

ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2023.285514

PERFORMANCE EVALUATION OF THE CLOUD COMPUTING APPLICATION FOR IOT-BASED PUBLIC TRANSPORT SYSTEMS (p. 6–13)**Ihor Zakutynskyi**

National Aviation University, Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0003-2905-3205>**Leonid Sibruk**

National Aviation University, Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0002-4119-7984>**Ihor Rabodzei**

National Aviation University, Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0002-2505-5249>

The object of research is cloud computing as an element of the server infrastructure for intelligent public transport systems. Given the increasing complexity and requirements for modern transportation, the application of the Internet of Things concept has a high potential to improve efficiency and passenger comfort. Since the load generated in IoT systems is dynamic and difficult to predict, the use of traditional infrastructure with dedicated servers is suboptimal. This study considers the use of cloud computing as the main server infrastructure for the above systems. The paper investigates the main cloud platforms that can be used to develop such systems and evaluates their advantages and disadvantages. The authors developed the overall architecture of the system and evaluated the performance and scalability of individual components of the server infrastructure. To test the system, a software emulator was developed that simulates the controller module installed in vehicles. Using the developed emulator, stress tests were conducted to analyze and confirm the ability to scale and process input data by the proposed architecture. The test scenarios were developed and conducted on the basis of the existing public transportation system in Kyiv, Ukraine. The experimental results showed that the proposed IoT architecture is able to scale efficiently according to the load generated by the connected devices. It has been found that when the number of incoming messages increases from 40 to 6000, the average message processing time remains unchanged, and the error rate does not increase, which is an indicator of stable system operation. The obtained results can be used in the development of modern public transport systems, as well as for the modernization of existing ones.

Keywords: internet of things, cloud computing, system architecture, public transport systems, scalability.

References

1. Future Of Industry Ecosystems: Shared Data And Insights. IDC. Available at: <https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/>
2. Mchergui, A., Hajlaoui, R., Moulahi, T., Alabdulatif, A., Lorenz, P. (2023). Steam computing paradigm: Cross-layer solutions over cloud, fog, and edge computing. *IET Wireless Sensor Systems*. doi: <https://doi.org/10.1049/wss2.12051>
3. Porru, S., Misso, F. E., Pani, F. E., Repetto, C. (2020). Smart mobility and public transport: Opportunities and challenges in rural and urban areas. *Journal of Traffic and Transportation Engineering (English Edition)*, 7 (1), 88–97. doi: <https://doi.org/10.1016/j.jtte.2019.10.002>
4. Farkas, K., Feher, G., Benczur, A., Sidlo, C. (2015). Crowdsending based public transport information service in smart cities. *IEEE Communications Magazine*, 53 (8), 158–165. doi: <https://doi.org/10.1109/mcom.2015.7180523>
5. Vieira, E., Almeida, J., Ferreira, J., Dias, T., Vieira Silva, A., Moura, L. (2023). A Roadside and Cloud-Based Vehicular Communications Framework for the Provision of C-ITS Services. *Information*, 14 (3), 153. doi: <https://doi.org/10.3390/info14030153>
6. Metzger, F., Hobfeld, T., Bauer, A., Kounev, S., Heegaard, P. E. (2019). Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud. *Proceedings of the IEEE*, 107 (4), 679–694. doi: <https://doi.org/10.1109/jproc.2019.2901578>
7. Khan, M. A., Nawaz, T., Khan, U. S., Hamza, A., Rashid, N. (2023). IoT-Based Non-Intrusive Automated Driver Drowsiness Monitoring Framework for Logistics and Public Transport Applications to Enhance Road Safety. *IEEE Access*, 11, 14385–14397. doi: <https://doi.org/10.1109/access.2023.3244008>
8. Hind, M., Noura, O., Sanae, M., Abraham, A. (2023). A Comparative Study for Modeling IoT Security Systems. *Lecture Notes in Networks and Systems*, 258–269. doi: https://doi.org/10.1007/978-3-031-35510-3_25
9. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, 11 (1), 16. doi: <https://doi.org/10.3390/electronics11010016>
10. Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., Johnson, R. C. (2023). Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures. *IEEE Internet of Things Journal*, 10 (13), 11224–11239. doi: <https://doi.org/10.1109/jiot.2023.3252594>
11. Zakutynskyi, I., Sibruk, L., Kokariev, A. (2023). IoT System for Monitoring and Managing Public Transport Data. *WSEAS TRANSACTIONS ON SYSTEMS*, 22, 242–248. doi: <https://doi.org/10.37394/23202.2023.22.25>
12. Kyivpastrans. Wikipedia. Available at: <https://en.wikipedia.org/wiki/Kyivpastrans>
13. Availability. Amazon. Available at: <https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/availability.html>
14. Image «RaspberryPi B3 +». Available at: https://media.distrelec.com/Web/ShopImages/landscape_large/8-/01/RaspberryPi_B3_plus_30109158-01.jpg
15. Image «Teltonika TRM 250». Available at: https://wiki.teltonika-networks.com/images/3/3f/Trm250_hd_1.png
16. Data modeling. Amazon. Available at: <https://docs.aws.amazon.com/timestream/latest/developerguide/data-modeling.html>
17. Massaro, A., Selicato, S., Galiano, A. (2020). Predictive Maintenance of Bus Fleet by Intelligent Smart Electronic Board Implementing Artificial Intelligence. *IoT*, 1 (2), 180–197. doi: <https://doi.org/10.3390/iot1020012>

DOI: 10.15587/1729-4061.2023.285414

IMPROVING THE TECHNOLOGY FOR PROCESSING THE AGGREGATED DATA FLOW OF A SECURE CORPORATE MULTISERVICE COMMUNICATION NETWORK (p. 14–23)**Liubov Berkman**

State University of Telecommunications, Kyiv, Ukraine

ORCID: <https://orcid.org/0000-0002-6772-1596>

Andrii Zakhazhevskiy

The National Defence University of Ukraine named after Ivan Cherniakhovskiy, Kyiv, Ukraine
ORCID: <https://orcid.org/0000-0001-7019-9949>

Kostiantyn Lavrinets

State University of Telecommunications, Kyiv, Ukraine
ORCID: <https://orcid.org/0009-0000-4846-3977>

This paper considers the process of dynamic reservation of the channel resource of a secure corporate multi-service communication network.

It has been established that the processes of building and functioning of the schemes of a secure corporate multi-service communication network and improving the quality of the implementation of its main work processes involve the evaluation and dynamic reservation of channel resources for incoming aggregated data flows of the network.

The model of dynamic reservation of the channel resource of the aggregated data stream of the secure corporate multi-service communication network was built and proposed. The proposed model makes it possible to set the quantitative values of the reserved channel resource for different service methods depending on the number of component flows in the total aggregated data flow of the VPN tunnel.

It was established that an increase in the density of the aggregated data stream requires an increase in the reserved channel resource. At the same time, its value is influenced by the way of servicing the aggregated data flow in the VPN tunnel of the secure corporate multi-service communication network. Application of the isolated service method gives a gain in the allocated resource for the channel reserve from 10 to 20 percent compared to the group service method for IR and video telephony. This is due to the more flexible management process of the border router's incoming data storage buffer under the isolated service mode.

The model of dynamic reservation of the channel resource of the secure corporate multi-service communication network reported in this paper could be used in the improvement of existing and development of new structures of the secure corporate multi-service communication network. The consequence of such an improvement is a reduction in the delay time for the processing of incoming data packets in the specified network.

Keywords: secure corporate multiservice communication network, aggregate flow, channel resource, VPN gateway.

References

- Popivskiy, V. V., Lemeshko, O. V., Kovalchuk, V. K., Plotnikov, M. D., Kartushyn, Yu. P. et al. (2012). *Telekomunikatsiini systemy ta mer ezhi. Struktura y osnovni funktsiyi. Vol. 1.*
- Zakhyst informatsiyi na ob'ekтах informatsiynoi diyalnosti. Stvorennia kompleksu tekhnichnoho zakhystu informatsiyi. Osnovni polozhennia. ND TZI 1.1-005-07. Available at: <https://tzi.com.ua/nd-tz-1.1-005-07.html>
- Halkin, V. V., Parkhomenko, I. I. (2016). *Vykorystannia VPN-tekhnolohiy dlia zakhystu informatsiyi v kanalakh korporatyvnykh mer ezh. Problema kiberbezpeky informatsiyno-telekomunikatsiynykh system: materialy nauk.- tekhn. konf. Kyiv: KNU, 66–76.*
- Buriachok, V. L., Anosov, A. O., Semko, V. V., Sokolov, V. Yu., Skladanyni, P. M. (2019). *Tekhnolohiyi zabezpechennia bezpeky merezhevoi infrastruktury. Kyiv: «KUBH», 218.* Available at: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBML.pdf
- Popovskiy, V. V., Oliinyk, V. F. (2011). *Matematychni osnovy upravlinnia i adaptatsiyi v telekomunikatsiynykh systemakh. Kharkiv: TOV "Kompaniya SMIT", 362.*
- IPSec – protokol zakhystu merezhevoho trafiku na IP-rivni.
- Talib, H. A., Alothman, R. B., Mohammed, M. S. (2023). Malicious attacks modelling: a prevention approach for ad hoc network security. *Indonesian Journal of Electrical Engineering and Computer Science*, 30 (3), 1856. doi: <https://doi.org/10.11591/ijeecs.v30.i3.pp1856-1865>
- Almomani, A. (2022). Classification of Virtual Private networks encrypted traffic using ensemble learning algorithms. *Egyptian Informatics Journal*, 23 (4), 57–68. doi: <https://doi.org/10.1016/j.eij.2022.06.006>
- Balachandran, A., Amritha, P. P. (2022). VPN Network Traffic Classification Using Entropy Estimation and Time-Related Features. *Smart Innovation, Systems and Technologies*, 509–520. doi: https://doi.org/10.1007/978-981-16-3945-6_50
- Ma, X., Zhu, W., Wei, J., Jin, Y., Gu, D., Wang, R. (2023). EETC: An extended encrypted traffic classification algorithm based on variant resnet network. *Computers & Security*, 128, 103175. doi: <https://doi.org/10.1016/j.cose.2023.103175>
- Naas, M., Fesl, J. (2023). A novel dataset for encrypted virtual private network traffic analysis. *Data in Brief*, 47, 108945. doi: <https://doi.org/10.1016/j.dib.2023.108945>
- Lemeshko, O., Lebedenko, T., Nevzorova, O., Snihurov, A., Mersni, A., Al-Dulaimi, A. (2019). Development of the Balanced Queue Management Scheme with Optimal Aggregation of Flows and Bandwidth Allocation. 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM). doi: <https://doi.org/10.1109/cadsm.2019.8779246>
- Patil, H. K., Chen, T. M. (2017). *Wireless Sensor Network Security. Computer and Information Security Handbook*, 317–337. doi: <https://doi.org/10.1016/b978-0-12-803843-7.00018-1>
- Afuwape, A. A., Xu, Y., Anajemba, J. H., Srivastava, G. (2021). Performance evaluation of secured network traffic classification using a machine learning approach. *Computer Standards & Interfaces*, 78, 103545. doi: <https://doi.org/10.1016/j.csi.2021.103545>
- Geyer, F., Scheffler, A., Bondorf, S. (2023). Network Calculus With Flow Prolongation – A Feedforward FIFO Analysis Enabled by ML. *IEEE Transactions on Computers*, 72 (1), 97–110. doi: <https://doi.org/10.1109/tc.2022.3204225>
- Kovalenko, A., Kuchuk, H., Tkachov, V. (2021). Method of ensuring the survivability of the computer network based on vpn-tunneling. *Control, Navigation and Communication Systems. Academic Journal*, 1 (63), 90–95. doi: <https://doi.org/10.26906/sunz.2021.1.090>
- Kuchuk, N., Gavrylenko, S., Sobchuk, V., Lukova-Chuiko, N. (2019). Redistribution of information flows in a hyperconvergent system. *Advanced Information Systems*, 3 (2), 116–121. doi: <https://doi.org/10.20998/2522-9052.2019.2.20>
- Svyrydov, A., Kovalenko, A., Kuchuk, H. (2018). The pass-through capacity redevelopment method of net critical section based on improvement ON/OFF models of traffic. *Advanced Information Systems*, 2 (2), 139–144. doi: <https://doi.org/10.20998/2522-9052.2018.2.24>
- ITU-T Technical Report. XSTR-SEC-MANUAL Security in telecommunications and information technology (7th edition) (2022). International Telecommunication Union. Available at: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTSS-2020-4-PDF-E.pdf
- Y.1541: Network performance objectives for IP-based services (2011). Available at: <https://www.itu.int/rec/T-REC-Y.1541-201112-I/en>
- Hnatushenko, V. V. (2014) Modeliuvannia ahrehovanoho trafiku peredachi danykh na osnovi modeli ON/OFF. *Systemni tekhnolohiyi*, 5, 65–72. Available at: http://nbuv.gov.ua/UJRN/st_2014_5_10

22. Lebedenko, T., Goloveshko, M., Holodkova, A. (2019). Investigation of the method of active queue management on the interfaces of telecommunication networks routers. *Control, Navigation and Communication Systems. Academic Journal*, 4 (56), 57–62. doi: <https://doi.org/10.26906/sunz.2019.4.057>
23. Lebedenko, T., Goloveshko, M., Severilov, A. (2019). The results of the experimental study of the Active Queue Management method at the interfaces of telecommunication networks. *Problems of Telecommunications*, 2 (25), 37–55. doi: <https://doi.org/10.30837/pt.2019.2.03>
24. Gnatyuk, S., Kinzyryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., Odarchenko, R. (2019). Secure Hash Function Constructing for Future Communication Systems and Networks. *Advances in Intelligent Systems and Computing*, 561–569. doi: https://doi.org/10.1007/978-3-030-12082-5_51
25. Brumnik, R., Kovtun, V., Okhrimenko, A., Kavun, S. (2014). Techniques for Performance Improvement of Integer Multiplication in Cryptographic Applications. *Mathematical Problems in Engineering*, 2014, 1–7. doi: <https://doi.org/10.1155/2014/863617>
26. Odarchenko, R., Gnatyuk, V., Gnatyuk, S., Abakumova, A. (2018). Security Key Indicators Assessment for Modern Cellular Networks. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). doi: <https://doi.org/10.1109/saic.2018.8516889>
27. Berkman, L., Turovsky, O., Kyrpach, L., Varfolomeeva, O., Dmytrenko, V., Pokotylo, O. (2021). Analyzing the code structures of multidimensional signals for a continuous information transmission channel. *Eastern-European Journal of Enterprise Technologies*, 5 (9 (113)), 70–81. doi: <https://doi.org/10.15587/1729-4061.2021.242357>

DOI: 10.15587/1729-4061.2023.286187

CONSTRUCTING THE MATHEMATICAL MODEL OF A RECOMMENDER SYSTEM FOR DECENTRALIZED PEER-TO-PEER COMPUTER NETWORKS (p. 24–35)

Volodymyr Mikhav

Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine

ORCID: <https://orcid.org/0000-0003-4816-4680>

Serhii Semenov

Pedagogical University of Krakow, Krakow, Poland

ORCID: <https://orcid.org/0000-0003-4472-9234>

Yelyzaveta Meleshko

Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine

ORCID: <https://orcid.org/0000-0001-8791-0063>

Mykola Yakymenko

Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine

ORCID: <https://orcid.org/0000-0003-3290-6088>

Yaroslav Shulika

Central Ukrainian National Technical University,
Kropyvnytskyi, Ukraine

ORCID: <https://orcid.org/0000-0002-6713-7269>

Recommender systems make it easier to search with a large amount of content, supplementing or replacing the classic search output with recommendations. In P2P networks, their use can have additional benefits. Because of indexing and search problems, previously added files may not be available to P2P network users. If the user cannot find the file he is looking for, one can provide him with a list of recommendations based on his preferences and search query.

The object of research is the process of creating recommendations for users of decentralized P2P networks to facilitate data search.

The urgent task of increasing the accuracy of mathematical modeling of recommender systems by taking into account the requirements for reliability and data security during changes in the structure of a decentralized P2P network is solved.

An analytical model of the recommender system of a decentralized P2P network has been developed, the main feature of which is taking into account the requirements of reliability and security of recommendation messages. This was done by introducing the following indicators into the general model of the decentralized recommender system – the probability of reliable packet transmission and the probability of safe packet transmission. The developed analytical model makes it possible to conduct a comparative analysis of different methods of operation of recommender systems and to set acceptable parameters under which the degree of relevance does not fall below a certain threshold.

The developed mathematical model of the system based on the GERT scheme differs from the known ones by taking into account the reliability and security requirements during changes in the structure of the decentralized P2P network. This has made it possible to improve the accuracy of simulation results up to 5 %.

The proposed mathematical model could be used for prototyping recommender systems in various fields of activity.

Keywords: recommender system, decentralized computer network, peer-to-peer network, GERT network, information security.

References

1. Fayyaz, Z., Ebrahimiyan, M., Nawara, D., Ibrahim, A., Kashef, R. (2020). Recommendation Systems: Algorithms, Challenges, Metrics, and Business Opportunities. *Applied Sciences*, 10 (21), 7748. doi: <https://doi.org/10.3390/app10217748>
2. Falk, K. (2019). *Practical recommender systems*. Manning, 432.
3. Roy, D., Dutta, M. (2022). A systematic review and research perspective on recommender systems. *Journal of Big Data*, 9 (1). doi: <https://doi.org/10.1186/s40537-022-00592-5>
4. Fulber-Garcia, V. (2023). Centralized Computing vs. Distributed Computing. *Baeldung*. Available at: <https://www.baeldung.com/cs/centralized-vs-distributed-computing>
5. Vergne, J. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. *Organization Theory*, 1 (4), 263178772097705. doi: <https://doi.org/10.1177/2631787720977052>
6. Kosalka, T. (2006). Decision making through the simulation of centralized and decentralized distribution storage systems. doi: <https://doi.org/10.33915/etd.1709>
7. Gong, S., Ye, H., Su, P. (2009). A Peer-to-Peer Based Distributed Collaborative Filtering Architecture. 2009 International Joint Conference on Artificial Intelligence. doi: <https://doi.org/10.1109/jcai.2009.154>
8. Karaarslan, E., Konacaklı, E. (2020). Data Storage in the Decentralized World: Blockchain and Derivatives. *Who Runs the World: Data*, 37–69. doi: <https://doi.org/10.26650/b/et06.2020.011.03>
9. Si, M., Li, Q. (2018). Shilling attacks against collaborative recommender systems: a review. *Artificial Intelligence Review*, 53 (1), 291–319. doi: <https://doi.org/10.1007/s10462-018-9655-x>
10. Meleshko, Y., Drieiev, O., Yakymenko, M., Lysytsia, D. (2020). Developing a model of the dynamics of states of a recommendation system under conditions of profile injection attacks. *Eastern-European Journal of Enterprise Technologies*, 4 (2 (106)), 14–24. doi: <https://doi.org/10.15587/1729-4061.2020.209047>

11. Meleshko, Y. V., Yakymenko, M., Semenov, S. (2021). A Method of Detecting Bot Networks Based on Graph Clustering in the Recommendation System of Social Network. *Computational Linguistics and Intelligent Systems*, 2870. Available at: <https://ceur-ws.org/Vol-2870/paper92.pdf>
12. The BitTorrent Protocol Specification (2017). Available at: http://www.bittorrent.org/beps/bep_0003.html
13. Gnutella Protocol Development (2003). Available at: <https://rfc-gnutella.sourceforge.net>
14. Kademia: A Design Specification (2010). Available at: <https://xlattice.sourceforge.net/components/protocol/kademia/specs.html>
15. Stoica, I., Morris, R., Karger, D., Kaashoek, M. F., Balakrishnan, H. (2001). Chord. *ACM SIGCOMM Computer Communication Review*, 31 (4), 149–160. doi: <https://doi.org/10.1145/964723.383071>
16. Zhang, S., Yin, H., Chen, T., Huang, Z., Nguyen, Q. V. H., Cui, L. (2022). PipAttack: Poisoning Federated Recommender Systems for Manipulating Item Promotion. *Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*. doi: <https://doi.org/10.1145/3488560.3498386>
17. Mohammed, A. S., Meleshko, Y., Balaji B. S., Serhii, S. (2019). Collaborative Filtering Method with the use of Production Rules. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. doi: <https://doi.org/10.1109/iccike47802.2019.9004257>
18. Ko, H., Lee, S., Park, Y., Choi, A. (2022). A Survey of Recommendation Systems: Recommendation Models, Techniques, and Application Fields. *Electronics*, 11 (1), 141. doi: <https://doi.org/10.3390/electronics11010141>
19. Naeen, H. M., Jalali, M. (2019). A decentralized trust-aware collaborative filtering recommender system based on weighted items for social tagging systems. *arXiv*. doi: <https://doi.org/10.48550/arXiv.1906.05143>
20. Wang, Y., Han, S., Zhou, J., Chen, L., Chen, C. L. P., Zhang, T. et al. (2023). Random Feature-Based Collaborative Kernel Fuzzy Clustering for Distributed Peer-to-Peer Networks. *IEEE Transactions on Fuzzy Systems*, 31 (2), 692–706. doi: <https://doi.org/10.1109/tfuzz.2022.3188363>
21. Wang, T., Wang, M. (2018). Distributed collaborative filtering recommendation algorithm based on DHT. *Cluster Computing*, 22 (S2), 2931–2941. doi: <https://doi.org/10.1007/s10586-018-1699-9>
22. Zhao, Z., Wang, Y., Wang, H. (2021). SDN-based cross-domain cooperative method for trusted nodes recommendation in Mobile crowd sensing. *Peer-to-Peer Networking and Applications*, 14 (6), 3793–3805. doi: <https://doi.org/10.1007/s12083-021-01217-z>
23. Lisi, A., De Salve, A., Mori, P., Ricci, L. (2019). A Smart Contract Based Recommender System. *Lecture Notes in Computer Science*, 29–42. doi: https://doi.org/10.1007/978-3-030-36027-6_3
24. Bobadilla, D., Lipizzi, C. (2021). A Blockchain-Based Collaborative Filtering Recommendation System Based on Trust. *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. doi: <https://doi.org/10.1109/iccwamtip53232.2021.9674128>
25. Badis, L., Amad, M., Aissani, D., Abbar, S. (2021). P2PCF: A collaborative filtering based recommender system for peer to peer social networks. *Journal of High Speed Networks*, 27 (1), 13–31. doi: <https://doi.org/10.3233/jhs-210649>
26. Yoo, H., Chung, K. (2017). Mining-based lifecare recommendation using peer-to-peer dataset and adaptive decision feedback. *Peer-to-Peer Networking and Applications*, 11 (6), 1309–1320. doi: <https://doi.org/10.1007/s12083-017-0620-2>
27. Zeng, X., Yu, X. (2023). P2P based on network behavior analysis trust value calculation method. *International Conference on Computer Network Security and Software Engineering (CNSSE 2023)*. doi: <https://doi.org/10.1117/12.2683177>
28. Semenov, S., Zhang, L., Cao, W., Bulba, S., Babenko, V., Davydov, V. (2021). Development of a fuzzy GERT-model for investigating common software vulnerabilities. *Eastern-European Journal of Enterprise Technologies*, 6 (2 (114)), 6–18. doi: <https://doi.org/10.15587/1729-4061.2021.243715>
29. Semenov, S., Liqiang, Z., Weiling, C., Davydov, V. (2021). Development a mathematical model for the software security testing first stage. *Eastern-European Journal of Enterprise Technologies*, 3 (2 (111)), 24–34. doi: <https://doi.org/10.15587/1729-4061.2021.233417>
30. Netflix Prize data: Dataset from Netflix's competition to improve their recommendation algorithm. Available at: <https://www.kaggle.com/datasets/netflix-inc/netflix-prize-data?resource=download>

DOI: 10.15587/1729-4061.2023.282100

DEVISING A METHOD FOR INCREASING THE NOISE IMMUNITY OF SYSTEMS WITH ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING UNDER THE CONDITIONS OF INTER-CHANNEL INTERFERENCE (p. 36–44)

Rostyslav Bykov

State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine

ORCID: <https://orcid.org/0000-0002-1020-1733>

Modern communication systems are based on orthogonal frequency division multiplexing (OFDM) technology, which allows reliable transmission of information under multipath conditions. The need to preserve the orthogonal properties of subcarriers leads to high sensitivity of these systems to frequency shifts of the signal. The method of signal formation for the OFDM system has been improved in this work. The use of spectrum-selective shaping pulses after the inverse fast Fourier transform (IFFT) stage at the transmitter side to reduce the level of inter-channel interference during carrier frequency shift was investigated. New pulse shapes were synthesized, obtained by using optimized multiparameter functions with a selective spectrum. The effectiveness of the application of synthesized pulses with a selective spectrum in reducing the influence of the frequency shift of the signal on the interference immunity of the OFDM system was analyzed. A comparison of the probability of a bit error with already existing forms of Nyquist pulses was carried out. In the MATLAB environment, a model of the transmitter and receiver of the OFDM system was developed for the experimental assessment of the influence of the proposed forming pulses on the immunity of the system under the conditions of inter-channel interference with different types of modulation. It was established that the lowest level of bit error probability under the conditions of inter-channel interference was observed for a two-parameter pulse with a selective spectrum and a piecewise linear approximation of the transition region. So, for a signal-to-noise ratio of 15 dB, BPSK modulation and a normalized frequency shift of 0.2, the probability of a bit error for a given pulse is $3 \cdot 10^{-4}$; for QPSK modulation and a normalized frequency shift of 0.1, 10^{-6} ; for QAM-16 modulation and a normalized frequency shift of 0.03, $2 \cdot 10^{-4}$.

Keywords: Nyquist shaping pulse, pulse with a selective spectrum, piecewise linear approximation, interchannel interference, OFDM.

References

1. Singh, P., Sahu, O. P. (2015). An Overview of ICI Self Cancellation Techniques in OFDM Systems. *2015 IEEE International Conference*

- on Computational Intelligence & Communication Technology. doi: <https://doi.org/10.1109/cict.2015.113>
2. Kumar, N., Kaur, G., Sohi, B. S. (2015). Comparative Analysis of Various Inter-Carrier Interference Cancellation Methods. *International Journal of Wireless and Microwave Technologies*, 5 (3), 18–32. doi: <https://doi.org/10.5815/ijwmt.2015.03.02>
 3. Tan, P., Beaulieu, N. C. (2009). Analysis of the effects of Nyquist pulse-shaping on the performance of OFDM systems with carrier frequency offset. *European Transactions on Telecommunications*, 20 (1), 9–22. doi: <https://doi.org/10.1002/ett.1316>
 4. Muschallik, C. (1996). Improving an OFDM reception using an adaptive Nyquist windowing. *IEEE Transactions on Consumer Electronics*, 42 (3), 259–269. doi: <https://doi.org/10.1109/30.536046>
 5. ETSI TS 136 211 V17.1.0 LTE. Evolved Universal Terrestrial Radio Access (E-UTRA). Physical channels and modulation. Available at: https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/17.01.00_60/ts_136211v170100p.pdf
 6. Muller-Weinfurtner, S. H., Huber, J. B. (2000). Optimum Nyquist windowing for improved OFDM receivers. *Globecom '00 - IEEE. Global Telecommunications Conference. Conference Record (Cat. No.00CH37137)*. doi: <https://doi.org/10.1109/glocom.2000.891232>
 7. Song, R., Guo, X., Leung, S. H. (2011). Optimum Second Order Polynomial Nyquist Windows for Reduction of ICI in OFDM Systems. *Wireless Personal Communications*, 65 (2), 455–467. doi: <https://doi.org/10.1007/s11277-011-0267-x>
 8. Kamal, S., Azurdia-Meza, C. A., Lee, K. (2016). Suppressing the effect of ICI power using dual sinc pulses in OFDM-based systems. *AEU - International Journal of Electronics and Communications*, 70 (7), 953–960. doi: <https://doi.org/10.1016/j.aeue.2016.04.013>
 9. Kamal, S., Azurdia-Meza, C. A., Lee, K. (2017). Improved Nyquist-Pulses to Enhance the Performance of OFDM-Based Systems. *Wireless Personal Communications*, 95 (4), 4095–4111. doi: <https://doi.org/10.1007/s11277-017-4044-3>
 10. Balan, A. L., Alexandru, N. D. (2012). Two improved nyquist filters with piece-wise rectangular-polynomial frequency characteristics. *AEU - International Journal of Electronics and Communications*, 66 (11), 880–883. doi: <https://doi.org/10.1016/j.aeue.2012.03.006>
 11. Alexandru, N. D., Balan, A. L., Diaconu, F., Dimian, M. (2013). Development of Improved Nyquist Filters with piecewise linear frequency characteristics. 2013 36th International Conference on Telecommunications and Signal Processing (TSP). doi: <https://doi.org/10.1109/tsp.2013.6614023>
 12. Alexandru, N. D., Balan, A. L. (2014). Investigation of the mechanism of improvement in improved Nyquist filters. *IET Signal Processing*, 8 (1), 95–105. doi: <https://doi.org/10.1049/iet-spr.2013.0050>
 13. Sharique, M., Chaturvedi, A. K. (2015). Transmitter Pulse Shaping to Reduce OOB Power and ICI in OFDM Systems. *Wireless Personal Communications*, 83 (2), 1567–1578. doi: <https://doi.org/10.1007/s11277-015-2464-5>
 14. Xiao, J., Yu, J., Cao, Z., Li, F., Chen, L. (2013). Flipped-exponential Nyquist pulse technique to optimize the PAPR in optical direct detection OFDM system. *Optics Communications*, 286, 176–181. doi: <https://doi.org/10.1016/j.optcom.2012.08.053>
 15. Jayaprakash, A., Reddy, G. R. (2015). Discrete Ambiguity Function Based Analysis of Filter Bank Multicarrier Systems. *IETE Technical Review*, 32 (5), 330–346. doi: <https://doi.org/10.1080/02564602.2015.1015941>
 16. Kongara, K. P., Smith, P. J., Mann, S. (2008). A comparison of CP-OFDM with IOTA-OFDM under typical system imperfections. *IET Seminar Digests*. doi: <https://doi.org/10.1049/ic.2008.0694>
 17. Sukachev, E. A. (2016). *Vvedenie v teoriyu signalov Naykvista*. Odessa: Osvita Ukrainy, 108.
 18. Proakis, J. G., Salehi, M. (2008). *Digital Communications*. McGraw-Hill. Available at: https://edisciplinas.usp.br/pluginfile.php/5636847/mod_resource/content/1/digital%20commun%205th%20-%20proakis%2C%20salehi.pdf
-
- DOI: 10.15587/1729-4061.2023.285540**
- DEVELOPMENT OF AN ERROR CORRECTION METHOD USING PERFECT BINARY ARRAYS (p. 45–53)**
- Pierre Murr**
International University of Science and Technology in Kuwait,
Ardiya Government Area, Kuwait
ORCID: <https://orcid.org/0009-0007-4094-0223>
- Serhii Yevseiev**
National Technical University “Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine
ORCID: <https://orcid.org/0000-0003-1647-6444>
- Stanislav Milevskiy**
National Technical University “Kharkiv Polytechnic Institute”,
Kharkiv, Ukraine
ORCID: <https://orcid.org/0000-0001-5087-7036>
- Marharyta Melnyk**
Private Institution «University of Science, Entrepreneurship
and Technologies», Kyiv, Ukraine
ORCID: <https://orcid.org/0000-0003-0619-7281>
- Vitaliy Katsalap**
The National Defence University of Ukraine named after Ivan
Cherniakhovskiy, Kyiv, Ukraine
ORCID: <https://orcid.org/0000-0003-4804-8022>
- Yurii Prybyliev**
The National Defence University of Ukraine named after Ivan
Cherniakhovskiy, Kyiv, Ukraine
ORCID: <https://orcid.org/0000-0003-1941-3561>
- Khazail Rzayev**
Azerbaijan Technical University, Baku, Azerbaijan
ORCID: <https://orcid.org/0000-0001-9272-4302>
- Andrii Bryla**
Uzhhorod National University, Uzhhorod, Ukraine
ORCID: <https://orcid.org/0000-0003-2518-9877>
- Oleksandr Shpak**
Uzhhorod National University, Uzhhorod, Ukraine
ORCID: <https://orcid.org/0000-0002-1179-7196>
- Pavlo Fedorka**
Uzhhorod National University, Uzhhorod, Ukraine
ORCID: <https://orcid.org/0000-0002-9242-5588>
- The research focuses on an innovative error correction method that uses perfect binary arrays (PBAs), a powerful mathematical tool with unique properties that make it ideal for error correction. The research is aimed at studying the impact of uncorrelated mixed-type errors in the data exchange path, which allows using it in smart technologies with limited computing capabilities. The effectiveness of the approach is confirmed by simulation and comparison with other error correction methods. In order to further study the structural, cross-correlation and distance properties of orthogonal two-dimensional codes and the correcting capabilities of the proposed method, an information technology system for data transmission based on an equivalent class of

perfect binary arrays has been developed. The proposed model evaluates the performance of the error correction code based on perfect binary arrays under various conditions, including correlated and uncorrelated interference and data exchange paths. A generator of PBA of equivalent classes has been built. An experimental evaluation of the correcting ability of the proposed two-dimensional codes was carried out by simulating various pre-code situations, including packet and random errors, for the cases of correlated and uncorrelated interference. Using a graphical interface, users will be able to enter the number and type of errors, determine whether they are random or packet errors, manually or automatically, move errors through the data packet, and view intermediate results. Thus, the complex nature of this study can be positioned as a promising approach and a reliable choice in the field of error correction.

Keywords: error correction information coding, error detection, perfect binary arrays.

References

- Lin, S., Costello, D. J. (2001). *Error Control Coding*. Prentice-Hall. Available at: <https://pg024ec.files.wordpress.com/2013/09/error-control-coding-by-shu-lin.pdf>
- Belim, S. V., Larionov, I. B. (2020). Noise proof coding based on orthogonal functions. *Journal of Physics: Conference Series*, 1441 (1), 012034. doi: <https://doi.org/10.1088/1742-6596/1441/1/012034>
- Kumari, S., Gahalod, L., Changlani, S. (2022). Study of Different Types of Error Detection and Correction Code in Wireless Communication. *International Journal of Scientific Research in Science, Engineering and Technology*, 9 (3), 448–455. doi: <https://doi.org/10.32628/ijrsret2293138>
- Patil, A., Darkunde, N. (2018). Algorithmic Approach for Error-Correcting Capability and Decoding of Linear Codes Arising from Algebraic Geometry. *Lecture Notes in Networks and Systems*, 509–517. doi: https://doi.org/10.1007/978-981-13-0586-3_51
- Huffman, W. C., Pless, V. (2003). *Fundamentals of error-correcting codes*. Cambridge University Press. doi: <https://doi.org/10.1017/cbo9780511807077>
- Moon, T. K. (2005). *Error Correction Coding*. John Wiley & Sons. doi: <https://doi.org/10.1002/0471739219>
- Salija, P., Yamuna, B., Padmanabhan, T. R., Mishra, D. (2022). A Generic Reliability Based Direct Decoding Algorithm for Turbo Codes. *Wireless Personal Communications*, 125 (1), 785–801. doi: <https://doi.org/10.1007/s11277-022-09577-2>
- Sholiyi, A.O. (2011). Irregular Block Turbo Codes for Communication Systems. Swansea University. Available at: <https://core.ac.uk/download/pdf/161881205.pdf>
- Venkatesh, D. Y., Mallikarjunaiah, K., Srikantaswamy, M. (2022). A Comprehensive Review of Low Density Parity Check Encoder Techniques. *Ingénierie Des Systèmes d'Information*, 27 (1), 11–20. doi: <https://doi.org/10.18280/isi.270102>
- Süzer, A. E., Oktal, H. (2023). A comparison analysis on forward error correction technology: a future perspective for GNSS. *Aircraft Engineering and Aerospace Technology*, 95 (8), 1311–1320. doi: <https://doi.org/10.1108/aeat-10-2021-0319>
- Abdelkareem, A. E. (2022). Hardware considerations of a DSP based wireless coded receiver under limited resources. *2022 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IOE)*. doi: <https://doi.org/10.1109/itss-ioe56359.2022.9990939>
- Saiz-Adalid, L.-J., Gracia-Moran, J., Gil-Tomas, D., Baraza-Calvo, J.-C., Gil-Vicente, P.-J. (2019). Ultrafast Codes for Multiple Adjacent Error Correction and Double Error Detection. *IEEE Access*, 7, 151131–151143. doi: <https://doi.org/10.1109/access.2019.2947315>
- Sokolov, A. (2019). Interrelation Between the Class of Bent-Sequences and the Class of Perfect Binary Arrays. *Computer Modeling and Intelligent Systems*, 2353, 339–349. doi: <https://doi.org/10.32782/cmis/2353-27>
- Jedwab, J., Li, S. (2022). Group rings and character sums: tricks of the trade. *arXiv*. doi: <https://doi.org/10.48550/arXiv.2211.11986>
- Goresky, M., Klapper, A. (2012). *Algebraic Shift Register Sequences*. Cambridge University Press. doi: <https://doi.org/10.1017/cbo9781139057448>
- Hedayat, A. S., Sloane, N. J. A., Stufken, J. (1999). *Orthogonal Arrays*. Springer Series in Statistics. Springer. doi: <https://doi.org/10.1007/978-1-4612-1478-6>
- Yurish, S. (2019). *Advances in Networks, Security and Communications: Reviews, Vol. 2*. All Rights Reserved - Standard Copyright License, 145–188. Available at: <https://www.lulu.com/shop/sergey-yurish/advances-in-networks-security-and-communications-reviews-vol-2/paperback/product-1gqqegqz.html?page=1&pageSize=4>
- Jedwab, J., Mitchell, C., Piper, F., Wild, P. (1994). Perfect binary arrays and difference sets. *Discrete Mathematics*, 125 (1-3), 241–254. doi: [https://doi.org/10.1016/0012-365x\(94\)90165-1](https://doi.org/10.1016/0012-365x(94)90165-1)
- Wild, P. (1988). Infinite families of perfect binary arrays. *Electronics Letters*, 24 (14), 845. doi: <https://doi.org/10.1049/el:19880575>
- Mazurkov, M., Chechel'nitskii, V. Y. (2003). The classes of equivalent and generative perfect binary arrays for cdma-technologies. *Radioelectronics and Communications Systems*, 46 (5), 40–46.
- Bomer, L., Antweiler, M. (1990). Two-dimensional perfect binary arrays with 64 elements. *IEEE Transactions on Information Theory*, 36 (2), 411–414. doi: <https://doi.org/10.1109/18.52492>
- Mazurkov, M. I., Chechel'nitskii, V. Ya., Murr, P. (2008). Information security method based on perfect binary arrays. *Radioelectronics and Communications Systems*, 51 (11), 612–614. doi: <https://doi.org/10.3103/s0735272708110095>
- Pless, V., Huffman, W. C. (Eds.) (1998). *Handbook of Coding Theory*. Elsevier.
- Dovgyi, S., Kopyika, O. (2022). Standard Model of System Architecture of Enterprise IT Infrastructure. *Lecture Notes in Networks and Systems*, 181–201. doi: https://doi.org/10.1007/978-3-031-16368-5_9
- Dovgyi, S., Kopyika, O., Kozlov, O. (2021). Architectures for the Information Systems, Network Resources, and Network Services (short paper). *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II. Volume I. Co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2021)*, 293–301. Available at: <https://ceur-ws.org/Vol-3187/short9.pdf>
- Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. *Eastern-European Journal of Enterprise Technologies*, 2 (9 (116)), 44–59. doi: <https://doi.org/10.15587/1729-4061.2022.254545>
- Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytskyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). *Modeling of security systems for critical infrastructure facilities*. Kharkiv:

PC TECHNOLOGY CENTER, 196. doi: <https://doi.org/10.15587/978-617-7319-57-2>

DOI: 10.15587/1729-4061.2023.285261
DEVELOPING A NEW ENCRYPTION ALGORITHM FOR IMAGES TRANSMITTED THROUGH WSN SYSTEMS (p. 54–60)

Sanaa ahmed kadhim

University of Information Technology and Communications,
Baghdad, Iraq

ORCID: <https://orcid.org/0000-0002-0133-8914>

Ruwaida Mohammed yas

Informatics Institute for Post-Graduation Studies (IIPS) / Iraqi
Commission for Computer & Informatics (ICCI), Baghdad, Iraq

ORCID: <https://orcid.org/0000-0002-1867-7402>

Saad abdual azize Abdul Rahman

AL-Ma'moon University College, Baghdad, Iraq

ORCID: <https://orcid.org/0000-0002-0111-8844>

Sura Khalil Abd

Dijlah University College, Baghdad, Iraq, 00964

ORCID: <https://orcid.org/0000-0002-9582-3725>

Wireless sensor networks (WSNs) have up until now faced many challenges because of their open, wide-ranging, and resource-limited nature, including security, efficiency, and energy consumption. In the military system, it is essential to provide high-level security to the significant data over wireless network which is proved to be unreliable public communications. To solve the above problem, high level of security with minimum complexity should be applied to be adequate to limited capabilities of transmission system. This paper presents a new algorithm named (SRS) for encrypting transmitted military images to keep them from getting hacked or broken by WSN. The SRS algorithm is designed to be lightweight, fast, and secure, taking into consideration the limited capabilities of the transmission system. It is implemented as a public key cryptosystem specifically designed for image encryption. The algorithm consists of two parts: encryption and decryption. The proposed system suggested some equations and calculations that are applied to the plain and coded images after being transmitted over the WSN. The results of testing the simulation model demonstrate the effectiveness of the system by evaluation using various metrics such as Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). Overall, the paper presents a new encryption algorithm, SRS, specifically designed for securing military images transmitted over wireless sensor networks. The algorithm aims to provide a balance between security, efficiency, and energy consumption, considering the resource-limited nature of WSNs. The simulation results indicate the improvement of the proposed system by 13 %, 10 %, and 55 % in packet delivery ratio (PDR), throughput, and dropping ratio, respectively, and it shows that the suggested SRS method increased execution time by 67 % compared to RSA based algorithm.

Keywords: wireless sensor network (WSN), military system SRS algorithm image encryption.

References

1. Khashan, O. A., Ahmad, R., Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, 115, 102448. doi: <https://doi.org/10.1016/j.adhoc.2021.102448>
2. Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., Liu, J. (2019). A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network. *IEEE Access*, 7, 53079–53090. doi: <https://doi.org/10.1109/access.2019.2911395>
3. Khashan, O. A. (2020). Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment. *IEEE Access*, 8, 66878–66887. doi: <https://doi.org/10.1109/access.2020.2984317>
4. Yas, R. M., Hashim, S. (2021). Intelligent Approaches for Enhancing Networked Routing Protocol. *Iraqi Journal of Science*, 4121–4147. doi: <https://doi.org/10.24996/ij.s.2021.62.11.32>
5. Mathur, S., Gupta, D., Goar, V., Kuri, M. (2017). Analysis and design of enhanced RSA algorithm to improve the security. 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT). doi: <https://doi.org/10.1109/ciaict.2017.7977330>
6. Rafash, A. G. H., Saeed, E. M. H., Talib, A.-S. M. (2021). Development of an enhanced scatter search algorithm using discrete chaotic Arnold's cat map. *Eastern-European Journal of Enterprise Technologies*, 6 (4 (114)), 15–20. doi: <https://doi.org/10.15587/1729-4061.2021.234915>
7. Khashan, O. A., Zin, A. M., Sundararajan, E. A. (2014). Performance study of selective encryption in comparison to full encryption for still visual images. *Journal of Zhejiang University SCIENCE C*, 15 (6), 435–444. doi: <https://doi.org/10.1631/jzus.c1300262>
8. Kadhim, S. A., abdual Rahman, S. A. A. (2021). A proposed method for encrypting and sending confidential data using polynomials. *Global Journal of Engineering and Technology Advances*, 8 (2), 082–087. doi: <https://doi.org/10.30574/gjeta.2021.8.2.0133>
9. Szalachowski, P., Kotulski, Z. (2012). One-Time Broadcast Encryption Schemes in Distributed Sensor Networks. *International Journal of Distributed Sensor Networks*, 8 (3), 536718. doi: <https://doi.org/10.1155/2012/536718>
10. Muhajjar, R. A., Flayh, N. A., Al-Zubaidie, M. (2023). A Perfect Security Key Management Method for Hierarchical Wireless Sensor Networks in Medical Environments. *Electronics*, 12 (4), 1011. doi: <https://doi.org/10.3390/electronics12041011>
11. Wazery, Y. M., Ali, M. A. S. (2018). An Intuitionistic Fuzzy Sets Implementation for Key Distribution in Hybrid Message Encryption Over Wsns. *International Journal of Advances in Applied Sciences*, 7 (3), 273. doi: <https://doi.org/10.11591/ijaas.v7.i3.pp273-285>
12. Zhao, G., Yang, X., Zhou, B., Wei, W. (2010). RSA-based digital image encryption algorithm in wireless sensor networks. 2010 2nd International Conference on Signal Processing Systems. doi: <https://doi.org/10.1109/icsps.2010.5555601>
13. Elhoseny, M., Elminir, H., Riad, A., Yuan, X. (2016). A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. *Journal of King Saud University - Computer and Information Sciences*, 28 (3), 262–275. doi: <https://doi.org/10.1016/j.jksuci.2015.11.001>
14. Ramasamy, J., Kumaresan, J. S. (2020). Image Encryption and Cluster Based Framework for Secured Image Transmission in Wireless Sensor Networks. *Wireless Personal Communications*, 112 (3), 1355–1368. doi: <https://doi.org/10.1007/s11277-020-07106-7>
15. Leelavathi, G., Shaila, K., Venugopal, K. R. (2020). Message and Image Encryption Embedding Data to GF(2m) Elliptic Curve Point for Nodes in Wireless Sensor Networks. *EAI/Springer Innovations in Communication and Computing*, 329–338. doi: https://doi.org/10.1007/978-3-030-19562-5_33
16. Li, H., Ge, B., Xia, C., Wang, T. (2021). Image Encryption for Wireless Sensor Networks with Modified Logistic Map and New Hash

Algorithm. *Wireless Algorithms, Systems, and Applications*, 29–37. doi: https://doi.org/10.1007/978-3-030-86137-7_4

17. Abdulhameed, H. A., Abdalmaen, H. F., Mohammed, A. T., Mosleh, M. F., Abdulhameed, A. A. (2022). A Lightweight Hybrid Cryptographic Algorithm for WSNs Tested by the Diehard Tests and the Raspberry Pi. 2022 International Conference on Computer Science and Software Engineering (CSASE). doi: <https://doi.org/10.1109/csase51777.2022.9759589>
18. Aruna Deepthi, S., Aruna, V., Leelavathi, R. (2022). Image Transmission Using Leach and Security Using RSA in Wireless Sensor Networks. *Advances in Intelligent Systems and Computing*, 39–51. doi: https://doi.org/10.1007/978-981-16-9573-5_3

DOI: 10.15587/1729-4061.2023.286466
USING SOFTWARE-DEFINED RADIO RECEIVERS FOR DETERMINING THE COORDINATES OF LOW-VISIBLE AERIAL OBJECTS (p. 61–73)

Hennadii Khudov

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

Oleksandr Kostianets

Ivan Kozhedub Kharkiv National Air Force University,
 Kharkiv, Ukraine
ORCID: <https://orcid.org/0009-0002-8936-2544>

Oleksandr Kovalenko

Central Ukrainian National Technical University,
 Kropyvnytskyi, Ukraine
ORCID: <https://orcid.org/0000-0001-9297-0650>

Oleh Maslenko

Scientific-Research Institute of Military Intelligence,
 Kyiv, Ukraine
ORCID: <https://orcid.org/0000-0001-6963-6574>

Yuriy Solomonenko

Ivan Kozhedub Kharkiv National Air Force University,
 Kharkiv, Ukraine
ORCID: <https://orcid.org/0000-0002-6503-7475>

The object of this study is the process of determining the coordinates of low-visible aerial objects. The main hypothesis of the research assumed that the signals emitted by airborne systems of airborne objects that are not visible to radar stations have a greater power than the signal reflected from the airborne object. This, in turn, could improve the signal/noise ratio and, accordingly, the accuracy of determining the coordinates of low-visible aerial objects. It is suggested to use Software-Defined Radio receivers to receive such signals emitted by on-board systems of low-visible aerial objects.

It was established that the main sources of signals for Software-Defined Radio receivers are signals of command, telemetry, target channels, manual control channels, and satellite navigation. It was established that an additional distinguishing feature when determining the coordinates of low-visible aerial objects is the uniqueness of their spectra and spectrograms.

The method of determining the coordinates of low-visible aerial objects when using Software-Defined Radio receivers has been improved, which, unlike the known ones, involves:

- the use as signals for Software-Defined Radio of signal receivers of on-board equipment of low-visible aerial objects;
- the use of a priori coordinate values of a low-visible aerial object;

– conducting additional spectral analysis of signals of on-board systems of low-visible aerial objects.

The spectra and spectrograms of signals of on-board systems of aerial objects when using non-directional and directional antennas were experimentally determined. The experimental studies confirm the possibility of using the Software-Defined Radio receiver to receive signals from airborne equipment and improve the signal-to-noise ratio.

The accuracy of determining the coordinates of aerial objects when using Software-Defined Radio receivers was evaluated. A decrease in the error of determining plane coordinates by the Software-Defined Radio system of receivers compared to the accuracy of determining coordinates by the P-19 MA radar station was established by an average of 1.88–2.47 times, depending on the distance to the aerial object.

Keywords: low-visible aerial object, Software-Defined Radio, receiver, determination of coordinates, accuracy.

References

1. Erl, J. (2022). Sensing digital objects in the air: Ultraleap introduces new technology. Available at: <https://mixed-news.com/en/sensing-digital-objects-in-the-air-ultraleap-introduces-new-technology/>
2. Sample, I. (2023). What do we know about the four flying objects shot down by the US? Available at: <https://www.theguardian.com/world/2023/feb/13/what-do-we-know-about-the-four-flying-objects-shot-down-by-the-us>
3. Carafano, J. J. (2022). Rapid advancements in military tech. Available at: <https://www.gisreportsonline.com/r/military-technology>
4. Stilwell, B. (2023). 4 Amazing Military Aviation Technologies We'll See in the Near Future. Available at: <https://www.military.com/off-duty/4-amazing-military-aviation-technologies-well-see-near-future.html>
5. Globa, L., Dovgyi, S., Kopyika, O., Kozlov, O. (2022). Approach to Uniform Platform Development for the Ecology Digital Environment of Ukraine. *Lecture Notes in Networks and Systems*, 83–100. doi: https://doi.org/10.1007/978-3-031-16368-5_4
6. Orlan-10 Uncrewed Aerial Vehicle (UAV). Available at: <https://www.airforce-technology.com/projects/orlan-10-unmanned-aerial-vehicle-uav/#catfish>
7. Russia behind the UAV technology curve (2021). Available at: https://issuu.com/edrmag/docs/edr_58_-_web/s/12783061
8. Chang, L. ZALA Lancet. Loitering munition. Available at: <https://www.militarytoday.com/aircraft/lancet.htm>
9. Chopra, A. (2022). Next gen military technologies. Available at: <https://www.sps-aviation.com/story/?id=3161&h=Next-Gen-Military-Technologies>
10. Wang, H., Cheng, H., Hao, H. (2020). The Use of Unmanned Aerial Vehicle in Military Operations. *Lecture Notes in Electrical Engineering*, 939–945. doi: https://doi.org/10.1007/978-981-15-6978-4_108
11. Richards, M. A., Scheer, J. A., Holm, W. A. (2010). Principles of modern radar. Vol. I. Basic principles. Raleigh: SciTech Publishing, 924. doi: <https://doi.org/10.1049/sbra021e>
12. Khudov, H., Zvonko, A., Kovalevskiy, S., Lishchenko, V., Zots, F. (2018). Method for the detection of small-sized air objects by observational radars. *Eastern-European Journal of Enterprise Technologies*, 2 (9 (92)), 61–68. doi: <https://doi.org/10.15587/1729-4061.2018.126509>
13. Melvin, W. L., Scheer, J. A. (2013). Principles of modern radar. Vol. II. Advanced techniques. Raleigh: SciTech Publishing, 846. doi: <https://doi.org/10.1049/sbra020e>

14. Melvin, W. L., Scheer, J. A. (2014). Principles of modern radar. Vol. III. Radar applications. Raleigh: SciTech Publishing, 820. doi: <https://doi.org/10.1049/sbra503e>
15. Bezouwen, J., Brandfass, M. (2017). Technology Trends for Future Radar. Available at: <https://www.microwavejournal.com/articles/29367-technology-trends-for-future-radar>
16. 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). doi: <https://doi.org/10.1109/ukrmico43733.2018.9047560>
17. Khudov, H. et al. (2020). The Coherent Signals Processing Method in the Multiradar System of the Same Type Two-coordinate Surveillance Radars with Mechanical Azimuthal Rotation. International Journal of Emerging Trends in Engineering Research, 8 (6), 2624–2630. doi: <https://doi.org/10.30534/ijeter/2020/66862020>
18. Marpl-ml, S. L. (1990). Tsifrovoy spektral'niy analiz i ego. Mosocw: Mir, 584.
19. Klimov, S. A. (2013). Metod povysheniya razreshayushey sposobnosti radiolokatsionnykh sistem pri tsifrovoy obrabotke signalov. Zhurnal radioelektroniki, 1. Available at: <http://jre.cplire.ru/jre/jan13/1/text.html>
20. Bhatta, A., Mishra, A. K. (2017). GSM-based commsense system to measure and estimate environmental changes. IEEE Aerospace and Electronic Systems Magazine, 32 (2), 54–67. doi: <https://doi.org/10.1109/maes.2017.150272>
21. 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. doi: <https://doi.org/10.1109/radar.2006.1631853>
22. Willis, N. J. (2004). Bistatic Radar. IET. doi: <https://doi.org/10.1049/sbra003e>
23. Lishchenko, V., Khudov, H., Tiutiunnyk, V., Kuprii, V., Zots, F., Misiyuk, G. (2019). The Method of Increasing the Detection Range of Unmanned Aerial Vehicles In Multiradar Systems Based on Surveillance Radars. 2019 IEEE 39th International Conference on Electronics and Nanotechnology (ELNANO). doi: <https://doi.org/10.1109/elnano.2019.8783263>
24. 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. doi: <https://doi.org/10.15587/1729-4061.2020.216118>
25. Leshchenko, S., Kolesnik, O., Gricenko, S., Burkovsky, S. (2017). Use of the ADS-B information in order to improve quality of the air space radar reconnaissance. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy, 3 (28), 69–75. Available at: http://nbuv.gov.ua/UJRN/Nitps_2017_3_11
26. Khudov, H., Diakonov, O., Kuchuk, N., Maliuha, V., Furmanov, K., Mylashenko, I. et al. (2021). Method for determining coordinates of airborne objects by radars with additional use of ADS-B receivers. Eastern-European Journal of Enterprise Technologies, 4 (9 (112)), 54–64. doi: <https://doi.org/10.15587/1729-4061.2021.238407>
27. LORAN-C. Available at: <https://skybrary.aero/articles/loran-c>
28. Multilateration (MLAT) Concept of Use. Available at: https://www.icao.int/APAC/Documents/edocs/mlat_concept.pdf
29. Neven, W. H., Quilter, T. J., Weedon, R., Hogendoorn, R. A. (2005). Wide Area Multilateration Report on EATMP TRS 131/04 Version 1.1. Available at: <https://www.eurocontrol.int/sites/default/files/2019-05/surveillance-report-wide-area-multilateration-200508.pdf>
30. Mantilla-Gaviria, I. A., Leonardi, M., Balbastre-Tejedor, J. V., de los Reyes, E. (2013). On the application of singular value decomposition and Tikhonov regularization to ill-posed problems in hyperbolic passive location. Mathematical and Computer Modelling, 57 (7-8), 1999–2008. doi: <https://doi.org/10.1016/j.mcm.2012.03.004>
31. Schau, H., Robinson, A. (1987). Passive source localization employing intersecting spherical surfaces from time-of-arrival differences. IEEE Transactions on Acoustics, Speech, and Signal Processing, 35 (8), 1223–1225. doi: <https://doi.org/10.1109/tassp.1987.1165266>
32. Khudov, H., Mynko, P., Ikhsanov, S., Diakonov, O., Kovalenko, O., Solomonenko, Y. et al. (2021). Development a method for determining the coordinates of air objects by radars with the additional use of multilateration technology. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 6–16. doi: <https://doi.org/10.15587/1729-4061.2021.242935>
33. Khudov, H., Yarosh, S., Droban, O., Lavrut, O., Hulak, Y., Porokhnia, I. et al. (2021). Development of a direct penetrating signal compensator in a distributed reception channel of a surveillance radar. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 16–26. doi: <https://doi.org/10.15587/1729-4061.2021.228133>
34. Oleksenko, O., Khudov, H., Petrenko, K., Horobets, Y., Kolianda, V., Kuchuk, N. et al. (2021). The Development of the Method of Radar Observation System Construction of the Airspace on the Basis of Genetic Algorithm. International Journal of Emerging Technology and Advanced Engineering, 11 (8), 23–30. doi: https://doi.org/10.46338/ijetae0821_04
35. Ryu, H., Wee, I., Kim, T., Shim, D. H. (2020). Heterogeneous sensor fusion based omnidirectional object detection. 2020 20th International Conference on Control, Automation and Systems (ICCAS). doi: <https://doi.org/10.23919/iccas50221.2020.9268431>
36. Salman, S., Mir, J., Farooq, M. T., Malik, A. N., Haleemdeen, R. (2021). Machine Learning Inspired Efficient Audio Drone Detection using Acoustic Features. 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST). doi: <https://doi.org/10.1109/ibcast51254.2021.9393232>
37. SHAHED-136 Loitering munition / Kamikaze-Suicide drone – Iran (2023). Available at: https://www.armyrecognition.com/iran_unmanned_ground_aerial_vehicles_systems/shahed-136_loitering_munition_kamikaze-suicide_drone_iran_data.html#google_vignette
38. How drones are conquering the battlefield in Ukraine's war (2023). Available at: <https://www.euronews.com/2023/06/06/how-drones-are-conquering-the-battlefield-in-ukraines-war>
39. Space, the unseen frontier in the war in Ukraine (2022). BBC News. Available at: <https://www.bbc.com/news/technology-63109532>
40. NASAMS Air Defence System. Available at: <https://www.kongsberg.com/kda/what-we-do/defence-and-security/integrated-air-and-missile-defence/nasams-air-defence-system/>
41. Fedorov, A., Holovniak, D., Khudov, H., Misiyuk, G. (2019). Method of Radar Adjustment with Automatic Dependent Surveillance Technology Use. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). doi: <https://doi.org/10.1109/picst47496.2019.9061245>
42. Byrne, J., Watling, J., Bronk, J., Somerville, G., Byrne, J., Crawford, J., Baker, J. (2022). The Orlan complex. Tracking the supply chains of Russia's most successful UAV. Royal United Services Institute for Defence and Security Studies. Available at: <https://static.rusi.org/SR-Orlan-complex-web-final.pdf>
43. Swiss Components For Cars and Electric Bicycles Were Found in russian Orlan-10 UAVs and Missiles (2023). Available at: <https://>

- en.defence-ua.com/industries/swiss_components_for_cars_and_electric_bicycles_were_found_in_russian_orlan_10_uavs_and_missiles-6267.html
44. What is a Spectrogram? Available at: <https://vibrationresearch.com/blog/what-is-a-spectrogram>
 45. What is a Spectrogram? Available at: <https://pnsn.org/spectrograms/what-is-a-spectrogram>
 46. Eleron-3SV. Available at: <https://robotrends.ru/robopedia/eleron-3sv>
 47. Saybel', A. G. (1958). *Osnovy teorii tochnosti radiotekhnicheskikh metodov mestoopredeleniya*. Moscow: Oborongiz, 55.
 48. Khudov, H., Zvonko, A., Lisohorskyi, B., Solomonenko, Y., Mynko, P., Glukhov, S. et al. (2022). Development of a rangefinding method for determining the coordinates of targets by a network of radar stations in counter-battery warfare. *EUREKA: Physics and Engineering*, 3, 121–132. doi: <https://doi.org/10.21303/2461-4262.2022.002380>
 49. Ruban, I., Khudov, H., Makoveichuk, O., Butko, I., Glukhov, S., Khizhnyak, I. et al. (2022). Application of the Particle Swarm Algorithm to the Task of Image Segmentation for Remote Sensing of the Earth. *Lecture Notes in Networks and Systems*, 573–585. doi: https://doi.org/10.1007/978-981-19-5845-8_40
 50. Khudov, H., Makoveichuk, O., Khizhnyak, I., Oleksenko, O., Khazhanets, Y., Solomonenko, Y. et al. (2022). Devising a method for segmenting complex structured images acquired from space observation systems based on the particle swarm algorithm. *Eastern-European Journal of Enterprise Technologies*, 2 (9 (116)), 6–13. doi: <https://doi.org/10.15587/1729-4061.2022.255203>
 51. AIRSPY. Available at: <https://airspy.com>
 52. Apaydin, G., Sevgi, L. (2017). Radio Wave Propagation and Parabolic Equation Modeling. The Institute of Electrical and Electronics Engineers. doi: <https://doi.org/10.1002/9781119432166>
 53. P-19MA. Available at: http://uoe.com.ua/products/en/?id=0&pid=catalogue&language=eng&catalogue_id=515&type=content
 54. HackRF One SDR-transiver (1 MHts – 6 HHts) maksymalna komplektatsiya. Available at: <https://radioscan.com.ua/ua/p1878031526-hackrf-one-sdr.html>

АНОТАЦІЇ
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2023.285514

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ СИСТЕМ ГРОМАДСЬКОГО ТРАНСПОРТУ НА ОСНОВІ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ (с. 6–13)

І. В. Закутинський, Л. В. Сібрук, І. Є. Рабодзей

Об'єктом дослідження є хмарні обчислення як елемент серверної інфраструктури для інтелектуальних систем громадського транспорту. З урахуванням зростання складності та вимог, що ставляться до сучасного транспорту, застосування концепції Інтернету речей має високий потенціал для покращення ефективності та комфорту пасажирів. Оскільки навантаження яке генерується в системах Інтернету речей є динамічним та важкопрогнозованим, то застосування традиційної інфраструктури з виділеними серверами є неоптимальним. У цьому дослідженні розглядається використання хмарних обчислень як основної серверної інфраструктури для вищенаведених систем. Проведено дослідження основних хмарних платформ, які можуть бути застосовані для розробки таких систем. Автори розробили архітектуру системи, а також оцінили продуктивність і масштабованість окремих її компонентів. Для тестування системи було розроблено програмний емулятор, який імітує модуль контролера, що встановлюється в транспортних засобах. За допомогою емулятора було проведено стрес-тести для аналізу та підтвердження здатності масштабування та обробки вхідних даних запропонованою архітектурою. Сценарії тестування були розроблені та проведені на основі наявної системи громадського транспорту м. Київ, Україна. Результати експериментів показали, що запропонована система Інтернету речей здатна масштабуватися відповідно до навантаження, яке генерується підключеними пристроями. Встановлено, що при збільшенні кількості вхідних повідомлень з 40 до 6000 середній час обробки повідомлення залишається незмінним, а також коефіцієнт помилок не зростає, що є показником стабільної роботи системи. Одержані результати можуть бути використані при розробці сучасних систем громадського транспорту, а також для модернізації вже існуючих.

Ключові слова: інтернет речей, хмарні обчислення, архітектура системи, системи міського транспорту, масштабованість.

DOI: 10.15587/1729-4061.2023.285414

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ОБРОБКИ АГРЕГОВАНОГО ПОТОКУ ДАНИХ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ЗВ'ЯЗКУ (с. 14–23)

Л. Н. Беркман, А. Г. Захаржевський, К. Г. Лаврінець

Досліджується процес динамічного резервування каналного ресурсу захищеної корпоративної мультисервісної мережі зв'язку.

Встановлено, що процеси побудови та функціонування схем захищеної корпоративної мультисервісної мережі зв'язку та підвищення якості реалізації її основних робочих процесів передбачає оцінку та динамічне резервування каналного ресурсу під вхідні агреговані потоки даних мережі.

Розроблена та запропонована модель динамічного резервування каналного ресурсу агрегованого потоку даних захищеної корпоративної мультисервісної мережі зв'язку. Запропонована модель дозволяє встановити кількісні значення зарезервованого каналного ресурсу для різних способів обслуговування в залежності від кількості складових потоків в загальному агрегованому потоці даних VPN-тунелю.

Встановлено, що збільшення щільності агрегованого потоку даних вимагає збільшення зарезервованого каналного ресурсу. При цьому, на його значення чинить вплив спосіб обслуговування агрегованого потоку даних в VPN-тунелі захищеної корпоративної мультисервісної мережі зв'язку. Застосування способу ізольованого обслуговування дає вигравш в виділеному ресурсі на каналний резерв від 10 до 20 відсотків в порівнянні з груповим методом обслуговування для IP та відеотелефонії. Це пояснюється більш гнучким процесом керування буфером зберігання вхідних даних прикордонного маршрутизатора при ізольованому способі обслуговування.

Подана в роботі модель динамічного резервування каналного ресурсу захищеної корпоративної мультисервісної мережі зв'язку може бути використана при удосконаленні існуючих та розробці нових структур захищеної корпоративної мультисервісної мережі зв'язку. Наслідком такого удосконалення є зменшення часу затримки про обробці пакетів вхідних даних в вказаній мережі.

Ключові слова: захищена корпоративна мультисервісна мережа зв'язку, агрегований потік, каналний ресурс, VPN-шлюз.

DOI: 10.15587/1729-4061.2023.286187

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ В ДЕЦЕНТРАЛІЗОВАНИХ ОДНОРАНГОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ (с. 24–35)

В. В. Міхав, С. Г. Семенов, Є. В. Мелешко, М. С. Якименко, Я. П. Шуліка

Рекомендаційні системи дозволяють полегшити пошук при великій кількості контенту, доповнюючи або заміняючи класичну пошукову видачу рекомендаціями. В P2P мережах їх застосування може мати додаткову користь. Через проблеми індексації і пошуку раніше додані файли можуть бути недоступні для користувача P2P мережі. Якщо користувач не може знайти шуканий файл, можна надати йому список рекомендацій з врахуванням його вподобань і пошукового запиту.

Об'єктом дослідження є процес створення рекомендацій користувачам децентралізованих P2P мереж для полегшення пошуку даних.

Вирішується актуальна проблема підвищення точності математичного моделювання рекомендаційних систем за рахунок врахування вимог до достовірності та безпеки даних під час змін у структурі децентралізованої P2P мережі.

Розроблена аналітична модель рекомендаційної системи децентралізованої P2P мережі, основною особливістю якої є врахування вимог достовірності та безпеки рекомендаційних повідомлень. Це виконано шляхом введення в загальну модель децентралізованої рекомендаційної системи наступних показників – ймовірність достовірної передачі пакета та ймовірність безпечної передачі пакета. Розроблена аналітична модель дозволяє проводити порівняльний аналіз різних методів роботи рекомендаційних систем та встановлювати припустимі параметри, при яких ступінь актуальності не падає нижче визначеного порогу.

Розроблена математична модель системи на основі GERT-схеми відрізняється від відомих врахуванням вимог достовірності і безпеки під час змін у структурі децентралізованої P2P мережі. Це дозволило покращити точність результатів моделювання до 5 %.

Запропонована математична модель може бути використана для прототипування рекомендаційних систем у різних сферах діяльності.

Ключові слова: рекомендаційна система, децентралізована комп'ютерна мережа, однорангова мережа, GERT-мережа, інформаційна безпека.

DOI: 10.15587/1729-4061.2023.282100

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМ З ОРТОГОНАЛЬНИМ ЧАСТОТНИМ ПОДІЛОМ КАНАЛІВ В УМОВАХ МІЖКАНАЛЬНОЇ ІНТЕРФЕРЕНЦІЇ (с. 36–44)

Р. Г. Биков

Сучасні системи зв'язку засновані на технології мультиплексування з ортогональним частотним поділом каналів (OFDM), яка дозволяє надійно передавати інформацію в умовах багатопроменевості. Необхідність збереження ортогональних властивостей піднесучих призводить до високої чутливості даних систем до частотних зсувів сигналу. У роботі удосконалений метод формування сигналу для OFDM системи. Досліджене застосування формуючих імпульсів з селективним спектром після етапу зворотного швидкого перетворення Фур'є (IFFT) на стороні передавача для зменшення рівня міжканальних завад при зсуві частоти несучої. Синтезовані нові форми імпульсів, отримані з використанням оптимізованих багатопараметричних функцій з селективним спектром. Проаналізована ефективність застосування синтезованих імпульсів з селективним спектром щодо зменшення впливу частотного зсуву сигналу на завадостійкість OFDM системи. Проведене порівняння ймовірності бітової помилки з вже існуючими формами імпульсів Найквіста. У середовищі MATLAB розроблена модель передавача і приймача OFDM системи для експериментальної оцінки впливу запропонованих формуючих імпульсів на завадостійкість системи в умовах міжканальної інтерференції при різних видах модуляції. Встановлено, що найменший рівень ймовірності бітової помилки в умовах міжканальної інтерференції спостерігається для двопараметричного імпульсу з селективним спектром та кусково-лінійною апроксимацією перехідної області. Так, для відношення сигнал/шуму 15 дБ, модуляції BPSK та нормованого частотного зсуву 0,2 ймовірність бітової помилки для даного імпульсу становить $3 \cdot 10^{-4}$, для модуляції QPSK та нормованого частотного зсуву 0,1–10⁻⁶, для модуляції QAM-16 та нормованого частотного зсуву 0,03–2 $\cdot 10^{-4}$.

Ключові слова: формуючий імпульс Найквіста, імпульс з селективним спектром, кусково-лінійна апроксимація, міжканальна інтерференція, OFDM.

DOI: 10.15587/1729-4061.2023.285540

РОЗРОБКА МЕТОДУ ВИПРАВЛЕННЯ ПОМИЛОК З ВИКОРИСТАННЯМ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШТОК (с. 45–53)

П'єр Мурр, С. П. Євсєєв, С. В. Мілевський, М. О. Мельник, В. О. Кацалап, Ю. Б. Прібилєв, Х. Н. Рзаєв, А. Ю. Брила, О. І. Шпак, П. П. Федорка

Об'єктом дослідження є інноваційний метод виправлення помилок, у якому використовуються досконалі двійкові решітки (ДДР), потужний математичний інструмент з унікальними властивостями, які роблять його ідеальним для виправлення помилок. Дослідження спрямоване на вивчення впливу некорельованих помилок змішаного типу у шляху обміну даними, що дозволяє його використання у смарт-технологіях з обмеженими обчислювальними можливостями. Ефективність підходу підтверджується моделюванням та порівнянням з іншими методами виправлення помилок. Для подальшого вивчення структурних, кореляційних та дистанційних властивостей ортогональних двовимірних кодів та коригувальних можливостей запропонованого методу розроблено систему інформаційних технологій для передачі даних на основі еквівалентного класу ідеальних двійкових масивів. Запропонована модель оцінює продуктивність коду виправлення помилок на основі ідеальних двійкових масивів за різних умов, у тому числі корельованих та некорельованих перешкод та шляхів обміну даними. Побудовано генератор ДДР еквівалентних класів. Проведено експериментальну оцінку корегуючої здатності запропонованих двовимірних кодів шляхом моделювання різних передкодових ситуацій, включаючи пакетні та випадкові помилки, для випадків корельованих та некорельованих перешкод. Використовуючи графічний інтерфейс, користувачі зможуть вводити кількість і тип помилок, визначати, чи є вони випадковими або пакетними помилками, вручну або в автоматичному режимі, переміщувати помилки по пакету даних і переглядати проміжні результати. Таким чином, комплексний характер цього дослідження можливо позиціювати як перспективний підхід та надійний вибір у галузі виправлення помилок.

Ключові слова: завадостійке кодування інформації, виявлення помилок, досконалі двійкові решітки.

DOI: 10.15587/1729-4061.2023.285261**РОЗРОБКА НОВОГО АЛГОРИТМУ ШИФРУВАННЯ ЗОБРАЖЕНЬ, ЩО ПЕРЕДАЮТЬСЯ ЧЕРЕЗ СИСТЕМИ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ (с. 54–60)****Sanaa Ahmed Kadhim, Ruwaida Mohammed Yas, Saad Abdual Azize Abdual Rahman, Sura Khalil Abd**

Бездротові сенсорні мережі (БСМ) дотепер стикалися з багатьма проблемами через їх відкритість, широкомасштабність і обмеженість ресурсів, включаючи безпеку, ефективність і споживання енергії. У військовій системі важливо забезпечити високий рівень безпеки для важливих даних через бездротову мережу, яка, як доведено, є ненадійним публічним зв'язком. Для вирішення вищезазначеної проблеми слід застосувати високий рівень безпеки з мінімальною складністю, щоб відповідати обмеженим можливостям системи передачі. У цьому документі представлено новий алгоритм під назвою (SRS) для шифрування переданих військових зображень, щоб захистити їх від злому або зламу БСМ. Алгоритм SRS розроблений як легкий, швидкий і безпечний, беручи до уваги обмежені можливості системи передачі. Він реалізований як криптосистема з відкритим ключем, спеціально розроблена для шифрування зображень. Алгоритм складається з двох частин: шифрування та дешифрування. Запропонована система пропонує деякі рівняння та обчислення, які застосовуються до простих і кодованих зображень після передачі через БСМ. Результати тестування імітаційної моделі демонструють ефективність системи шляхом оцінки з використанням різних показників, таких як співвідношення сигнал/шум, середня квадратична помилка і пікове співвідношення сигнал/шум. Загалом у документі представлено новий алгоритм шифрування, SRS, спеціально розроблений для захисту військових зображень, що передаються через бездротові сенсорні мережі. Алгоритм спрямований на забезпечення балансу між безпекою, ефективністю та споживанням енергії, враховуючи обмеженість ресурсів БСМ. Результати моделювання вказують на покращення запропонованої системи на 13 %, 10 % і 55 % у коефіцієнті доставки пакетів, пропускну здатності та коефіцієнті відкидання, відповідно, і це показує, що запропонований метод SRS збільшив час виконання на 67 % порівняно з алгоритмом на основі RSA.

Ключові слова: бездротова сенсорна мережа, SRS алгоритм шифрування зображення для військової системи.

DOI: 10.15587/1729-4061.2023.286466**ВИКОРИСТАННЯ SOFTWARE-DEFINED RADIO ПРИЙМАЧІВ ДЛЯ ВИЗНАЧЕННЯ КООРДИНАТ МАЛОПОМІТНИХ ПОВІТРЯНИХ ОБ'ЄКТІВ (с. 61–73)****Г. В. Худов, О. В. Костянець, О. В. Коваленко, О. В. Масленко, Ю. С. Соломоненко**

Об'єктом дослідження є процес визначення координат малопомітних повітряних об'єктів. Основна гіпотеза дослідження полягала в тому, що сигнали, що випромінюються бортовими системами малопомітних для радіолокаційних станцій повітряних об'єктів, мають більшу потужність, ніж відбитий від повітряного об'єкту сигнал. Це, в свою чергу, дозволить підвищити відношення сигнал/шум та, відповідно, точність визначення координат малопомітних повітряних об'єктів. Для прийому таких сигналів, що випромінюються бортовими системами малопомітних повітряних об'єктів, запропоновано використовувати Software-Defined Radio приймачі.

Встановлено, що основними джерелами сигналів для Software-Defined Radio приймачів є сигнали командного, телеметричного, цільового каналів, каналів ручного управління та супутникової навігації. Встановлено, що додатковою розпізнавальною ознакою при визначенні координат малопомітних повітряних об'єктів є унікальність їх спектрів та спектрограм.

Удосконалено метод визначення координат малопомітних повітряних об'єктів при використанні Software-Defined Radio приймачів, який, на відміну від відомих, передбачає:

- використання у якості сигналів для Software-Defined Radio приймачів сигналів бортового обладнання малопомітного повітряного об'єкту;
- використання апріорних значень координат малопомітного повітряного об'єкту;
- проведення додаткового спектрального аналізу сигналів бортових систем малопомітного повітряного об'єкту.

Експериментально визначені спектри та спектрограми сигналів бортових систем повітряних об'єктів при використанні ненаправленої та направленої антен. Проведені експериментальні дослідження підтверджують можливість використання Software-Defined Radio приймача для прийому сигналів бортової апаратури повітряних об'єктів та підвищення відношення сигнал/шум.

Проведено оцінювання точності визначення координат повітряних об'єктів при використанні Software-Defined Radio приймачів. Встановлено зменшення похибки визначення площинних координат системою Software-Defined Radio приймачів у порівнянні з точністю визначення координат радіолокаційною станцією П-19 МА в середньому в 1,88–2,47 разів в залежності від дальності до повітряного об'єкту.

Ключові слова: малопомітний повітряний об'єкт, Software-Defined Radio, приймач, визначення координат, точність.