ABSTRACT AND REFERENCES

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2024.298598

IMPROVING A METHOD FOR NON-COHERENT PROCESSING OF SIGNALS BY A NETWORK OF TWO SMALL-SIZED RADARS FOR DETECTING A STEALTH UNMANNED AERIAL VEHICLE (p. 6–13)

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

Serhii Yarosh
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-5208-9372

Oleksandr Kostyria
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-3363-2015

Oleksandr Oleksenko
Air Force Command of UA Armed Forces, Vinnytsia, Ukraine
ORCID: https://orcid.org/0000-0002-6853-9630

Mykola Khomik
The National Defence University of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-1201-7702

Andrii Zvonko
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine
ORCID: https://orcid.org/0000-0002-7410-799X

Bohdan Lisohorskyi
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5345-0345

Petro Mynko
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2621-8900

Serhii Sukonko
National Academy of the National Guard of Ukraine, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-2224-4068

Taras Kravets
Hetman Petro Sahaidachnyi National Army Academy, Lviv, Ukraine
ORCID: https://orcid.org/0000-0001-5398-7441

The object of this study is the process of detecting stealth unmanned aerial vehicles by a network of two small-sized radars with incoherent signal processing. The main hypothesis of the study assumed that combining two small-sized radars into a network could improve the quality of detection of stealth unmanned aerial vehicles with incoherent signal processing.

The improved method for detecting a stealth unmanned aerial vehicle by a network of two small-sized radars with incoherent signal processing, unlike the known ones, provides for the following:

– synchronous inspection of the airspace by small-sized radars;

– sounding signal emission by each small-sized radar;

– reception of echo signals from a stealth unmanned aerial vehicle by two small-sized radars;

– coordinated filtering of incoming echo signals (separation of echo signals);

– quadratic detection of signals at the outputs of matched filters;

– summation of the detected signals at the outputs of the matched filters;

– summation of the outputs of adders of two small-sized radars.

The scheme of a stealth unmanned aerial vehicle detector is presented, optimal according to the Neumann-Pearson criterion, with incoherent signal processing.

The quality of detection of a stealth unmanned aerial vehicle by a network of two small-sized radars with incoherent signal processing was evaluated. It was found that with incoherent processing, the gain in the value of the conditional probability of correct detection is on average from 19 % to 26 %, depending on the value of the signal-to-noise ratio. The gain in the value of the conditional probability of correct detection is greater at low values of the signal-to-noise ratio. At the same time, the gain in signal-to-noise value is more significant with coherent signal processing than with non-coherent signal processing by a network of two small-sized radars.

Keywords: small-sized radar, aerial object detection, incoherent processing, conditional probability of correct detection.

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. Carafano, J. J. (2022). Rapid advancements in military tech. Available at: https://www.gisreportsonline.com/r/military-technology
3. Sentinel Radar. Available at: https://www.rtx.com/raytheon/what-we-do/land/sentinel-radar
4. NASAMS anti-aircraft missile system. Available at: https://en.missilery.info/missile/nasams
5. US Sentinel Radar Was Recorded in Ukraine. Available at: https://en.defence-ua.com/weapon_and_tech/us_sentinel_radar_was_recorded_in_ukraine-3357.html
6. Kalibr. Naval Cruise missile family. Available at: https://www.military-today.com/missiles/kalibr.htm
7. Orlan-10 Uncrewed Aerial Vehicle (UAV). Available at: https://www.airforce-technology.com/projects/orlan-10-unmanned-aerial-vehicle-uav/#catfish
8. Khudov, H., Berezhnyi, A., Oleksenko, O., Maliuha, V., Balyk, I., Herda, M. et al. (2023). Increasing of the accuracy of determining the coordinates of an aerial object in the two-position network of small-sized radars. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 6–13. https://doi.org/10.15587/1729-4061.2023.289623
9. Bezouwen, J., Brandfass, M. (2017). Technology Trends for Future Radar. Microwave Journal. Available at: http://www.microwavejournal.com/articles/29367-technology-trends-for-future-radar
10. Richards, M. A., Scheer, J. A., Holm, W. A. (Eds.) (2010). Principles of Modern Radar: Basic principles. Institution of Engineering and Technology. https://doi.org/10.1049/sbra021e

11. Chernyak, V. (2014). Signal detection with MIMO radars. Uspehi sovremennoj radiojelectroniki, 7, 35–48.
12. 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). https://doi.org/10.1109/ukrmico43733.2018.9047560
13. Khudov, H. (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. https://doi.org/10.30534/ijeter/2020/66862020
14. 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. https://doi.org/10.1109/radar.2006.1631853
15. Multilateration (MLAT) Concept of Use. Edition 1.0 (2007). ICAO Asia and Pacific Office. Available at: https://www.icao.int/APAC/Documents/edocs/mlat_concept.pdf
16. Willis, N. J. (2004). Bistatic Radar. Institution of Engineering and Technology. Institution of Engineering and Technology. https://doi.org/10.1049/sbra003e
17. 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). https://doi.org/10.1109/elnano.2019.8783263
18. Ruban, I., Khudov, H., Lishchenko, V., Pukhovyi, O., Popov, S., Kolos, R., Kravets, T. 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
19. LORAN-C. Available at: https://skybrary.aero/articles/loran-c
20. 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/surveilllance-report-wide-area-multilateration-200508.pdf
21. 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. https://doi.org/10.1016/j.mcm.2012.03.004
22. 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. https://doi.org/10.1109/tassp.1987.1165266
23. 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). https://doi.org/10.23919/iccas50221.2020.9268431
24. 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). https://doi.org/10.1109/ibcast51254.2021.9393232
25. Liu, Y., Yi, J., Wan, X., Cheng, F., Rao, Y., Gong, Z. (2018). Experimental Research on Micro-Doppler Effect of Multi-rotor Drone with Digital Television Based Passive Radar. Journal of Radars, 7 (5), 585–592. https://doi.org/10.12000/JR18062
26. Wang, W. (2016). Overview of frequency diverse array in radar and navigation applications. IET Radar, Sonar & Navigation, 10 (6), 1001–1012. https://doi.org/10.1049/iet-rsn.2015.0464
27. Li, J., Stoica, P. (Eds.) (2008). MIMO Radar Signal Processing. John Wiley & Sons, Inc. https://doi.org/10.1002/9780470391488
28. Li, Y. (2021). MIMO Radar Waveform Design: An Overview. Journal of Beijing Institute of Technology, 30 (1), 44–59. https://doi.org/10.15918/j.jbit1004-0579.2021.002
29. 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. https://doi.org/10.46338/ijetae0821_04
30. Khudov, H., Berezhnyi, A., Yarosh, S., Oleksenko, O., Khomik, M., Yuzova, I. et al. (2023). Improving a method for detecting and measuring coordinates of a stealth aerial vehicle by a network of two small-sized radars. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 6–13. https://doi.org/10.15587/1729-4061.2023.293276
31. Chang, L. ZALA Lancet. Loitering munition. Available at: https://www.militarytoday.com/aircraft/lancet.htm
32. Shin, S. -J. (2017). Radar measurement accuracy associated with target RCS fluctuation. Electronics Letters, 53 (11), 750–752. https://doi.org/10.1049/el.2017.0901
33. Kishk, A., Chen, X. (Eds.) (2023). MIMO Communications - Fundamental Theory, Propagation Channels, and Antenna Systems. IntechOpen. https://doi.org/10.5772/intechopen.110927

DOI: 10.15587/1729-4061.2024.298268

OPTIMIZATION OF THE LEACH ALGORITHM IN THE SELECTION OF CLUSTER HEADS BASED ON RESIDUAL ENERGY IN WIRELESS SENSOR NETWORKS (p. 14–21)

Ferry Fachrizal
Universitas Sumatera Utara, Sumatera Utara, Indonesia
ORCID: https://orcid.org/0009-0004-2489-6144

Muhammad Zarlis
BINUS University, Kemanggisan, Palmerah Jakarta, Indonesia
ORCID: https://orcid.org/0000-0003-0520-7273

Poltak Sihombing
Universitas Sumatera Utara, Sumatera Utara, Indonesia
ORCID: https://orcid.org/0000-0001-5348-4537

Suherman Suherman
Universitas Sumatera Utara, Padang Bulan, Kec. Medan Baru, Kota Medan, Sumatera Utara
ORCID: https://orcid.org/0000-0002-7375-4626

This research has a research object, namely the optimization of the LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm in the context of wireless sensor networks. The problem in this research is the imbalance in energy consumption across clusters, which has an impact on battery life and affects network performance. Other problems include selecting a cluster head that is not focused so that it is difficult to balance network performance as well as computational limitations that require optimization. The results obtained

from this research are in the form of optimizing the leaching algorithm by modifying the clustering-based leaching algorithm that will be used in wireless sensor networks. In carrying out modifications, this research uses several stages in the process of selecting sensor nodes that will become members who function as cluster heads in a cluster that will be used in a wireless sensor network. In the LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm the cluster head will be selected based on the modified probability value. Modifying the algorithm by considering two factors, namely distance and remaining energy used in the Cluster Head selection process on the network and increasing network usage time must be based on the energy consumption used and then compared with the remaining energy. When modifying the LEACH (Low-Energy Adaptive Clustering Hierarchy) algorithm, it is necessary to pay attention to the distance factor between the nodes on a sensor and the selected cluster so that it can result in increased network performance. Network lifetime is indicated by the average death time of the first Node in the network. This research is novel in producing a modified leaching algorithm by improving network performance and extending battery life so that it can be used for wireless sensor networks in the context of natural disaster mitigation.

Keywords: cluster head, sensor network, leach algorithm, energy optimization, battery life.

References

1. Wu, F., Wu, T., Yuce, M. R. (2019). Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/wf-iot.2019.8767280
2. Liu, J., Zhao, Z., Ji, J., Hu, M. (2020). Research and application of wireless sensor network technology in power transmission and distribution system. Intelligent and Converged Networks, 1 (2), 199–220. https://doi.org/10.23919/icn.2020.0016
3. Swamy, S. N., Jadhav, D., Kulkarni, N. (2017). Security threats in the application layer in IOT applications. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). https://doi.org/10.1109/i-smac.2017.8058395
4. Shivalingagowda, C., Ahmad, H., Jayasree, P. V. Y., Sah, D. K. (2021). Wireless Sensor Network Routing Protocols Using Machine Learning. Lecture Notes in Networks and Systems, 99–120. https://doi.org/10.1007/978-981-16-0386-0_7
5. Khutsoane, O., Isong, B., Gasela, N., Abu-Mahfouz, A. M. (2020). WaterGrid-Sense: A LoRa-Based Sensor Node for Industrial IoT Applications. IEEE Sensors Journal, 20 (5), 2722–2729. https://doi.org/10.1109/jsen.2019.2951345
6. Ertam, F., Kilincer, I. F., Yaman, O., Sengur, A. (2020). A New IoT Application for Dynamic WiFi based Wireless Sensor Network. 2020 International Conference on Electrical Engineering (ICEE). https://doi.org/10.1109/icee49691.2020.9249771
7. Yahya, O. H., Alrikabi, H., Aljazaery, I. A. (2020). Reducing the Data Rate in Internet of Things Applications by Using Wireless Sensor Network. International Journal of Online and Biomedical Engineering (IJOE), 16 (03), 107. https://doi.org/10.3991/ijoe.v16i03.13021
8. Mejjaouli, S., Babiceanu, R. F. (2015). RFID-wireless sensor networks integration: Decision models and optimization of logistics systems operations. Journal of Manufacturing Systems, 35, 234–245. https://doi.org/10.1016/j.jmsy.2015.02.005
9. You, G., Zhu, Y. (2020). Structure and Key Technologies of Wireless Sensor Network. 2020 Cross Strait Radio Science & amp; Wireless Technology Conference (CSRSWTC). https://doi.org/10.1109/csrswtc50769.2020.9372727
10. Zhihui, H. (2015). Research on WSN Routing Algorithm Based on Energy Efficiency. 2015 Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA). https://doi.org/10.1109/isdea.2015.178
11. Jin, Z., Jian-Ping, Y., Si-Wang, Z., Ya-Ping, L., Guang, L. (2009). A Survey on Position-Based Routing Algorithms in Wireless Sensor Networks. Algorithms, 2 (1), 158–182. https://doi.org/10.3390/a2010158
12. Bendjeddou, A., Laoufi, H., Boudjit, S. (2018). LEACH-S: Low Energy Adaptive Clustering Hierarchy for Sensor Network. 2018 International Symposium on Networks, Computers and Communications (ISNCC). https://doi.org/10.1109/isncc.2018.8531049
13. Mittal, N., Singh, U., Salgotra, R. (2019). Tree-Based Threshold-Sensitive Energy-Efficient Routing Approach For Wireless Sensor Networks. Wireless Personal Communications, 108 (1), 473–492. https://doi.org/10.1007/s11277-019-06413-y
14. Fallo, K., Wibisono, W., Pamungkas, K. N. P. (2019). Pengembangan mekanisme grid based clustering untuk peningkatan kinerja LEACH pada lingkungan Wireless Sensor Network. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 5 (2), 164. https://doi.org/10.26594/register.v5i2.1708
15. Bhola, J., Soni, S., Cheema, G. K. (2019). Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11 (3), 1281–1288. https://doi.org/10.1007/s12652-019-01382-3
16. Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M., Ali, S. (2017). Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey. Wireless Communications and Mobile Computing, 2017, 1–14. https://doi.org/10.1155/2017/6457942
17. Palan, N. G., Barbadekar, B. V., Patil, S. (2017). Low energy adaptive clustering hierarchy (LEACH) protocol: A retrospective analysis. 2017 International Conference on Inventive Systems and Control (ICISC). https://doi.org/10.1109/icisc.2017.8068715
18. Kumar, V., Malik, N., Dhiman, G., Lohani, T. K. (2021). Scalable and Storage Efficient Dynamic Key Management Scheme for Wireless Sensor Network. Wireless Communications and Mobile Computing, 2021, 1–11. https://doi.org/10.1155/2021/5512879
19. Cheikh, M., Simpson, O., Sun, Y. (2017). Energy efficient relay selection method for clustered wireless sensor network. In Proceedings of European Wireless 2017.
20. Wu, M., Li, Z., Chen, J., Min, Q., Lu, T. (2022). A Dual Cluster-Head Energy-Efficient Routing Algorithm Based on Canopy Optimization and K-Means for WSN. Sensors, 22 (24), 9731. https://doi.org/10.3390/s22249731
21. Cho, J. H., Lee, H. (2020). Dynamic Topology Model of Q-Learning LEACH Using Disposable Sensors in Autonomous Things Environment. Applied Sciences, 10 (24), 9037. https://doi.org/10.3390/app10249037
22. Sharmin, S., Ahmedy, I., Md Noor, R. (2023). An Energy-Efficient Data Aggregation Clustering Algorithm for Wireless Sensor Networks Using Hybrid PSO. Energies, 16 (5), 2487. https://doi.org/10.3390/en16052487

23. Tadros, C. N., Shehata, N., Mokhtar, B. (2023). Unsupervised Learning-Based WSN Clustering for Efficient Environmental Pollution Monitoring. Sensors, 23 (12), 5733. https://doi.org/10.3390/s23125733
24. Khalifeh, A., Abid, H., Darabkh, K. A. (2020). Optimal Cluster Head Positioning Algorithm for Wireless Sensor Networks. Sensors, 20 (13), 3719. https://doi.org/10.3390/s20133719
25. Wang, J., Zhang, Z., Xia, F., Yuan, W., Lee, S. (2013). An Energy Efficient Stable Election-Based Routing Algorithm for Wireless Sensor Networks. Sensors, 13 (11), 14301–14320. https://doi.org/10.3390/s131114301
26. Koyuncu, H., Tomar, G. S., Sharma, D. (2020). A New Energy Efficient Multitier Deterministic Energy-Efficient Clustering Routing Protocol for Wireless Sensor Networks. Symmetry, 12 (5), 837. https://doi.org/10.3390/sym12050837

DOI: 10.15587/1729-4061.2024.298476

DEVELOPMENT OF THE METHOD OF DETECTING AND CORRECTING DATA TRANSMISSION ERRORS IN IOT SYSTEMS FOR MONITORING THE STATE OF OBJECTS (p. 22–33)

Vladyslav Sokolovskyi
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-2381-3373

Eduard Zharikov
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-1811-9336

Sergii Telenyk
Cracow University of Technology, Kraków, Poland
ORCID: https://orcid.org/0000-0001-9202-9406

The object of the study is the IOT system for monitoring the state of objects.

The problem being solved is the development of an innovative method of detecting and correcting data transmission errors in the networks of Internet of Things systems.

The essence of the results is that a method of detecting and correcting multiple transmission errors during byte-by-byte transmission of a block of information has been developed. The method is distinguished by an original coding scheme, which involves the calculation of control bits, as well as the shuffling of block bits by performing bit shift operations. The peculiarity of the method is that any bit can be distorted when transmitting a code word, but it belongs to different code combinations of the Hamming code. This allows multiple data transmission errors to be detected and corrected during decoding, and multiple errors of different bytes belonging to the same block can be corrected.

Simple algorithms for encoding and decoding procedures have been developed, and programs for information block encoding procedures and decoding procedures with error detection and correction have been developed. A software model of the data transmission channel was also developed with the possibility of introducing multiple errors when simulating the data transmission process. All programs are developed in Python, although other languages are possible.

An experiment was conducted using the developed software model of the data transmission channel. The efficiency of the developed method has been experimentally confirmed and it has been proven that its use increases the immunity of the data transmission channel. This is due to the fact that the developed method allows detecting and correcting all code word transmission errors with a multiplicity from 1 to 8, which was confirmed experimentally.

The main field of use of the developed method is considered to be IoT system networks. First of all, systems for monitoring the state of objects.

Keywords: method of error correction, Hamming codes, Internet of Things, monitoring of the state of objects.

References

1. Internet Of Things (IoT). Available at: https://www.gartner.com/en/information-technology/glossary/internet-of-things
2. IoT Platforms. Available at: https://www.gartner.com/en/information-technology/glossary/iot-platforms
3. Shannon, C. E. (1948). A Mathematical Theory of Communication. Bell System Technical Journal, 27 (4), 623–656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x
4. Huffman, W. C., Pless, V. (2003). Fundamentals of Error-Correcting Codes. Cambridge University Press. https://doi.org/10.1017/cbo9780511807077
5. Subhasri, G., Radha, N. (2019). VLSI design of Parity check Code with Hamming Code for Error Detection and Correction. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). https://doi.org/10.1109/iccs45141.2019.9065790
6. Tolentino, L. K. S., Valenzuela, I. C., Juan, R. O. S. (2019). Overhead Interspersing of Redundancy Bits Reduction Algorithm by Enhanced Error Detection Correction Code. Journal of Engineering Science and Technology Review, 12 (2), 34–39. https://doi.org/10.25103/jestr.122.05
7. Chen, Z., Zhao, Y., Lu, J., Liang, B., Chen, X., Li, C. (2022). TECED: A Two-Dimensional Error-Correction Codes Based Energy-Efficiency SRAM Design. Electronics, 11 (10), 1638. https://doi.org/10.3390/electronics11101638
8. Tolentino, L. K., Padilla, M. V., Serfa Juan, R. (2018). FPGA-based redundancy bits reduction algorithm using the enhanced error detection correction code. International Journal of Engineering & Technology, 7 (3), 1008. https://doi.org/10.14419/ijet.v7i3.12681
9. Koppala, N., Subhas, C. (2022). Low overhead optimal parity codes. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20 (3), 501. https://doi.org/10.12928/telkomnika.v20i3.23301
10. Toghuj, W. (2020). Modifying Hamming code and using the replication method to protect memory against triple soft errors. TELKOMNIKA (Telecommunication Computing Electronics and Control), 18 (5), 2533. https://doi.org/10.12928/telkomnika.v18i5.13345
11. Saiz-Adalid, L.-J., Gil, P., Ruiz, J.-C., Gracia-Moran, J., Gil-Tomas, D., Baraza-Calvo, J.-C. (2016). Ultrafast Error Correction Codes for Double Error Detection/Correction. 2016 12th European Dependable Computing Conference (EDCC). https://doi.org/10.1109/edcc.2016.28
12. Rurik, W., Mazumdar, A. (2016). Hamming codes as error-reducing codes. 2016 IEEE Information Theory Workshop (ITW). https://doi.org/10.1109/itw.2016.7606865

13. Moon, T. K. (2005). Error correction coding: mathematical methods and algorithms. John Wiley & Sons. https://doi.org/10.1002/0471739219
14. Kadel, R., Paudel, K., Guruge, D. B., Halder, S. J. (2020). Opportunities and Challenges for Error Control Schemes for Wireless Sensor Networks: A Review. Electronics, 9 (3), 504. https://doi.org/10.3390/electronics9030504
15. Bettayeb, M., Ghunaim, S., Mohamed, N., Nasir, Q. (2019). Error Correction Codes in Wireless Sensor Networks: A Systematic Literature Review. 2019 International Conference on Communications, Signal Processing, and Their Applications (ICCSPA). https://doi.org/10.1109/iccspa.2019.8713725
16. Sridevi, N., Jamal, K., Mannem, K. (2021). Implementation of Error Correction Techniques in Memory Applications. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). https://doi.org/10.1109/iccmc51019.2021.9418432
17. Clark, G. C., Cain, J. B. (1981). Error-Correction Coding for Digital Communications. Springer US. https://doi.org/10.1007/978-1-4899-2174-1
18. Hamming, R. W. (1950). Error Detecting and Error Correcting Codes. Bell System Technical Journal, 29 (2), 147–160. https://doi.org/10.1002/j.1538-7305.1950.tb00463.x

DOI: 10.15587/1729-4061.2024.298844

DEVELOPMENT OF THE SOCIOCYBERPHYSICAL SYSTEMS` MULTI-CONTOUR SECURITY METHODOLOGY (p. 34–51)

Stanislav Milevskyi
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5087-7036

Olha Korol
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-8733-9984

Galyna Mykytyn
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: https://orcid.org/0000-0003-4275-8285

Iryna Lozova
National Aviation University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7224-4763

Svetlana Solnyshkova
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-5115-9148

Iryna Husarova
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-1421-0864

Alla Hrebeniuk
National Academy of the Security Service of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-8703-3432

Andrii Vlasov
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-6080-237X

Vladyslav Sukhoteplyi
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2566-4167

Dmytro Balagura
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID: https://orcid.org/0009-0006-9839-3317

The constant increase in the number of threats to the security of critical infrastructure objects, which include socio-cyberphysical systems, leads to a decrease in the quality of security services and the level of security of infrastructure elements. The object of research is the process of building a complex system of protection in socio-cyberphysical systems. The imperfection of the mechanisms for ensuring the security of critical infrastructure objects, which include socio-cyberphysical systems, the technological complexity of identifying new security threats necessitates an urgent need for a radical revision of the current approaches to its provision. So, it becomes clear that the development of a new approach to ensuring the security of information resources in socio-cyberphysical systems is needed. The article proposes a new approach to the methodological foundations of building multi-contour information protection systems with internal and external circuits on each of the platforms of socio-cyberphysical systems. This approach is based on a universal classifier of threats, which takes into account not the technical aspect of threats, but also their integration with social engineering methods, their synergy of hybridity. The sociopolitical influence on the realization of threats is taken into account, and practical mechanisms for providing basic security services based on post-quantum algorithms are also proposed. To provide basic security services in the proposed multi-contour protection system, it is proposed to use post-quantum algorithms – McEliece crypto-code constructions, which provide Perr=10^{-9}–10^{-12}, safe time Tsec=1025–1035 group operations. Within the framework of the proposed approach, the problem of increasing the level of information security has been formalized and further ways of solving it have been determined.

Keywords: socio-cyberphysical system, cyber security, information security, security of information, critical infrastructure facilities.

References

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2
2. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, 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. https://doi.org/10.15587/978-617-7319-57-2
3. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. https://doi.org/10.15587/978-617-7319-72-5
4. 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

5. Dzheniuk, N., Yevseiev, S., Lazurenko, B., Serkov, O., Kasilov, O. (2023). A method of protecting information in cyber-physical space. Advanced Information Systems, 7 (4), 80–85. https://doi.org/10.20998/2522-9052.2023.4.11
6. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 39–49. https://doi.org/10.15587/1729-4061.2023.293511
7. Haag, S., Siponen, M., Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52 (2), 25–67. https://doi.org/10.1145/3462766.3462770
8. Li, Y., Xin, T., Siponen, M. (2022). Citizens' Cybersecurity Behavior: Some Major Challenges. IEEE Security & Privacy, 20 (1), 54–61. https://doi.org/10.1109/msec.2021.3117371
9. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. https://doi.org/10.15587/1729-4061.2020.205702
10. Khoroshko, V. O., Pavlov, I. M., Bobalo, Y. Ya., Dudykevich, V. B. et al. (2020). Design of complex information protection systems. Lviv: Ed. Lviv Polytechnic, 320.
11. Brailovskyi, M. M., Zybin, S. V., Piskun, I. V., Khoroshko, V. O., Khokhlacheva, Yu. E. (2021). Information protection technologies. Kyiv: Central Committee "Comprint", 296.
12. Dudykevich, V. B., Khoroshko, V. O., Yaremchuk, Yu. E. (2018). Basics of information security. Vinnytsia: Ed. He. national technical Univ, 315.
13. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS PUB 202. https://doi.org/10.6028/NIST.FIPS.202
14. Migration to Post-Quantum Cryptography. Available at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
15. Clarridge, A., Salomaa, K. (2009). A Cryptosystem Based on the Composition of Reversible Cellular Automata. Lecture Notes in Computer Science, 314–325. https://doi.org/10.1007/978-3-642-00982-2_27
16. Lightweight Cryptography. Available at: https://csrc.nist.gov/Projects/lightweight-cryptography
17. Davydiuk, A. (2023). Implementation of new tools and methods for increasing the level of cyber security of critical infrastructure objects. Ukrainian Scientific Journal of Information Security, 25 (3). https://doi.org/10.18372/2410-7840.25.17937
18. Khomik, M., Harasymchuk, O. (2023). Analysis of threats to generators of pseudo-random numbers and pseudo-random sequences and protection measures. Ukrainian Information Security Research Journal, 25 (4). https://doi.org/10.18372/2410-7840.25.18222
19. Klimovych, S. (2023). Methodology of traffic masking in a specialized data transmission network. Ukrainian Scientific Journal of Information Security, 25 (3). https://doi.org/10.18372/2410-7840.25.17935
20. Risk assessment methodologies. Available at: https://www.cisa.gov/sites/default/files/publications/Risk%2520Assessment%2520Methodologies.pdf
21. UNOCT launches Update of the UN Compendium of Good Practices on the Protection of Critical Infrastructure against Terrorist Attacks. Available at: https://www.un.org/counterterrorism/events/unoct-launches-2022-update-un-compendium-good-practices-protection-critical-infrastructure
22. Methodology for assessing regional infrastructure resilience (2021). Washington. Available at: https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD%2520EAD%2520Signed_with%2520alt-text_0.pdf
23. Theocharidou, M., Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II, A new approach. Publications Office of the European Union. https://doi.org/10.2788/621843
24. Giannopoulos, G., Dorneanu, B., Jonkeren, O. (2013). Risk Assessment Methodology for Critical Infrastructure Protection. EUR 25745 EN. Luxembourg (Luxembourg): Publications Office of the European Union. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC78292
25. Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide (2018). Available at: https://www.fema.gov/sites/default/files/2020-07/threat-hazard-identification-risk-assessment-stakeholder-preparedness-review-guide.pdf
26. National Protection Framework (2016). Available at: https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf
27. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. https://doi.org/10.15587/1729-4061.2016.86175
28. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. https://doi.org/10.15587/1729-4061.2017.108461
29. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. https://doi.org/10.15587/1729-4061.2018.150903
30. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. https://doi.org/10.15587/1729-4061.2019.156620
31. Yevseiev, S., Havrylova, A., Korol, O., Dmitriiev, O., Nesmiian, O., Yufa, Y., Hrebennikov, A. (2022). Research of collision properties of the modified UMAC algorithm on crypto-code constructions. EUREKA: Physics and Engineering, 1, 34–43. https://doi.org/10.21303/2461-4262.2022.002213
32. Yevseiev, S., Havrylova, A., Milevskyi, S., Sinitsyn, I., Chalapko, V., Dukin, H. et al. (2023). Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies, 3 (9 (123)), 33–48. https://doi.org/10.15587/1729-4061.2023.281795
33. 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 Enter-

prise Technologies, 2 (9 (116)), 44–59. https://doi.org/10.15587/1729-4061.2022.254545

34. Yevseiev, S., Abdalla, A., Osiievskyi, S., Larin, V., Lytvynenko, M. (2020). Development of an advanced method of video information resource compression in navigation and traffic control systems. EUREKA: Physics and Engineering, 5, 31–42. https://doi.org/10.21303/2461-4262.2020.001405
35. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S. et al. (2021). Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency. Eastern-European Journal of Enterprise Technologies, 1 (2 (109)), 14–23. https://doi.org/10.15587/1729-4061.2021.225346
36. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. https://doi.org/10.15587/1729-4061.2021.229221
37. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. https://doi.org/10.15587/1729-4061.2021.233533
38. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, 1, 24–31. https://doi.org/10.21303/2461-4262.2021.001615
39. Cybersecurity classifier. Available at: https://skl.sspu.sumy.ua/
40. Milevsky, S. (2023). Development of threat classifier in socio-cyber-physical systems. Ukrainian Scientific Journal of Information Security, 29 (3). https://doi.org/10.18372/2225-5036.29.18070
41. Yevseiev, S., Milevskyi, S., Bortnik, L., Voropay, A., Bondarenko, K., Pohasii, S. (2022). Socio-Cyber-Physical Systems Security Concept. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). https://doi.org/10.1109/hora55278.2022.9799957
42. Yevseiev, S., Ryabukha, Y., Milov, O., Milevskyi, S., Pohasii, S., Melenti, Y. et al. (2021). Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies, 6 (2 (114)), 30–43. https://doi.org/10.15587/1729-4061.2021.249313
43. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I. et al. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. https://doi.org/10.15587/1729-4061.2021.241638
44. Ranjitha, C. R., Thomas, J., Chithra, K. R. (2016). A brief study on LDPC codes. International Journal of Engineering Research and General Science, 4, (2), 612–618. Available at: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf
45. Broul´ım, J. (2018). LDPC codes - new methodologies. University of West Bohemia, 127. Available at: https://cds.cern.ch/record/2730008/files/CERN-THESIS-2018-479.pdf
46. Zhu, H., Pu, L., Xu, H., Zhang, B. (2018). Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic. Wireless Communications and Mobile Computing, 2018, 1–9. https://doi.org/10.1155/2018/5264724
47. Singh, H. (2020). Code based Cryptography: Classic McEliece. arXiv.org. https://doi.org/10.48550/arXiv.1907.12754
48. Otmani, A., Tillich, J.-P., Dallot, L. (2010). Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 3 (2), 129–140. https://doi.org/10.1007/s11786-009-0015-8
49. Liva, G., Song, S., Lan, L., Zhang, Y., Lin, S., Ryan, W. E. (2017). Design of LDPC Codes: A Survey and New Results. Journal of Communications Software and Systems, 2 (3), 191. https://doi.org/10.24138/jcomss.v2i3.283
50. Richardson, T. J., Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 47 (2), 638–656. https://doi.org/10.1109/18.910579
51. Chandrasetty, V. A., Aziz, S. M. (2011). FPGA Implementation of a LDPC Decoder using a Reduced Complexity Message Passing Algorithm. Journal of Networks, 6 (1). https://doi.org/10.4304/jnw.6.1.36-45
52. Wang, Y. (2008). Generalized constructions, decoding and implementation of LDPC codes. University of Hawaii at Manoa.
53. Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S. et al. (2000). 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.800-22
54. Milevsky, S. (2023). Sociocyberphysical systems' security models. Ukrainian Information Security Research Journal, 25 (4). https://doi.org/10.18372/2410-7840.25.18224

DOI: 10.15587/1729-4061.2024.295160

DETERMINING THE EFFECT OF A FLOATING POINT ON THE FALCON DIGITAL SIGNATURE ALGORITHM SECURITY (p. 52–59)

Oleksandr Potii
State Service of Special Communications and Information Protection of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2366-0541

Olena Kachko
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Institute of Information Technologies PrJSC, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-9249-0497

Serhii Kandii
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-0552-8341

Yevhenii Kaptol
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-8612-2196

The object of research is digital signatures. The Falcon digital signature scheme is one of the finalists in the NIST post-quantum cryptography competition. Its distinctive feature is the use of floating-point arithmetic. However, floating-point arithmetic has so-called rounding noise, which accumulates during computations and in some cases may lead to significant changes in the processed values. The work considers the problem of using rounding noise to build attacks on implementation. The main result of the study is a novel at-

tack on implementation, which enables the secret key recovery. This attack differs from existing attacks in using two separately secure implementations with different computation orders. As a result of the analysis, the conditions under which secret key recovery is possible were revealed. The attack requires 300,000 signatures and two implementations to recover key. The probability of successful attack ranges from 70 % to 76 %. This probability is explained by the structure of the Gaussian sampling algorithm used in the Falcon digital signature. At the same time, a necessary condition for conducting an attack is identical seed during signature generation. This condition makes the attack more theoretical than practical since the correct implementation of the Falcon makes probability of two identical seeds negligible. However, the possible usage of floating-point noise shows potential existence of additional attack vectors for the Falcon that should be covered in security models. The results could be used in the construction of digital signature security models and their implementation in existing information and communication systems.

Keywords: quantum-resistant transformations, lattice-based cryptography, attack on implementation, NIST PQC, NTRU.

References

1. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Available at: https://falcon-sign.info/
2. Post-Quantum Cryptography. NIST. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography
3. Tran, T., Liu, B. (1977). Accumulation of roundoff errors in floating point FFT. IEEE Transactions on Circuits and Systems, 24 (3), 132–143. https://doi.org/10.1109/tcs.1977.1084316
4. Gentry, C., Peikert, C., Vaikuntanathan, V. (2008). How to Use a Short Basis:Trapdoors for hard lattices and new cryptographic constructions. Available at: https://eprint.iacr.org/2007/432.pdf
5. Lyubashevsky, V., Prest, T. (2015). Quadratic Time, Linear Space Algorithms for Gram-Schmidt Orthogonalization and Gaussian Sampling in Structured Lattices. Lecture Notes in Computer Science, 789–815. https://doi.org/10.1007/978-3-662-46800-5_30
6. Ducas, L., Nguyen, P. Q. (2012). Faster Gaussian Lattice Sampling Using Lazy Floating-Point Arithmetic. Lecture Notes in Computer Science, 415–432. https://doi.org/10.1007/978-3-642-34961-4_26
7. Prest, T. (2015). Gaussian Sampling in Lattice-Based Cryptography. Paris: ENS PARIS. Available at: https://theses.hal.science/tel-01245066
8. Prest, T. (2017). Sharper Bounds in Lattice-Based Cryptography Using the Rényi Divergence. Lecture Notes in Computer Science, 347–374. https://doi.org/10.1007/978-3-319-70694-8_13
9. Ducas, L., Prest, T. (2016). Fast Fourier Orthogonalization. Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation. https://doi.org/10.1145/2930889.2930923
10. Karabulut, E., Aysu, A. (2021). FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks. 2021 58th ACM/IEEE Design Automation Conference (DAC). https://doi.org/10.1109/dac18074.2021.9586131
11. Guerreau, M., Martinelli, A., Ricosset, T., Rossi, M. (2022). The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022 (3), 141–164. https://doi.org/10.46586/tches.v2022.i3.141-164
12. Zhang, S., Lin, X., Yu, Y., Wang, W. (2023). Improved Power Analysis Attacks on Falcon. Lecture Notes in Computer Science, 565–595. https://doi.org/10.1007/978-3-031-30634-1_19
13. Falcon source files (reference implementation). Available at: https://falcon-sign.info/impl/falcon.h.html

DOI: 10.15587/1729-4061.2024.298431

DEVISING A METHOD FOR THE VIRTUAL CLUSTERING OF THE INTERNET OF THINGS EDGE ENVIRONMENT (p. 60–71)

Heorhii Kuchuk
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2862-438X

Oleksandr Mozhaiev
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-1412-2696

Nina Kuchuk
National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-0784-1465

Serhii Tiulieniev
Scientific Research Center for Forensic Science of Information Technologies and Intellectual Property of the Ministry of Justice of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9685-1536

Mykhailo Mozhaiev
Scientific Research Center for Forensic Science of Information Technologies and Intellectual Property of the Ministry of Justice of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-1566-9260

Yurii Gnusov
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-9017-9635

Mykhailo Tsuranov
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2115-7029

Tetiana Bykova
Scientific Research Center for Forensic Science of Information Technologies and Intellectual Property of the Ministry of Justice of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-6722-9470

Sergii Klivets
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-8109-0639

Alexander Kuleshov
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-8223-3814

The object of research is the process of load distribution in the edge environment of the Internet of Things.

The task to improve the efficiency of the functioning of the network of computing devices in the Internet of Things edge environment has been solved. Free resources of heterogeneous single-board computers were used to this end.

In the process of conducting research, an approach to the construction of an architecture for a virtual cluster of computers with limited resources was devised. The design took into account specific features of the edge environment on the Internet of Things. This has made it possible to propose a four-layer architecture instead of the

standard seven-layer architecture of IoT sensor information processing device networks.

Stages in the virtual cluster construction in the edge environment on the Internet of Things were also defined. A three-stage procedure to form a virtual cluster was justified. This procedure made it possible to devise a method for the virtual clustering in the Internet of Things edge environment based on the proposed virtual cluster architecture.

The proposed method for building a virtual cluster in the Internet of Things edge environment was investigated. With a small network load, a virtual cluster has no advantage over a classic cluster. But with the growth of the network load, the virtual cluster prevails over the classic cluster in total performance; the advantage in total performance can exceed 10 %. It was also proven that for a heterogeneous environment, performance changes at full network load significantly depend on the number of virtual node groups. The research results on the method for building a virtual cluster in the Internet of Things edge environment can be explained by improving the balance of the network load at virtual clustering.

Keywords: Internet of Things, virtual cluster, edge environment, heterogeneity, fuzzy computing, balance.

References

1. Schulz, A. S. (2023). User Interactions with Internet of Things (IoT) Devices in Shared Domestic Spaces. Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia. https://doi.org/10.1145/3626705.3632615
2. Pardo, C., Wei, R., Ivens, B. S. (2022). Integrating the business networks and internet of things perspectives: A system of systems (SoS) approach for industrial markets. Industrial Marketing Management, 104, 258–275. https://doi.org/10.1016/j.indmarman.2022.04.012
3. Zakharchenko, A., Stepanets, O. (2023). Digital twin value in intelligent building development. Advanced Information Systems, 7 (2), 75–86. https://doi.org/10.20998/2522-9052.2023.2.11
4. Chalapathi, G. S. S., Chamola, V., Vaish, A., Buyya, R. (2021). Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions. Advances in Information Security, 293–325. https://doi.org/10.1007/978-3-030-57328-7_12
5. Zuev, A., Karaman, D., Olshevskiy, A. (2023). Wireless sensor synchronization method for monitoring short-term events. Advanced Information Systems, 7 (4), 33–40. https://doi.org/10.20998/2522-9052.2023.4.04
6. Krishnan, S., Ilmudeen, A. (2023). Internet of Medical Things in Smart Healthcare. Apple Academic Press. https://doi.org/10.1201/9781003369035
7. Fatlawi, A., Al-Dujaili, M. J. (2023). Integrating the internet of things (IoT) and cloud computing challenges and solutions: A review. AIP Conference Proceedings. https://doi.org/10.1063/5.0181842
8. Qayyum, T., Trabelsi, Z., Waqar Malik, A., Hayawi, K. (2022). Mobility-aware hierarchical fog computing framework for Industrial Internet of Things (IIoT). Journal of Cloud Computing, 11 (1). https://doi.org/10.1186/s13677-022-00345-y
9. Lu, S., Wu, J., Wang, N., Duan, Y., Liu, H., Zhang, J., Fang, J. (2021). Resource provisioning in collaborative fog computing for multiple delay-sensitive users. Software: Practice and Experience, 53 (2), 243–262. https://doi.org/10.1002/spe.3000
10. Petrovska, I., Kuchuk, H. (2023). Adaptive resource allocation method for data processing and security in cloud environment. Advanced Information Systems, 7 (3), 67–73. https://doi.org/10.20998/2522-9052.2023.3.10
11. Kuchuk, G., Nechausov, S., Kharchenko, V. (2015). Two-stage optimization of resource allocation for hybrid cloud data store. 2015 International Conference on Information and Digital Technologies. https://doi.org/10.1109/dt.2015.7222982
12. Li, G., Liu, Y., Wu, J., Lin, D., Zhao, S. (2019). Methods of Resource Scheduling Based on Optimized Fuzzy Clustering in Fog Computing. Sensors, 19(9), 2122. https://doi.org/10.3390/s19092122
13. Jamil, B., Shojafar, M., Ahmed, I., Ullah, A., Munir, K., Ijaz, H. (2019). A job scheduling algorithm for delay and performance optimization in fog computing. Concurrency and Computation: Practice and Experience, 32 (7). https://doi.org/10.1002/cpe.5581
14. Gomathi, B., Saravana Balaji, B., Krishna Kumar, V., Abouhawwash, M., Aljahdali, S., Masud, M., Kuchuk, N. (2022). Multi-Objective Optimization of Energy Aware Virtual Machine Placement in Cloud Data Center. Intelligent Automation & Soft Computing, 33 (3), 1771–1785. https://doi.org/10.32604/iasc.2022.024052
15. Proietti Mattia, G., Beraldi, R. (2023). P2PFaaS: A framework for FaaS peer-to-peer scheduling and load balancing in Fog and Edge computing. SoftwareX, 21, 101290. https://doi.org/10.1016/j.softx.2022.101290
16. Kuchuk, N., Mozhaiev, O., Semenov, S., Haichenko, A., Kuchuk, H., Tiulieniev, S. et al. (2023). Devising a method for balancing the load on a territorially distributed foggy environment. Eastern-European Journal of Enterprise Technologies, 1 (4 (121)), 48–55. https://doi.org/10.15587/1729-4061.2023.274177
17. Kuchuk, N., Ruban, I., Zakovorotnyi, O., Kovalenko, A., Shyshatskyi, A., Sheviakov, I. (2023). Traffic Modeling for the Industrial Internet of NanoThings. 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek). https://doi.org/10.1109/khpiweek61412.2023.10312856
18. Sharma, S., Saini, H. (2019). A novel four-tier architecture for delay aware scheduling and load balancing in fog environment. Sustainable Computing: Informatics and Systems, 24, 100355. https://doi.org/10.1016/j.suscom.2019.100355
19. 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. https://doi.org/10.15587/1729-4061.2021.238407
20. Malik, U. M., Javed, M. A., Frnda, J., Rozhon, J., Khan, W. U. (2022). Efficient Matching-Based Parallel Task Offloading in IoT Networks. Sensors, 22 (18), 6906. https://doi.org/10.3390/s22186906
21. Liu, L., Chen, H., Xu, Z. (2022). SPMOO: A Multi-Objective Offloading Algorithm for Dependent Tasks in IoT Cloud-Edge-End Collaboration. Information, 13 (2), 75. https://doi.org/10.3390/info13020075
22. Ghenai, A., Kabouche, Y., Dahmani, W. (2018). Multi-user dynamic scheduling-based resource management for Internet of Things applications. 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC). https://doi.org/10.1109/iintec.2018.8695308
23. Kuchuk, G. A., Akimova, Yu. A., Klimenko, L. A. (2000). Method of optimal allocation of relational tables. Engineering Simulation, 17 (5), 681–689.
24. Wei, J.-Y., Wu, J.-J. (2023). Resource Allocation Algorithm in Industrial Internet of Things Based on Edge Computing. Dongbei Daxue

Xuebao / Journal of Northeastern University, 44 (8). https://doi.org/10.12068/j.issn.1005-3026.2023.08.002

25. Yaloveha, V., Podorozhniak, A., Kuchuk, H. (2022). Convolutional neural network hyperparameter optimization applied to land cover classification. Radioelectronic and computer systems, 1, 115–128. https://doi.org/10.32620/reks.2022.1.09
26. Zhang, Z. (2021). A computing allocation strategy for Internet of things' resources based on edge computing. International Journal of Distributed Sensor Networks, 17 (12), 155014772110648. https://doi.org/10.1177/15501477211064800
27. Attar, H., Khosravi, M. R., Igorovich, S. S., Georgievan, K. N., Alhihi, M. (2021). E-Health Communication System with Multiservice Data Traffic Evaluation Based on a G/G/1 Analysis Method. Current Signal Transduction Therapy, 16 (2), 115–121. https://doi.org/10.2174/1574362415666200224094706
28. Kammoun, N., Abassi, R., Guemara, S. (2019). Towards a New Clustering Algorithm based on Trust Management and Edge Computing for IoT. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). https://doi.org/10.1109/iwcmc.2019.8766492
29. Kovalenko, A., Kuchuk, H. (2022). Methods to Manage Data in Self-healing Systems. Studies in Systems, Decision and Control, 113–171. https://doi.org/10.1007/978-3-030-96546-4_3
30. Yang, J., Bao, L., Liu, W., Yang, R., Wu, C. Q. (2023). On a Meta Learning-Based Scheduler for Deep Learning Clusters. IEEE Transactions on Cloud Computing, 11 (4), 3631–3642. https://doi.org/10.1109/tcc.2023.3308161
31. Pisching, M. A., Pessoa, M. A. O., Junqueira, F., dos Santos Filho, D. J., Miyagi, P. E. (2018). An architecture based on RAMI 4.0 to discover equipment to process operations required by products. Computers & Industrial Engineering, 125, 574–591. https://doi.org/10.1016/j.cie.2017.12.029

DOI: 10.15587/1729-4061.2024.298687

THE DEPENDENCE OF THE EFFECTIVENESS OF NEURAL NETWORKS FOR RECOGNIZING HUMAN VOICE ON LANGUAGE (p. 72–81)

Aigul Nurlankyzy
Satbayev University, Almaty, Republic of Kazakhstan
Almaty University of Power Engineering and Telecommunications, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0791-8573

Ainur Akhmediyarova
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-4439-7313

Ainur Zhetpisbayeva
S. Seifullin Kazakh Agro Technical Research University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-4525-5299

Timur Namazbayev
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-2389-2262

Asset Yskak
S. Seifullin Kazakh Agro Technical Research University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1196-3155

Nurdaulet Yerzhan
Satbayev University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0009-0000-2734-3167

Bekbolat Medetov
S. Seifullin Kazakh Agro Technical Research University, Astana, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-5594-8435

This study examines the effectiveness of neural network architectures (multilayer perceptron MLP, convolutional neural network CNN, recurrent neural network RNN) for human voice recognition, with an emphasis on the Kazakh language. Problems related to language, the difference between speakers, and the influence of network architecture on recognition accuracy are considered. The methodology includes extensive training and testing, studying the accuracy of recognition in different languages, and different sets of data on speakers. Using a comparative analysis, this study evaluates the performance of three architectures trained exclusively in the Kazakh language. The testing included statements in Kazakhs and other languages, while the number of speakers varied to assess its impact on recognition accuracy.

During the study, the results showed that CNN neural networks are more effective in recognizing human voice than RNN and MLP. Also, it was found that the CNN has a higher accuracy in recognizing the human voice in the Kazakh language, both for a small and for a large number of announcers. For example, for 20 speakers, the recognition error in Russian was 21.86 %, whereas in Kazakhs it was 10.6 %. A similar trend was observed for 80 speakers: 16.2 % Russians and 8.3 % Kazakhs. It can also be argued that learning one language does not guarantee high recognition accuracy in other languages. Therefore, the accuracy of human voice recognition by neural networks depends significantly on the language in which training is conducted.

In addition, this study highlights the importance of different sets of speaker data to achieve optimal results. This knowledge is crucial for advancing the development of reliable human voice recognition systems that can accurately identify different human voices in different language contexts.

Keywords: Artificial intelligence, neural networks, CNN, RNN, MLP, voice activity detector, human voice recognition, the effectiveness of training, language specifics, recognition accuracy.

References

1. Mihalache, S., Burileanu, D. (2022). Using Voice Activity Detection and Deep Neural Networks with Hybrid Speech Feature Extraction for Deceptive Speech Detection. Sensors, 22 (3), 1228. https://doi.org/10.3390/s22031228
2. Lee, Y., Min, J., Han, D. K., Ko, H. (2020). Spectro-Temporal Attention-Based Voice Activity Detection. IEEE Signal Processing Letters, 27, 131–135. https://doi.org/10.1109/lsp.2019.2959917
3. Sofer, A., Chazan, S. E. (2022). CNN self-attention voice activity detector. arXiv. https://doi.org/10.48550/arXiv.2203.02944
4. Zhang, X.-L., Xu, M. (2022). AUC optimization for deep learning-based voice activity detection. EURASIP Journal on Audio, Speech, and Music Processing, 2022 (1). https://doi.org/10.1186/s13636-022-00260-9
5. Jia, F., Majumdar, S., Ginsburg, B. (2021). MarbleNet: Deep 1D Time-Channel Separable Convolutional Neural Network for Voice Activity Detection. ICASSP 2021 - 2021 IEEE International Con-

ference on Acoustics, Speech and Signal Processing (ICASSP). https://doi.org/10.1109/icassp39728.2021.9414470

6. Heo, Y., Lee, S. (2023). Supervised Contrastive Learning for Voice Activity Detection. Electronics, 12 (3), 705. https://doi.org/10.3390/electronics12030705
7. Faghani, M., Rezaee-Dehsorkh, H., Ravanshad, N., Aminzadeh, H. (2023). Ultra-Low-Power Voice Activity Detection System Using Level-Crossing Sampling. Electronics, 12 (4), 795. https://doi.org/10.3390/electronics12040795
8. Lee, G. W., Kim, H. K. (2020). Multi-Task Learning U-Net for Single-Channel Speech Enhancement and Mask-Based Voice Activity Detection. Applied Sciences, 10 (9), 3230. https://doi.org/10.3390/app10093230
9. Arslan, O., Engin, E. Z. (2019). Noise Robust Voice Activity Detection Based on Multi-Layer Feed-Forward Neural Network. Electrica, 19 (2), 91–100. https://doi.org/10.26650/electrica.2019.18042
10. Oh, Y. R., Park, K., Park, J. G. (2020). Online Speech Recognition Using Multichannel Parallel Acoustic Score Computation and Deep Neural Network (DNN)- Based Voice-Activity Detector. Applied Sciences, 10 (12), 4091. https://doi.org/10.3390/app10124091
11. Sehgal, A., Kehtarnavaz, N. (2018). A Convolutional Neural Network Smartphone App for Real-Time Voice Activity Detection. IEEE Access, 6, 9017–9026. https://doi.org/10.1109/access.2018.2800728
12. Mukherjee, H., Obaidullah, Sk. Md., Santosh, K. C., Phadikar, S., Roy, K. (2018). Line spectral frequency-based features and extreme learning machine for voice activity detection from audio signal. International Journal of Speech Technology, 21 (4), 753–760. https://doi.org/10.1007/s10772-018-9525-6
13. Ali, Z., Talha, M. (2018). Innovative Method for Unsupervised Voice Activity Detection and Classification of Audio Segments. IEEE Access, 6, 15494–15504. https://doi.org/10.1109/access.2018.2805845
14. Jung, Y., Kim, Y., Choi, Y., Kim, H. (2018). Joint Learning Using Denoising Variational Autoencoders for Voice Activity Detection. Interspeech 2018. https://doi.org/10.21437/interspeech.2018-1151
15. Yoshimura, T., Hayashi, T., Takeda, K., Watanabe, S. (2020). End-to-End Automatic Speech Recognition Integrated with CTC-Based Voice Activity Detection. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). https://doi.org/10.1109/icassp40776.2020.9054358
16. Bredin, H., Laurent, A. (2021). End-To-End Speaker Segmentation for Overlap-Aware Resegmentation. Interspeech 2021. https://doi.org/10.21437/interspeech.2021-560
17. Lavechin, M., Gill, M.-P., Bousbib, R., Bredin, H., Garcia-Perera, L. P. (2020). End-to-End Domain-Adversarial Voice Activity Detection. Interspeech 2020. https://doi.org/10.21437/interspeech.2020-2285
18. Cornell, S., Omologo, M., Squartini, S., Vincent, E. (2020). Detecting and Counting Overlapping Speakers in Distant Speech Scenarios. Interspeech 2020. https://doi.org/10.21437/interspeech.2020-2671
19. Tan, X., Zhang, X.-L. (2021). Speech Enhancement Aided End-To-End Multi-Task Learning for Voice Activity Detection. ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). https://doi.org/10.1109/icassp39728.2021.9414445
20. Varzandeh, R., Adiloglu, K., Doclo, S., Hohmann, V. (2020). Exploiting Periodicity Features for Joint Detection and DOA Estimation of Speech Sources Using Convolutional Neural Networks. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). https://doi.org/10.1109/icassp40776.2020.9054754
21. Medetov, B., Kulakayeva, A., Zhetpisbayeva, A., Albanbay, N., Kabduali, T. (2023). Identifying the regularities of the signal detection method using the Kalman filter. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 26–34. https://doi.org/10.15587/1729-4061.2023.289472
22. Mussakhojayeva, S., Khassanov, Y., Atakan Varol, H. (2022). KSC2: An Industrial-Scale Open-Source Kazakh Speech Corpus. Interspeech 2022. https://doi.org/10.21437/interspeech.2022-421
23. Mussakhojayeva, S., Khassanov, Y., Atakan Varol, H. (2021). A Study of Multilingual End-to-End Speech Recognition for Kazakh, Russian, and English. Lecture Notes in Computer Science, 448–459. https://doi.org/10.1007/978-3-030-87802-3_41
24. Mussakhojayeva, S., Dauletbek, K., Yeshpanov, R., Varol, H. A. (2023). Multilingual Speech Recognition for Turkic Languages. Information, 14 (2), 74. https://doi.org/10.3390/info14020074
25. Musaev, M., Mussakhojayeva, S., Khujayorov, I., Khassanov, Y., Ochilov, M., Atakan Varol, H. (2021). USC: An Open-Source Uzbek Speech Corpus and Initial Speech Recognition Experiments. Lecture Notes in Computer Science, 437–447. https://doi.org/10.1007/978-3-030-87802-3_40
26. Ardila, R., Branson, M., Davis, K., Henretty, M., Kohler, M., Meyer, J. et al. (2020). Common voice: A massively-multilingualspeech corpus. arXiv. https://doi.org/10.48550/arXiv.1912.06670
27. Medetov, B., Serikov, T., Tolegenova, A., Zhexebay, D., Yskak, A., Namazbayev, T., Albanbay, N. (2023). Development of a model for determining the necessary FPGA computing resource for placing a multilayer neural network on it. Eastern-European Journal of Enterprise Technologies, 4 (4 (124)), 34–45. https://doi.org/10.15587/1729-4061.2023.281731
28. Aigul, K., Altay, A., Yevgeniya, D., Bekbolat, M., Zhadyra, O. (2022). Improvement of Signal Reception Reliability at Satellite Spectrum Monitoring System. IEEE Access, 10, 101399–101407. https://doi.org/10.1109/access.2022.3206953
29. Aitmagambetov, A., Butuzov, Y., Butuzov, Y., Tikhvinskiy, V., Tikhvinskiy, V., Kulakayeva, A. et al. (2021). Energy budget and methods for determining coordinates for a radiomonitoring system based on a small spacecraft. Indonesian Journal of Electrical Engineering and Computer Science, 21 (2), 945. https://doi.org/10.11591/ijeecs.v21.i2.pp945-956
30. Albanbay, N., Medetov, B., Zaks, M. A. (2021). Exponential distribution of lifetimes for transient bursting states in coupled noisy excitable systems. Chaos: An Interdisciplinary Journal of Nonlinear Science, 31 (9). https://doi.org/10.1063/5.0059102
31. Albanbay, N., Medetov, B., Zaks, M. A. (2020). Statistics of Lifetimes for Transient Bursting States in Coupled Noisy Excitable Systems. Journal of Computational and Nonlinear Dynamics, 15 (12). https://doi.org/10.1115/1.4047867

АНОТАЦІЇ
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2024.298598

УДОСКОНАЛЕННЯ МЕТОДУ НЕКОГЕРЕНТНОЇ ОБРОБКИ СИГНАЛІВ МЕРЕЖЕЮ ДВОХ МАЛОГАБАРИТНИХ РАДАРІВ ПРИ ВИЯВЛЕННІ МАЛОПОМІТНОГО ПОВІТРЯНОГО ОБ'ЄКТА (с. 6–13)

Г. В. Худов, С. П. Ярош, О. О. Костиря, О. О. Олексенко, М. М. Хомик, А. А. Звонко, Б. А. Лісогорський, П. Є. Минко, С. М. Суконько, Т. М. Кравець

Об'єктом дослідження є процес виявлення малопомітних повітряних об'єктів мережею двох малогабаритних радарів при некогерентній обробці сигналів. Основна гіпотеза дослідження полягала в тому, що об'єднання двох малогабаритних радарів у мережу дозволить підвищити якість виявлення малопомітних повітряних об'єктів при некогерентній обробці сигналів.

Удосконалений метод виявлення малопомітного повітряного об'єкту мережею двох малогабаритних радарів при некогерентній обробці сигналів, на відміну від відомих, передбачає:

– синхронний огляд повітряного простору малогабаритними радарами;

– випромінювання зондувального сигналу кожним малогабаритним радаром;

– приймання ехо-сигналів від малопомітного повітряного об'єкта двома малогабаритними радарами;

– узгоджена фільтрації вхідних ехо-сигналів (розділення ехо-сигналів);

– квадратичне детектування сигналів на виходах узгоджених фільтрів;

– підсумовування продетектованих сигналів на виходах узгоджених фільтрів;

– підсумовування виходів суматорів двох малогабаритних радарів.

Наведена схема оптимального по критерію Неймана-Пірсона виявлювача малопомітного повітряного об'єкту при некогерентній обробці сигналів.

Проведено оцінювання якості виявлення малопомітного повітряного об'єкту мережею двох малогабаритних радарів при некогерентній обробці сигналів. Встановлено, що при некогерентній обробці виграш у значенні умовної імовірності правильного виявлення складає в середньому від 19 % до 26 % в залежності від значення величини сигнал/шум. Виграш у значенні умовної ймовірності правильного виявлення є більшим при малих значеннях відношення сигнал/шум. В той же час, виграш у значенні сигнал/шум є більш суттєвим при когерентній обробці сигналів, ніж при некогерентній обробці сигналів мережею двох малогабаритних радарів.

Ключові слова: малогабаритний радар, виявлення повітряного об'єкту, некогерентна обробка, умовна ймовірність правильного виявлення.

DOI: 10.15587/1729-4061.2024.298268

ОПТИМІЗАЦІЯ АЛГОРИТМУ LEACH У ВИБОРІ КЛАСТЕРНИХ ГОЛІВ, ЗАСНОВАНА НА ЗАЛИШКОВІЙ ЕНЕРГІЇ В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ (с. 14–21)

Ferry Fachrizal, Muhammad Zarlis, Poltak Sihombing, Suherman Suherman

Об'єктом дослідження є алгоритм LEACH (Low-Energy Adaptive Clustering Hierarchy) в контексті бездротових сенсорних мереж. Проблема в цьому дослідженні полягає в дисбалансі споживання енергії між кластерами, який впливає на час роботи батареї та впливає на продуктивність мережі. Інші проблеми включають вибір голови кластера, який не сфокусований, тому важко збалансувати продуктивність мережі, а також обчислювальні обмеження, які потребують оптимізації. Отримані результати представлені у формі оптимізації алгоритму вимивання шляхом модифікації алгоритму вимивання на основі кластеризації, який буде використовуватися в бездротових сенсорних мережах.

Здійснюючи модифікації, це дослідження використовує кілька етапів у процесі вибору сенсорних вузлів, які стануть членами, що функціонуватимуть як голови кластера в кластері, який використовуватиметься в бездротовій сенсорній мережі. В алгоритмі LEACH (Low-Energy Adaptive Clustering Hierarchy) голова кластера буде обрана на основі модифікованого значення ймовірності. Модифікація алгоритму шляхом врахування двох факторів, а саме відстані та залишку енергії, що використовується в процесі вибору керівника кластера в мережі, і збільшення часу використання мережі має базуватися на споживанні енергії, а потім порівнюватись із залишком енергії. Змінюючи алгоритм LEACH (Low-Energy Adaptive Clustering Hierarchy), потрібно звернути увагу на коефіцієнт відстані між вузлами датчика та вибраним кластером, щоб це могло призвести до підвищення продуктивності мережі. Тривалість життя мережі вказується середнім часом смерті першого вузла в мережі.

Це дослідження є новим у створенні модифікованого алгоритму вилуговування шляхом покращення продуктивності мережі та подовження терміну служби батареї, щоб його можна було використовувати для бездротових сенсорних мереж у контексті пом'якшення стихійних лих.

Ключові слова: кластерна головка, мережа датчиків, алгоритм вилуговування, оптимізація енергії, час роботи батареї.

DOI: 10.15587/1729-4061.2024.298476

РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ТА ВИПРАВЛЕННЯ ПОМИЛОК ПЕРЕДАЧІ ДАНИХ У IoT СИСТЕМАХ МОНІТОРИНГУ СТАНУ ОБ'ЄКТІВ (с. 22–33)

В. В. Соколовський, Е. В. Жаріков, С. Ф. Теленик

Об'єктом дослідження є IOT системи моніторингу стану об'єктів.

Проблема, що вирішувалась, – це розробка інноваційного методу виявлення і виправлення помилок передачі даних у мережах систем інтернету речей.

Суть результатів у тому, що розроблено метод виявлення та виправлення багатократних помилок передачі при побайтовій передачі блока інформації. Метод відрізняється оригінальною схемою кодування, яка передбачає розрахунок контрольних бітів, а також перемішування бітів блока шляхом виконання операцій бітового зсуву. Особливість методу у тому, що при передачі кодового слова будь який біт може бути спотворений, але він належить до різних кодових комбінацій коду Хемінга. Це дозволяє при декодуванні виявити та виправити багатократні помилки передачі даних, а також дозволяє виправляти численні помилки різних байтів, що належать до одного блоку.

Розроблені прості алгоритми процедур кодування та декодування, та розроблені програми процедури кодування інформаційного блоку та процедури декодування з виявленням та виправленням помилок. Також розроблена програмна модель каналу передачі даних з можливістю внесення багатократних помилок при моделюванні процесу передачі даних. Усі програми розроблені на мові Python, хоча можливо використання інших мов.

Використовуючи розроблену програмну модель каналу передачі даних був проведений експеримент. Експериментально підтверджено працездатність розробленого методу та доказано, що при його використанні підвищується завадостійкість каналу передачі даних. Це обумовлено тим, що розроблений метод дозволяє виявляти та виправляти усі помилки передачі кодового слова з кратністю від 1 до 8-ми, що і було підтверджено експериментально.

Основною сферою використання розробленого методу вбачається мережі IoT систем. Насамперед систем моніторингу стану об'єктів.

Ключові слова: метод виправлення помилок, коди Хемінга, інтернет речей, моніторинг стану об'єктів.

DOI: 10.15587/1729-4061.2024.298844

РОЗРОБКА МЕТОДОЛОГІЇ БАГАТОКОНТУРНОЇ СИСТЕМИ БЕЗПЕКИ У СОЦІОКІБЕРФІЗИЧНИХ СИСТЕМАХ (с. 34–51)

С. В. Мілевський, О. Г. Король, Г. В. Микитин, І. Л. Лозова, С. Г. Солнишкова, І. Г. Гусарова, А. В. Гребенюк, А. В. Власов, В. М. Сухотеплий, Д. С. Балагура

Постійно кількість загроз безпеці об'єктів критичної інфраструктури, до яких належать і соціокіберфізичні системи призводить до зниження якості послуг безпеки та рівня захищеності елементів інфраструктури. Об'єктом дослідження є процес побудови комплексної системи захисту в соціокіберфізичних системах. Недосконаліть механізмів забезпечення безпеки об'єктів критичної інфраструктури, до яких належать і соціокіберфізичні системи, технологічна складність виявлення нових загроз безпеці зумовлює нагальну необхідність кардинального перегляду чинних підходів до її забезпечення. Отже, ставати зрозуміло, що розробка нового підходу до забезпечення безпеки інформаційних ресурсів у соціокіберфізичних системах. У статті запропоновано новий підхід методологічних засад побудови багатоконтурних систем захисту інформації із внутрішнім та зовнішнім контурами на кожній із платформ соціокіберфізичних систем. Такий підхід формується на універсальному класифікаторі загроз, який враховує не технічний аспект загроз, а і їх комплексування з методами соціальної інженерії, їхньої синергії гібридності. Враховується соціополітичний вплив на реалізацію загроз, а також запропоновано практичні механізми забезпечення основних послуг безпеки на основі постквантових алгоритмів. Для забезпечення основних послуг безпеки у запропонованої багатоконтурної системи захисту пропонується використовувати постквантові алгоритми – крипто-кодові конструкції Мак-Еліса, які забезпечують Рпом=10^{-9}–10^{-12},безпечній час Тбезп =10^{25}–10^{35} групових операцій. У рамках запропонованого підходу у загальному вигляді формалізовано проблему підвищення рівня захищеності інформації та визначено подальші шляхи її вирішення.

Ключові слова: соціокіберфізична система, кібербезпека, інформаційна безпека, безпека інформації, об'єкти критичної інфраструктури.

DOI: 10.15587/1729-4061.2024.295160

ВИЗНАЧЕННЯ ВПЛИВУ ПЛАВАЮЧОЇ ТОЧКИ НА БЕЗПЕКУ АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ FALCON (с. 52–59)

О. В. Потій, О. Г. Качко, С. О. Кандій, Є. Ю. Каптьол

Об'єктом дослідження є електронні підписи. Схема електронного підпису Falcon є одним з фіналістів конкурсу NIST з постквантової криптографії. Однією з її ключових особливостей є використання обчислень з плаваючою крапкою. Проте, обчислення з пла-

ваючою крапкою мають так званий шум округлення, що накопичується під час обчислень і у деяких випадках може призводити до суттєвих змін в оброблюваних значеннях. Робота присвячена проблемі використання шуму округлення для побудови атак на реалізацію електронних підписів. Головним результатом роботи є нова атака на реалізацію, що дозволяє відтворити таємний ключ. Нова атака відрізняється від вже існуючих атак використанням двох окремо безпечних реалізацій з різним порядком обчислень. У результаті проведеного аналізу було виявлено умови, за яких відтворення таємного ключа є можливим. Атака потребує 300000 підписів та наявності двох реалізацій для відтворення ключа. Ймовірність вдалого завершення атаки складає від 70 % до 76 %. Така ймовірність пояснюється структурою алгоритму вибірки Гауса, що використовується в електронному підписі Falcon. При цьому необхідною умовою проведення атаки є однакові seed при виробленні підпису. Ця умова робить атаку скоріш теоретичною, ніж практичною, оскільки при правильному впровадженні ЕП Falcon ймовірність використання двох однакових seed є незначною. Проте, можливість використання шуму обчислень з плаваючою крапкою показує, що для ЕП Falcon існують додаткові вектори атак, що мають враховуватися в моделях безпеки та потребують детальних досліджень. Отримані результати можуть бути використані при побудові моделей безпеки електронних підписів та їх впровадженні в існуючі інформаційно-комунікаційні системи.

Ключові слова: квантово-стійкі перетворення, криптографія на решітках, атака на реалізацію, NIST PQC, NTRU.

DOI: 10.15587/1729-4061.2024.298431

РОЗРОБКА МЕТОДУ ВІРТУАЛЬНОЇ КЛАСТЕРІЗАЦІЇ ГРАНИЧНОГО СЕРЕДОВИЩА ІНТЕРНЕТУ РЕЧЕЙ (с. 60–71)

Г. А. Кучук, О. О. Можаєв, Н. Г. Кучук, С. А. Тюлєнєв, М. О. Можаєв, Ю. В. Гнусов, М. В. Цуранов, Т. М. Бикова, С. І. Клівець, О. В. Кулєшов

Об'єктом дослідження є процес розподілу навантаження у граничному середовищі Інтернету речей.

Вирішене завдання підвищення ефективності функціонування мережі обчислювальних пристроїв граничного середовища Інтернету речей. Для цього були задіяні вільні ресурси гетерогенних одноплатних комп'ютерів.

В процесі проведення досліджень розроблений підхід до формування архітектури для віртуального кластера комп'ютерів з обмеженими ресурсами. При розробці враховувались специфічні особливості граничного середовища Інтернету речей. Це дозволило запропонувати чотирирівневу архітектуру замість стандартної семирівневої архітектури мереж пристроїв обробки інформації датчиків Інтернету речей.

Також визначені етапи формування віртуального кластера у граничному середовищі Інтернету речей. Обґрунтована трьохетапна процедура формування віртуального кластера. Дана процедура дозволила розробити метод віртуальної кластеризації граничного середовища Інтернету речей на базі запропонованої архітектури віртуального кластера.

Досліджений запропонований метод побудови віртуального кластера граничного середовища Інтернету речей. При невеликій завантаженості мережі віртуальний кластер не має переваги над класичним кластером. Але при зростанні завантаженості мережі віртуальний кластер переважає класичний кластер за сумарною продуктивністю, перевага за сумарною продуктивністю може перевищувати 10 %. Також доведено, що для гетерогенного середовища зміни продуктивності при повному завантаженні мережі суттєво залежать від кількості віртуальних груп вузлів. Отримані результати дослідження метода побудови віртуального кластера граничного середовища Інтернету речей можна пояснити підвищенням збалансованості навантаження мережі при віртуальній кластеризації.

Ключові слова: інтернет речей, віртуальний кластер, граничне середовище, гетерогенність, туманні обчислення, збалансованість.

DOI: 10.15587/1729-4061.2024.298687

ЗАЛЕЖНІСТЬ ЕФЕКТИВНОСТІ НЕЙРОМЕРЕЖ ДЛЯ РОЗПІЗНАВАННЯ ЛЮДСЬКОГО ГОЛОСУ В ЗАЛЕЖНОСТІ ВІД МОВИ (с. 72–81)

Aigul Nurlankyzy, Ainur Akhmediyarova, Ainur Zhetpisbayeva, Timur Namazbayev, Asset Yskak, Nurdaulet Yerzhan, Bekbolat Medetov

У цьому дослідженні розглядається ефективність архітектур нейронних мереж (багатошаровий персептрон БШП, згорткова нейронна мережа ЗНМ, рекурентна нейронна мережа РНМ) для розпізнавання голосу людини, з акцентом на казахську мову. Розглядаються проблеми, пов'язані з мовою, відмінністю мовців, впливом архітектури мережі на точність розпізнавання. Методологія включає тривале навчання та тестування, вивчення точності розпізнавання різними мовами та різні набори даних про носіїв мови. Використовуючи порівняльний аналіз, це дослідження оцінює продуктивність трьох архітектур, які навчаються виключно казахською мовою. Тестування включало висловлювання казахською та іншими мовами, у той час як кількість носіїв змінювалася, щоб оцінити його вплив на точність розпізнавання.

Під час дослідження результати показали, що нейронні мережі ЗНМ більш ефективні в розпізнаванні людського голосу, ніж РНМ і БШП. Також виявилося, що ЗНМ має більш високу точність розпізнавання людського голосу казахською мовою, як для невеликої, так і для великої кількості дикторів. Наприклад, для 20 мовців помилка розпізнавання російською склала 21,86 %, а

казахською – 10,6 %. Подібна тенденція спостерігалася для 80 носіїв мови: 16,2 % росіян і 8,3 % казахів. Можна також стверджувати, що вивчення однієї мови не гарантує високої точності розпізнавання іншими мовами. Тому точність розпізнавання людського голосу нейронними мережами істотно залежить від мови, якою ведеться навчання.

Крім того, це дослідження підкреслює важливість різних наборів даних про спікерів для досягнення оптимальних результатів. Ці знання мають вирішальне значення для просування в розробці надійних систем розпізнавання людського голосу, які можуть точно ідентифікувати різні людські голоси в різних мовних контекстах.

Ключові слова: штучний інтелект, нейронні мережі, ЗНМ, РНМ, БШП, детектор голосової активності, розпізнавання людського голосу, ефективність навчання, мовні особливості, точність розпізнавання.