi.org/10.2867/941947
20. AI Fraud Detection in Banking. IBM. Available at: https://www.ibm.com/think/topics/ai-fraud-detection-in-banking
21. Bhatia, S., Liu, R., Hooi, B., Yoon, M., Shin, K., Faloutsos, C. (2022). Real-Time Anomaly Detection in Edge Streams. ACM Transactions on Knowledge Discovery from Data, 16 (4), 1–22. https://doi.org/10.1145/3494564
22. Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Dogan, H., Aksu, G. (2023). Enhancing Anti-Money Laundering: Development of a Synthetic Transaction Monitoring Dataset. 2023 IEEE International Conference on E-Business Engineering (ICEBE), 47–54. https://doi.org/10.1109/icebe59045.2023.00028
23. Altman, E. (2019). IBM Transactions for Anti Money Laundering (AML). Available at: https://www.kaggle.com/datasets/ealtman2019/ibm-transactions-for-anti-money-laundering-aml
24. Li, M., Jia, L., Su, X. (2025). Global-local graph attention with cyclic pseudo-labels for bitcoin anti-money laundering detection. Scientific Reports, 15 (1). https://doi.org/10.1038/s41598-025-08365-9
25. Rakhmetulayeva, S., Kulbayeva, A., Bolshibayeva, A., Serbin, V. (2025). Identifying the graph-based typology features for machine learning models in financial fraud detection. Eastern-European Journal of Enterprise Technologies, 3 (9 (135)), 40–54. https://doi.org/10.15587/1729-4061.2025.327410
26. Urmashev, B., Buribayev, Z., Amirgaliyeva, Z., Ataniyazova, A., Zhassuzak, M., Turegali, A. (2021). Development of a weed detection system using machine learning and neural network algorithms. Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 70–85. https://doi.org/10.15587/1729-4061.2021.246706
27. Isolauri, E. A., Ameer, I. (2022). Money laundering as a transnational business phenomenon: a systematic review and future agenda. Critical Perspectives on International Business, 19 (3), 426–468. https://doi.org/10.1108/cpoib-10-2021-0088
28. Gaviyau, W., Sibindi, A. B. (2023). Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique. Journal of Risk and Financial Management, 16 (7), 313. https://doi.org/10.3390/jrfm16070313
29. Ercanbrack, J. G. (2024). Hawala in criminal court: the role of law and commercial culture in informal financial exchange. Crime, Law and Social Change, 82 (3), 659–683. https://doi.org/10.1007/s10611-024-10162-w
30. Farber, S., Yehezkel, S. A. (2024). Financial Extremism: The Dark Side of Crowdfunding and Terrorism. Terrorism and Political Violence, 37 (5), 651–670. https://doi.org/10.1080/09546553.2024.2362665
31. Rocha-Salazar, J.-J., Segovia-Vargas, M.-J., Camacho-Miñano, M.-M. (2021). Money laundering and terrorism financing detection using

neural networks and an abnormality indicator. Expert Systems with Applications, 169, 114470. https://doi.org/10.1016/j.eswa.2020.114470

32. Akartuna, E. A., Johnson, S. D., Thornton, A. (2024). Motivating a standardised approach to financial intelligence: a typological scoping review of money laundering methods and trends. Journal of Experimental Criminology. https://doi.org/10.1007/s11292-024-09623-y
33. Bolshibayeva, A., Rakhmetulayeva, S., Ukibassov, B., Zhanabekov, Z. (2024). Advancing real-time echocardiographic diagnosis with a hybrid deep learning model. Eastern-European Journal of Enterprise Technologies, 6 (9 (132)), 60–70. https://doi.org/10.15587/1729-4061.2024.314845
34. Rakhmetulayeva, S., Ukibassov, B., Zhanabekov, Z., Bolshibayeva, A. (2024). Development of data-efficient training techniques for detection and segmentation models in atrial septum defect analysis. Eastern-European Journal of Enterprise Technologies, 5 (2 (131)), 13–23. https://doi.org/10.15587/1729-4061.2024.312621

DOI: 10.15587/1729-4061.2025.340493

AN INTERPRETABLE ECG-BASED APPROACH FOR DETECTING HEMODYNAMICALLY SIGNIFICANT ARRHYTHMIAS USING LIGHTWEIGHT MACHINE LEARNING MODELS (p. 117–124)

Ainur Bekbay
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-7963-7439

Lashin Bazarbay
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-8694-8622

Zhanar Bigaliyeva
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-7440-5591

Vinera Baiturganova
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0007-1717-5041

Akezhan Sabibolda
Institute of Mechanics and Mechanical Engineering named after Academician U. A. Dzholdasbekov, Almaty, Republic of Kazakhstan
Almaty Academy of Ministry of Internal Affairs, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-1186-7940

Yersaiyn Mailybayev
International University of Transportation and Humanities, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-1977-3690

Nurzhigit Smailov
Institute of Mechanics and Mechanical Engineering named after Academician U. A. Dzholdasbekov, Almaty, Republic of Kazakhstan
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-7264-2390

The object of this study is the diagnostic process of patients with suspected hemodynamically significant arrhythmia in emergency and telemedicine settings, where rapid and interpretable decision support is required. The problem addressed is the limited access to echocardiographic assessment in emergency and resource-constrained environments, where interpretable and computationally efficient alternatives are urgently needed, particularly for mobile and field-deployed applications.

The main results show that machine learning models, such as XGBoost, achieved strong diagnostic performance (F1-score = 0.84, AUC = 0.91), while rule-based classifiers provided clinically interpretable accuracy. These results enabled partial compensation for the absence of echocardiography and contributed to reliable triage in acute and time-sensitive settings.

This effectiveness stems from key features of the method: reliance on interpretable ECG features (tQRS, tRR, HR, and EF derived from tQRS/tRR) and low computational complexity, setting it apart from more opaque deep learning methods. The results are explained by the strong correlation between these features and both electrical and mechanical heart function, enabling hemodynamic assessment without imaging. This supports clinical trust in the algorithm's outputs.

The proposed approach is applicable in primary screening, emergency triage, telemedicine, and remote monitoring, combining accuracy with explainability and autonomy from imaging tools. Therefore, research on interpretable ECG-based detection of hemodynamically significant arrhythmias remains highly relevant, especially in settings lacking access to specialized diagnostics.

Keywords: ECG-based EF estimation, ejection fraction, machine learning, ECG classification, tQRS/tRR ratio.

References

1. Hannun, A. Y., Rajpurkar, P., Haghpanahi, M., Tison, G. H., Bourn, C., Turakhia, M. P., Ng, A. Y. (2019). Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. Nature Medicine, 25 (1), 65–69. https://doi.org/10.1038/s41591-018-0268-3
2. Ribeiro, A. H., Ribeiro, M. H., Paixão, G. M. M., Oliveira, D. M., Gomes, P. R., Canazart, J. A. et al. (2020). Automatic diagnosis of the 12-lead ECG using a deep neural network. Nature Communications, 11 (1). https://doi.org/10.1038/s41467-020-15432-4
3. Attia, Z. I., Kapa, S., Lopez-Jimenez, F., McKie, P. M., Ladewig, D. J., Satam, G. et al. (2019). Screening for cardiac contractile dysfunction using an artificial intelligence–enabled electrocardiogram. Nature Medicine, 25 (1), 70–74. https://doi.org/10.1038/s41591-018-0240-2
4. Eleyan, A., Alboghbaish, E. (2024). Electrocardiogram Signals Classification Using Deep-Learning-Based Incorporated Convolutional Neural Network and Long Short-Term Memory Framework. Computers, 13 (2), 55. https://doi.org/10.3390/computers13020055
5. Goto, S., Kimura, M., Katsumata, Y., Goto, S., Kamatani, T., Ichihara, G. et al. (2019). Artificial intelligence to predict needs for urgent revascularization from 12-leads electrocardiography in emergency patients. PLOS ONE, 14 (1), e0210103. https://doi.org/10.1371/journal.pone.0210103
6. Alamatsaz, N., Tabatabaei, L. S., Yazdchi, M., Payan, H., Alamatsaz, N., Nasimi, F. (2022). A lightweight hybrid CNN-LSTM model for ECG-based arrhythmia detection. arXiv. https://doi.org/10.48550/arXiv.2209.00988
7. Li, Q., Rajagopalan, C., Clifford, G. D. (2014). A machine learning approach to multi-level ECG signal quality classification. Computer Methods and Programs in Biomedicine, 117 (3), 435–447. https://doi.org/10.1016/j.cmpb.2014.09.002
8. Acharya, U. R., Fujita, H., Lih, O. S., Hagiwara, Y., Tan, J. H., Adam, M. (2017). Automated detection of arrhythmias using different intervals of tachycardia ECG segments with convolutional neural network. Information Sciences, 405, 81–90. https://doi.org/10.1016/j.ins.2017.04.012

9. Samet, P. (1973). Hemodynamic Sequelae of Cardiac Arrhythmias. Circulation, 47 (2), 399–407. https://doi.org/10.1161/01.cir.47.2.399
10. Acharya, U. R., Fujita, H., Oh, S. L., Hagiwara, Y., Tan, J. H., Adam, M. (2017). Application of deep convolutional neural network for automated detection of myocardial infarction using ECG signals. Information Sciences, 415-416, 190–198. https://doi.org/10.1016/j.ins.2017.06.027
11. Mailybayev, Y., Muratbekova, G., Altayeva, Z., Zhatkanbayev, O. (2022). Development of models and improvement of methods for formalization of design problems and automating technical and operational works of railway stations. Eastern-European Journal of Enterprise Technologies, 4 (3 (118)), 6–16. https://doi.org/10.15587/1729-4061.2022.263167
12. Annam, J. R., Surampudi, B. R. (2016). Inter-patient heart-beat classification using complete ECG beat time series by alignment of R-peaks using SVM and decision rule. 2016 International Conference on Signal and Information Processing (IConSIP), 1–5. https://doi.org/10.1109/iconsip.2016.7857480
13. Smailov, N., Uralova, F., Kadyrova, R., Magazov, R., Sabibolda, A. (2025). Optymalizacja metod uczenia maszynowego do deanonimizacji w sieciach społecznościowych. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15 (1), 101–104. https://doi.org/10.35784/iapgos.7098
14. Goettling, M., Hammer, A., Malberg, H., Schmidt, M. (2024). xECGArch: a trustworthy deep learning architecture for interpretable ECG analysis considering short-term and long-term features. Scientific Reports, 14 (1). https://doi.org/10.1038/s41598-024-63656-x
15. Zilberman, A., Rogel, S. (1990). Hemodynamic evaluation of common cardiac arrhythmias. International Journal of Cardiology, 27 (3), 341–349. https://doi.org/10.1016/0167-5273(90)90291-c
16. Smailov, N., Orynbet, M., Nazarova, A., Torekhan, Z., Koshkinbayev, S., Yssyraiyl, K. et al. (2025). Optymalizacja pracy światłowodowych czujników w warunkach kosmicznych. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15 (2), 130–134. https://doi.org/10.35784/iapgos.7200
17. Hamo, C. E., DeJong, C., Hartshorne-Evans, N., Lund, L. H., Shah, S. J., Solomon, S., Lam, C. S. P. (2024). Heart failure with preserved ejection fraction. Nature Reviews Disease Primers, 10 (1). https://doi.org/10.1038/s41572-024-00540-y
18. Sabibolda, A., Tsyporenko, V., Smailov, N., Tsyporenko, V., Abdykadyrov, A. (2024). Estimation of the Time Efficiency of a Radio Direction Finder Operating on the Basis of a Searchless Spectral Method of Dispersion-Correlation Radio Direction Finding. Advances in Asian Mechanism and Machine Science, 62–70. https://doi.org/10.1007/978-3-031-67569-0_8
19. Braunwald, E., Frahm, C. J., Ross, J. (1961). Studies on starling's law of the heart. V. Left ventricular function in man. Journal of Clinical Investigation, 40 (10), 1882–1890. https://doi.org/10.1172/jci104412
20. Smailov, N., Akmardin, S., Ayapbergenova, A., Ayapbergenova, G., Kadyrova, R., Sabibolda, A. (2025). Analiza wydajności VLC w optycznych systemach komunikacji bezprzewodowej do zastosowań wewnętrznych. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15 (2), 135–138. https://doi.org/10.35784/iapgos.6971
21. deChazal, P., O'Dwyer, M., Reilly, R. B. (2004). Automatic Classification of Heartbeats Using ECG Morphology and Heartbeat Interval Features. IEEE Transactions on Biomedical Engineering, 51 (7), 1196–1206. https://doi.org/10.1109/tbme.2004.827359
22. Yildirim, O., Baloglu, U. B., Tan, R.-S., Ciaccio, E. J., Acharya, U. R. (2019). A new approach for arrhythmia classification using deep coded features and LSTM networks. Computer Methods and Programs in Biomedicine, 176, 121–133. https://doi.org/10.1016/j.cmpb.2019.05.004
23. Abdykadyrov, A., Smailov, N., Sabibolda, A., Tolen, G., Dosbayev, Z., Ualiyev, Z., Kadyrova, R. (2024). Optimization of distributed acoustic sensors based on fiber optic technologies. Eastern-European Journal of Enterprise Technologies, 5 (5 (131)), 50–59. https://doi.org/10.15587/1729-4061.2024.313455
24. Acharya, U. R., Oh, S. L., Hagiwara, Y., Tan, J. H., Adam, M., Gertych, A., Tan, R. S. (2017). A deep convolutional neural network model to classify heartbeats. Computers in Biology and Medicine, 89, 389–396. https://doi.org/10.1016/j.compbiomed.2017.08.022
25. Bekbay, A., Ozhikenov, K., Ozhikenova, A., Bodin, O., Bezborodova, O., Rakhmatullov, F. (2019). Heart State Monitoring Using Multi-Agent Technology. 2019 8th Mediterranean Conference on Embedded Computing (MECO), 1–4. https://doi.org/10.1109/meco.2019.8760007
26. Bekbay, A., Alimbayeva, Z., Alimbayev, C., Bayanbay, N., Ozhikenov, K., Mukazhanov, Y. (2022). Development of an atrioventricular block prediction of method for portable heart monitoring system. Eastern-European Journal of Enterprise Technologies, 3 (5 (117)), 15–27. https://doi.org/10.15587/1729-4061.2022.258791
27. Smailov, N., Tsyporenko, V., Sabibolda, A., Tsyporenko, V., Abdykadyrov, A., Kabdoldina, A. et al. (2024). Usprawnienie cyfrowego korelacyjno-interferometrycznego ustalania kierunku za pomocą przestrzennego sygnału analitycznego. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 14 (3), 43–48. https://doi.org/10.35784/iapgos.6177
28. Smailov, N., Tsyporenko, V., Ualiyev, Z., Issova, A., Dosbayev, Z., Tashtay, Y. et al. (2025). Improving accuracy of the spectral-correlation direction finding and delay estimation using machine learning. Eastern-European Journal of Enterprise Technologies, 2 (5 (134)), 15–24. https://doi.org/10.15587/1729-4061.2025.327021
29. Rahman, H. U., Ahmad, J., Akhmediyarova, A., Oralbekova, D., Mamyrbayev, O. (2024). Deciphering the Role of Circadian Clock in Inflammatory Response and Immune Disorders Using Model Checking and Petri Nets. IEEE Access, 12, 196576–196590. https://doi.org/10.1109/access.2024.3521499
30. Zilgarayeva, A., Smailov, N., Pavlov, S., Mirzakulova, S., Alimova, M., Kulambayev, B., Nurpeissova, D. (2024). Optical sensor to improve the accuracy of non-invasive blood sugar monitoring. Indonesian Journal of Electrical Engineering and Computer Science, 34 (3), 1489. https://doi.org/10.11591/ijeecs.v34.i3.pp1489-1498

Анотації

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2025.341735

УДОСКОНАЛЕННЯ МЕТОДУ ВИЗНАЧЕННЯ КООРДИНАТ РОЗВІДУВАЛЬНОГО БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ МАЛОБАЗОВОЮ МЕРЕЖЕЮ ДВОХ SOFTWARE-DEFINED RADIO ПРИЙМАЧІВ (с. 6–13)

І. В. Рубан, Г. В. Худов, Є. В. Бернік, О. М. Маковейчук, В. Г. Малюга, С. В. Яровой, Р. Г. Худов, В. Г. Худов, Л. Л. Побережний, О. О. Гончаренко

Об'єктом дослідження є процес визначення координат розвідувального безпілотного літального апарату. Проблема, що вирішувалась, полягала у визначенні координат розвідувального безпілотного літального апарату малобазовою мережею мобільних пристроїв пасивної локації.

Удосконалено метод визначення координат розвідувального безпілотного літального апарату, який, на відміну від відомих, передбачає:

– визначення пеленгів на розвідувальний безпілотний літальний апарат;

– використання тріангуляційного методу.

Проведено оцінювання точності визначення координат розвідувального безпілотного літального апарату малобазовою мережею двох Software-Defined Radio приймачів. Встановлено, що форма та орієнтація еліпсів похибок залежить від положення розвідувального безпілотного літального апарату відносно Software-Defined Radio приймачів. Точність визначення координат суттєво погіршується у випадках, коли полярний кут спостереження з центру бази наближається до 0° або 180°. Найвища точність визначення координат досягається тоді, коли розвідувальний безпілотний літальний апарат знаходиться на траверзі до середини бази.

Встановлено, що для малих баз спостерігається більш виражена нерівномірність залежності точності від положення розвідувального безпілотного літального апарату у порівнянні з більшими базами. На великих дальностях похибки при малих базах різко зростають. Встановлено, що зі зменшенням довжини бази площа еліпсів похибок зростає, що свідчить про погіршення потенційних характеристик точності системи та збільшення середньої кругової похибки. При цьому геометричні особливості зберігаються, орієнтація еліпсів та характер їхнього розташування відносно лінії бази залишаються сталими.

Ключові слова: безпілотний літальний апарат, малобазова мережа, Software-Defined Radio приймач, пеленг.

DOI: 10.15587/1729-4061.2025.340918

РОЗРОБКА СИМУЛЯТОРА ДЛЯ ПІДТРИМКИ ПЛАНУВАННЯ УСПІШНОСТІ МІСІЙ БПЛА В УМОВАХ БОЙОВИХ ДІЙ (с. 14–26)

А. М. Тищенко, І. В. Стьопочкіна

Об'єктом дослідження є мережі безпілотних літальних апаратів (БпЛА), що функціонують в умовах дії деструктивних та ворожих факторів. Серед деструктивних факторів враховано зміни потужності сигналу на боці приймача через вплив відстані та обмеження заряду батарей. Серед ворожих факторів розглянуто кіберфізичні загрози, спричинені системами радіоелектронної протидії (РЕП) та атаками на основі шкідливого програмного забезпечення. Для розв'язання цієї проблеми було розроблено алгоритмічні та програмні рішення для моделювання поведінки БпЛА в таких умовах. Запропонована модель відрізняється від існуючих інтеграцією таких факторів, як погіршення сигналу внаслідок дії систем РЕП та динаміка поширення шкідливого програмного забезпечення в мережі.

Сценарії включають поведінку БпЛА під впливом радіоперешкод, імовірнісне поширення шкідливого програмного забезпечення (ШПЗ), а також перехід між режимами роботи у відповідь на загрози. Результати досягнуто шляхом врахування широкого спектру параметрів, в тому числі: ідентифікатора пристрою, потужності сигналу, радіусу передавача, частоти передачі, геолокації, типу завдання, чутливості до шкідливого ПЗ, черги обробки повідомлень, затримок поширення та швидкості руху. Ці характеристики дозволяють моделі реалістично відтворювати поведінку системи в умовах невизначеності та загроз, забезпечуючи можливість аналізу як захисних, так і наступальних стратегій кібербезпеки та побудови відповідних сценаріїв операцій.

Запропоноване програмне рішення характеризується високим рівнем деталізації моделювання та використанням мови програмування Rust, що забезпечує продуктивність, модульність і можливість розширення. Розроблене рішення дозволяє візуалізувати поведінку до 100 БпЛА та більше у вигляді зображень та анімацій. Програмний пакет і його вихідний код оприлюднено у відкритому репозиторії GitHub, що забезпечує практичне застосування та подальше використання в дослідженнях.

Ключові слова: моделювання мереж БпЛА, кіберфізична безпека, шкідливе програмне забезпечення, радіоелектронна протидія.

DOI: 10.15587/1729-4061.2025.341734

РОЗРОБКА МОДЕЛІ АНАЛІЗУ ТА РОЗДІЛЕННЯ СЛУЖБОВОГО І КОРИСНОГО ТРАФІКУ У КІБЕРФІЗИЧНИХ СИСТЕМАХ (с. 27–40)

М. Ю. Толкачов, Н. В. Дженюк, С. П. Євсеєв, В. П. Шульга, Є. О. Меленті, С. А. Микусь, І. Р. Опірський, А. О. Смірнов, М. О. Мельник, М. О. Жигалов

Об'єктом дослідження є процеси формування, передачі й обробки службового та корисного трафіку в кіберфізичних системах Smart Manufacturing Ecosystem багаторівневої архітектури, вразливих до кібератак, спрямованих на компрометацію управлінських даних, автентифікації й координації. У сучасних комп'ютерних мережах службовий трафік визначає стабільність і безпеку інфраструктури, оскільки будь-яке спотворення або перехоплення службового трафіку може призвести до порушення роботи системи загалом. У смарт-системах, промисловому інтернеті речей та критичній інфраструктурі обсяг службових повідомлень сягає значних масштабів, адже саме вони підтримують синхронність роботи тисяч систем у режимі реального часу.

У роботі досліджено проблему захисту службового трафіку в кіберфізичних системах Smart Manufacturing Ecosystem. Запропоновано математичну модель сегментації службового та корисного трафіку, яка враховує критерії стійкості (сегментація доступу, контроль цілісності та автентичності) і безпеки (ймовірність компрометації, критичність каналу, рівень довіри до середовища передачі). Для побудови інтегрального показника ризику використано метод згорток, що дозволяє поєднати різнотипні параметри та визначати доцільність розділення трафіку для цільового аналізу. Дослідження виконано на прикладі промислових протоколів Modbus, DNP3, OPC UA, MQTT та HTTP, що широко застосовуються у виробничих мережах. Показано, що застосування моделі дозволяє знизити інтегральний ризик атак на службовий трафік у середньому на 15–20% порівняно з підходами без сегментації. Розроблена модель формує наукове підґрунтя для створення методів і практичних рішень кіберзахисту, які забезпечують підвищення стійкості інфраструктури Smart Manufacturing та здатні протистояти сучасним і майбутнім викликам у сфері кібербезпеки.

Ключові слова: службовий трафік, промислові протоколи, кіберфізична система, кібербезпека, піраміда виробництва, IoT-мережі.

DOI: 10.15587/1729-4061.2025.340917

РОЗРОБКА АЛГОРИТМУ З ТИМЧАСОВОЮ КРИПТОГРАФІЧНОЮ СТІЙКІСТЮ ДЛЯ ШИФРУВАННЯ ВІДЕОПОТОКУ З БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА (с. 41–53)

Л. В. Ковальчук, А. М. Давиденко, Т. М. Клименко, А. В. Недашківська, С. Я. Гільгурт

Об'єктом дослідження є процес захисту відеопотоку, що передається з бортової відеокамери безпілотного літального апарату (БПЛА) на наземну станцію у фронтовій та прифронтовій зоні. Специфіка проблеми, що вирішувалася, визначається, з одного боку, обмеженими обчислювальними ресурсами бортової апаратури, яка повинна в режимі реального часу зашифровувати інтенсивний потік даних, з іншого – відносно коротким періодом життя БПЛА в умовах бойового застосування (особливо для FPV-дронів-камікадзе) в межах від 10 хвилин до кількох діб. В переважній більшості відомих робіт в даній галузі розглядаються алгоритми, орієнтовані на застосування в інших умовах, причому головні зусилля спрямовані на досягнення максимальної крипостійкості. На відміну від висвітлених у відкритій літературі розробок, в даному дослідженні вдалося вирішити зазначену проблему шляхом врахування її специфічних особливостей та застосування певного компромісу між швидкодією та ресурсоємністю алгоритму, з одного боку, та його стійкістю, з іншого. Досягти даного результату вдалося завдяки проведенню детального порівняльного аналізу та класифікації найближчих за характеристиками рішень, що складає більшість дослідження. За його підсумками в якості першого наближення був обраний алгоритм PRESENT. Запропоноване рішення базується на використанні усіченої до 16 раундів модифікації даного алгоритму в режимі лічильника. Аналіз отриманого рішення свідчить, що його криптографічна стійкість вимагає більше 2 місяців обчислювальної роботи при здійсненні найкращої атаки, тобто стійкість алгоритму є цілком прийнятною. Для практичного використання отриманих теоретичних результатів необхідно ретельно перевірити властивості реалізованого в апаратурі запропонованого рішення в польових умовах, максимально наближених до бойових, та за необхідності внести потрібні корективи.

Ключові слова: БПЛА, шифрування відеоданих, тимчасова стійкість, малоресурсні криптоалгоритми, блокові шифри, PRESENT.

DOI: 10.15587/1729-4061.2025.339985

РОЗРОБКА АДАПТИВНОГО МЕХАНІЗМУ КЕРУВАННЯ ПЕРЕВАНТАЖЕННЯМ ДЛЯ МУЛЬТИМЕДІА-СТРИМІНГУ В РЕАЛЬНОМУ ЧАСІ ЗА ЗМІННИХ УМОВАХ МЕРЕЖІ (с. 54–63)

Marvin Chandra Wijaya

Це дослідження зосереджено на потоковій передачі мультимедіа в реальному часі з використанням протоколів RTP та RTCP. Основна проблема, яку розглядає дослідження, полягає в тому, що стандартний контроль перевантаження RTP/RTCP недостатньо адаптований до змінних та нестабільних мережевих умов, що призводить до збільшення втрати пакетів, наскрізної затримки, нестабільних бітрейтів та низької якості відео. Для потокової передачі RTP було розроблено динамічний механізм контролю перевантаження, адаптований до про-

пускної здатності, який використовує зворотний зв›язок RTCP для динамічної зміни бітрейту та частоти кадрів у реальному часі під час сеансу потокової передачі. Результати контрольованого експерименту показують, що середня втрата пакетів зменшується з 8,2% до 3,4%; наскрізна затримка зменшується в середньому із 220 мс до 135 мс; та забезпечує стабільніший середній бітрейт, ніж стандартні системи RTP/RTCP. Крім того, ця система також забезпечує стабільнішу середню частоту кадрів, ніж стандартні системи RTP/RTCP, та вищу середню частоту кадрів за поганих мережевих умов. Цей результат можна пояснити здатністю адаптивного механізму постійно контролювати втрату пакетів, перешкоди та затримки, а також негайно реагувати на умови, замість того, щоб чекати появи звітів RTCP через фіксовані проміжки часу. Ключовим моментом щодо запропонованого дизайну є інтеграція бітрейту та частоти кадрів для забезпечення плавного відтворення та задоволення користувача від перегляду зі зниженим ризиком переривання та покращеною стабільністю в динамічних та непередбачуваних мережевих середовищах. Цей внесок може бути практично застосований у застосунках реального часу, таких як відеоконференції, телемедицина або прямі трансляції під час проходження мобільних або бездротових мереж, де умови завжди динамічні та непередбачувані. Запропонований метод може бути практично застосований за несприятливих умов інтернет-мережі, що є його перевагою.

Ключові слова: адаптивна система, мультимедіа, перевантаження мережі, протокол керування транспортом у реальному часі, потокове відео.

DOI: 10.15587/1729-4061.2025.340994

ВИЗНАЧЕННЯ ВПЛИВУ ФАЗОВОЇ МОДУЛЯЦІЇ ТА ОПТИМАЛЬНОЇ ОБРОБКИ СИГНАЛУ НА ЗАВАДОСТІЙКІСТЬ І ДАЛЬНІСТЬ ЗВ'ЯЗКУ (с. 64–81)

Ю. П. Гончаренко, Г. А. Голуб, Н. М. Цивенкова, І. І. Поліщук, А. Ю. Денисюк, І. С. Омаров, О. М. Сукманюк

Об'єкт дослідження – аналогові системи високочастотного (ВЧ) зв'язку з використанням широкосмугових сигналів, модульованих кодом Баркера. У роботі розв'язується проблема підвищення ефективності аналогових систем ВЧ-зв'язку при передаванні широкосмуговх сигналів. Досліджено закономірності формування завадостійкого широкосмугового сигналу з фазовою модуляцією Баркер-кодом і роботу блоку розширення та відновлення спектру сигналу. Встановлено, що фазова модуляція дозволяє досягти такої спектральної ширини, амплітуди головного піку автокореляційної функції і часової роздільної здатності, що забезпечує ефективне кореляційне виділення корисного сигналу та підвищує його завадостійкість. Показано, що модуляція сигналу п'ятирозрядним кодом формує спектр шириною 1 МГц, амплітуду головного піку автокореляційної функції 9 од. і часову роздільну здатність 1–2 мкс, що забезпечує зростання завадостійкості до 9 дБ при С/Ш=1 дБ порівняно з базовим сигналом без модуляції. Використання тринадцятирозрядного коду дозволяє збільшити цей показник до 13 дБ при С/Ш=–3 дБ.

Підтверджено ефективність блоку розширення та відновлення спектру модульованого сигналу при його передаванні на відстані без втрати якості зв'язку. Модуляція сигналу 5 та 13-розрядним кодом, порівняно з немодульованим, збільшила дальність зв'язку у 9 та 25 разів відповідно. Результати досягаються завдяки оптимальним автокореляційним властивостям Баркер-кодів та апаратним рішенням, які формують широкосмуговий сигнал без ускладнення схеми. Це пояснюється здатністю Баркер-кодів формувати вузький кореляційний імпульс і розширювати спектр сигналу, що знижує чутливість до вузькосмугових завад. Результати мають цінність застосування в аналогових системах ВЧ-зв'язку, енергетичних мережах, зокрема при низькому співвідношенні С/Ш.

Ключові слова: автокореляційна функція, аналоговий сигнал, код Баркера, узгоджений фільтр, фазова модуляція.

DOI: 10.15587/1729-4061.2025.340990

РОЗРОБКА МЕРЕЖЕВОЇ АРХІТЕКТУРИ НА ОСНОВІ СТРАТОСФЕРНИХ ДИРИЖАБЛІВ ДЛЯ ТЕЛЕКОМУНІКАЦІЇ У ВІДДАЛЕНИХ РАЙОНАХ (с. 82–92)

Mukhit Abdullayev, Ainur Kuttybayeva, Kalmukhamed Tazhen, Anar Khabay, Nurzhamal Ospanova, Yerlan Tashtay, Arnur Sabyrbayev, Ilyas Samat, Rimma Abdykadyrkyzy, Daria Zhumakhanova

Об'єктом цього дослідження є телекомунікаційна платформа на базі стратосферного дирижабля, що використовується як висотна платформна станція (HAPS), призначена для роботи на висотах 20–30 км та забезпечення широкосмугового зв'язку в регіонах з обмеженою наземною інфраструктурою, таких як сільські та віддалені райони Республіки Казахстан. Ключовою проблемою, що досліджувалась, є забезпечення стабільного зв'язку телекомунікаційних платформ на базі HAPS за умов сильних стратосферних вітрів, з обмеженою вантажопідйомністю та енергетичними ресурсами, а також розробка масштабованої мережевої архітектури для координації кількох дирижаблів.

Запропонована мережева концепція на основі модульних нанодирижаблів, яка зменшує опір, підвищує ремонтопридатність та забезпечує безперервне обслуговування. Були проведені розрахунки вантажопідйомності, аеродинамічного опору різних форм оболонки, енергетичного балансу та радіуса покриття однієї станції. Експериментальні випробування прототипу підтвердили можливість використання суб-ГГц діапазону (433 МГц) для забезпечення зв'язку на великі відстані в наземних випробувальних умовах, де ослаблення сигналу виявилося мінімальним порівняно з вищими частотами.

Завдяки отриманим характеристикам було підтверджено гіпотезу про використання групи менших дирижаблів замість одного великого носія. Це пояснюється їхньою зниженою чутливістю до вітрових навантажень, гнучкістю конфігурації мережі та нижчими експлуатаційними ризиками. На відміну від традиційних супутникових систем, запуск та обслуговування яких є дорогими, стра-

тосферні дирижаблі можна відновлювати, ремонтувати та перерозгортати за відносно низькою ціною, що є економічно вигідним рішенням для регіонів, що розвиваються.

Результати можуть бути застосовані при створенні національних мереж зв'язку для віддалених та малонаселених районів Республіки Казахстан, в операціях з реагування на надзвичайні ситуації та як додатковий рівень до супутникових сузір'їв. Запропонована концепція демонструє, що модульні мережі HAPS є реалістичною та масштабованою альтернативою, здатною забезпечувати широкосмуговий доступ за реальних атмосферних та географічних обмежень.

Ключові слова: висотні платформні станції (HAPS), стратосферний дирижабль, телекомунікаційна мережа, технологія LoRa, частота нижче ГГц.

DOI: 10.15587/1729-4061.2025.340833

ПРОГНОЗУВАННЯ МІСІЙ РОБОТОТЕХНІЧНИХ ПЛАТФОРМ З ВИКОРИСТАННЯМ KERNEL ACTIVATION NETWORK З АСИМЕТРИЧНИМ ЯДРОМ (с. 93–103)

О. І. Лактіонов, А. С. Янко, Б. Р. Боряк, О. В. Михайліченко

Об'єктом дослідження є процеси прогнозування функціональної ефективності робототехнічних платформ, що впливають на оптимізацію планування їхніх місій. В умовах зростаючого попиту на автономні мобільні системи критичною проблемою є забезпечення високої ефективності їхньої динаміки за різних навантажень, рельєфів та швидкостей, що вимагає надійних інструментів для ухвалення рішень ще до фізичного запуску.

Для вирішення проблеми розроблено та програмно реалізовано метод на основі кастомізованої Kernel Activation Network (KAN), що прогнозує функціональну ефективність платформи. Результати демонструють значне підвищення точності: KAN досягає MSE 0.00055727 на синтетичних даних та 0.00041720 на експериментальній вибірці, тоді як інші архітектури демонструють 0.00105989 і вище.

Ключова інновація KAN – використання несиметричного хі-квадрат ядра паралельно з Гаусовим ядром, а також інтеграція вхідних оцінок, що враховують потрійну взаємодію факторів. Це пояснює здатність мережі ефективно фіксувати складні нелінійні залежності між численними параметрами платформи (опір кочення, аеродинамічний опір, сила скелелазіння тощо) та умовами середовища. Застосування несиметричного ядра значно спрощує архітектуру мережі, дозволяючи досягти високої точності при меншій обчислювальній складності.

На практиці отримані результати слугують додатковим інструментом для оптимізації планування місій робототехнічних платформ. Це дозволяє оптимізувати вибір обладнання, розробляти стратегічні логістичні маршрути, підвищувати безпеку та надійність автономних систем у реальних умовах. Досягнутий Technology Readiness Level становить 4.

Ключові слова: прогнозування функціоналу, взаємодія факторів, несиметричне ядро, нейронна мережа, робототехнічна платформа.

DOI: 10.15587/1729-4061.2025.340033

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ПЕРЕДПРОЦЕСОРА ГРАФОВИХ ОЗНАК НА ОСНОВІ ДИСКА ДЛЯ ВИЯВЛЕННЯ ФІНАНСУВАННЯ ТЕРОРИЗМУ (с. 104–116)

Aigerim Bolshibayeva, Sabina Rakhmetulayeva, Aliya Kulbayeva, Ansar-Ul-Haque Yasar

Об'єктом дослідження є потокові платіжні транзакції, змодельовані як спрямовані мультиграфи. Ця робота досліджує виявлення фінансування тероризму в мережах платіжних транзакцій за допомогою обробки графів на основі дисків та виявлення аномалій. Ключовою проблемою, що розглядається, є високе споживання пам'яті детекторами на основі графів, що перешкоджає аналізу в системах з обмеженою оперативною пам'яттю, типовою для малих та середніх фінансових установ.

Для вирішення цієї проблеми було створено дисковий препроцесор графових ознак (ДППГО). Під час обробки потоку ДППГО динамічно маркує підключені компоненти та ідентифікує вісім шаблонів графів, характерних для фінансування тероризму, включаючи зірки типу «розгалужені/розгалужені» та багатострибкові ланцюги. Система зберігає дескриптори компонентів у стовпчастому сховищі на SSD та використовує гарячий кеш, керований LRU, для обслуговування ознак, що дозволяє оцінювати транзакції в режимі реального часу з затримкою менше секунди.

У потоці AMLSim з двома мільйонами транзакцій система інтегрується з легким ізоляційним лісом (Isolation Forest) та досягає показника F1 0,76, одночасно зменшуючи піковий обсяг оперативної пам'яті з 18,3 ГБ до 9,8 ГБ та підтримуючи середню затримку 410 ± 15 мс для 10 000 транзакцій. Обчислення на мотив залишається ≤ 28,4 мс (медіана < 24 мс), що підтримує оцінювання в режимі реального часу на стандартному обладнанні.

ДППГО створює модельно-агностичні ознаки графів, які взаємодіють зі стандартними детекторами аномалій без перенавчання ГНМ.

Внесок цього дослідження включає архітектуру зовнішньої пам›яті для потокового вилучення ознак графів; схему маркування ознак на основі мотивів, що зберігається на SSD та кешується LRU; та емпіричну оцінку, що демонструє покращення продуктивності та ефективності пам'яті в режимі реального часу для даних боротьби з відмиванням грошей.

Ключові слова: фінансування тероризму, обробка графів, алгоритми зовнішньої пам'яті, виявлення аномалій, відповідність.

DOI: 10.15587/1729-4061.2025.340493

ІНТЕРПРЕТОВАНИЙ ПІДХІД НА ОСНОВІ ЕКГ ДЛЯ ВИЯВЛЕННЯ ГЕМОДИНАМІЧНО ЗНАЧУЩИХ АРИТМІЙ З ВИКОРИСТАННЯМ ЛЕГКИХ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ (с. 117–124)

Ainur Bekbay, Lashin Bazarbay, Zhanar Bigaliyeva, Vinera Baiturganova, Akezhan Sabibolda, Yersaiyn Mailybayev, Nurzhigit Smailov

Об'єктом цього дослідження є діагностичний процес пацієнтів з підозрою на гемодинамічно значущу аритмію в умовах невідкладної допомоги та телемедицини, де потрібна швидка та інтерпретована підтримка рішень. Проблема, що розглядається, полягає в обмеженому доступі до ехокардіографічної оцінки в умовах невідкладної допомоги та обмежених ресурсів, де терміново потрібні інтерпретовані та обчислювально ефективні альтернативи, особливо для мобільних та польових застосувань.

Основні результати показують, що моделі машинного навчання, такі як XGBoost, досягли високої діагностичної ефективності (F1-оцінка = 0,84, AUC = 0,91), тоді як класифікатори на основі правил забезпечили клінічно інтерпретовану точність. Ці результати дозволили частково компенсувати відсутність ехокардіографії та сприяли надійному сортуванню в гострих та чутливих до часу умовах.

Ця ефективність випливає з ключових особливостей методу: опори на інтерпретовані ознаки ЕКГ (tQRS, tRR, HR та EF, отримані з tQRS/tRR) та низької обчислювальної складності, що відрізняє його від більш непрозорих методів глибокого навчання. Результати пояснюються сильною кореляцією між цими характеристиками та як електричною, так і механічною функцією серця, що дозволяє проводити гемодинамічну оцінку без візуалізації. Це підтримує клінічну довіру до результатів алгоритму.

Запропонований підхід застосовується в первинному скринінгу, невідкладному сортуванні, телемедицині та дистанційному моніторингу, поєднуючи точність із поясненням та автономністю від інструментів візуалізації. Тому дослідження інтерпретованого виявлення гемодинамічно значущих аритмій на основі ЕКГ залишаються дуже актуальними, особливо в умовах відсутності доступу до спеціалізованої діагностики.

Ключові слова: оцінка фракції викиду на основі ЕКГ, фракція викиду, машинне навчання, класифікація ЕКГ, співвідношення tQRS/tRR.