ABSTRACT AND REFERENCES
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2021.242935

DEVELOPMENT A METHOD FOR DETERMINING THE COORDINATES OF AIR OBJECTS BY RADARS WITH THE ADDITIONAL USE OF MULTILATERATION TECHNOLOGY (p. 6–16)

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

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

Shamil Ikhsanov
Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine
ORCID: https://orcid.org/0000-0002-9053-7068

Oleksii Diakonov
Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine
ORCID: https://orcid.org/0000-0001-7438-7066

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

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

Yevhen Drob
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-2015-220X

Oleh Kharun
National Academy of the State Border Guard Service of Ukraine named after B. Khmelnitsky, Khmelnitsky, Ukraine
ORCID: https://orcid.org/0000-0003-3474-8095

Serhii Cherkashyn
National Academy of the National Guard of Ukraine, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-1973-3648

Oleksii Serdiuk
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-3600-0611

This paper reports an experimental study aimed at confirming disruptions in the operation of ADS-B receivers. The experimental investigation into disruptions in the operation of ADS-B receivers involved the FlightAware Piaware receiver. Examples of the disrupted performance of ADS-B receivers are given. It was found that the experimentally detected disruptions in the operation of ADS-B receivers could lead to a decrease in the accuracy of determining the coordinates of air objects with the joint use of the radar station and multilateration technology.

A method for determining the coordinates of an air object by radar station with additional use of multilateration technology has been devised. The method involves the following stages: entering initial data, the calculation of distances between the points of reception and the air object, the computation of the inconsistency vector, the calculation of the matrix of partial derivatives taking into consideration the estimates of the coordinates of an air object at the previous iteration, the computation of the correction, the calculation of the refined coordinates of the air object. Unlike those known ones, the improved method for determining the coordinates of an air object by a radar station additionally uses multilateration technology.

The accuracy of determining the air objects' coordinates by a radar station with the additional use of multilateration technology was estimated. It was established that the additional application of multilateration technology would reduce the error in determining the coordinates of an air object by 1.58 to 2.39 times on average, compared to using only an autonomous radar station.

Keywords: radar station, multilateration technology, air object, definition method, root mean square error.

References

1. Melvin, W. L., Scheer, J. A. (Eds.) (2013). Principles of modern radar. Vol. II. Advanced techniques. Raleigh: SciTech Publishing, 846.
2. Melvin, W. L., Scheer, J. A. (Eds.) (2013). Principles of modern radar. Vol. III. Radar applications. IET, 820. doi: https://doi.org/10.1049/sbra503e
3. Van 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
4. 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
5. 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
6. Marpl-ml, S. L. (1990). Cifrovoy spektral'nyy analiz i ego prilozheniya. Moscow: Mir, 584.
7. Klimov, S. A. (2013). Metod povysheniya razreshayuschey sposobnosti radiolokacionnyh sistem pri cifrovoy obrabotke signalov. Zhurnal radioelektroniki, 1. Available at: http://jre.cplire.ru/jre/jan13/1/text.html
8. 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
9. 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
10. Willis, N. J. (2004). Bistatic Radar. IET. doi: https://doi.org/10.1049/sbra003e

11. Khudov, H., Zvonko, A., Kovalevskyi, S., Lishchenko, V., Zots, F. (2018). Method for the detection of smallsized 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
12. 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
13. Leshchenko, S. P., Kolesnyk, O. M., Hrytsaienko, S. A., Burkovskyi, S. I. (2017). Use of the ADS-B information in order to improve quality of the air space radar reconnaissance. Science and Technology of the Air Force of Ukraine, 3 (28), 69–75. doi: https://doi.org/10.30748/nitps.2017.28.09
14. 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
15. LORAN-C. Available at: https://www.skybrary.aero/index.php/LORAN-C
16. Multilateration (MLAT) Concept of Use. Edition 1.0. Available at: https://www.icao.int/APAC/Documents/edocs/mlat_concept.pdf
17. Neven, W. H. L., Quilter, T. J., Weedon, R., Hogendoorn, R. A. (2004). Wide Area Multilateration Wide Area Multilateration Report on EATMP TRS 131/04 Version 1.1. ational Aerospace Laboratory NLR. Available at: https://www.eurocontrol.int/sites/default/files/2019-05/surveilllance-report-wide-area-multilateration-200508.pdf
18. 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
19. 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
20. Leonardi, M., Mathias, A., Galati, G. (2009). Two efficient localization algorithms for multilateration. International Journal of Microwave and Wireless Technologies, 1 (3), 223–229. doi: https://doi.org/10.1017/s1759078709000245
21. Yeromina, N., Kravchenko, I., Kobzev, I., Volk, M., Borysenko, V., Lukyanova, V. et. al. (2021). The Definition of the Paramethers of Superconducting Film for Production of Protection Equipment Against Electromagnetic Environmental Effects. International Journal of Emerging Technology and Advanced Engineering, 11 (7), 38–47. doi: https://doi.org/10.46338/ijetae0721_06
22. Monakov, A. A. (2018). Algoritm ocenki mestopolozheniya ob'ekta v aktivnyh sistemah mul'tilateracii. XXIV Mezhdunar. nauch.-tehn. konf. «Radiolokaciya, navigaciya, svyaz'». Vol. 3. Voronezh, 134–142.
23. Monakov, A. A. (2018). Modified Bancroft Algorithm for Multilateration Systems. Journal of the Russian Universities. Radioelectronics, 1, 50–55. doi: https://doi.org/10.32603/1993-8985-2018-21-1-50-55
24. Monakov, A. A. (2018). Localization algorithm for multilateration systems. Journal of the Russian Universities. Radioelectronics, 4, 38–46. doi: https://doi.org/10.32603/1993-8985-2018-21-4-38-46
25. Skrypnik, O., Shegidevich, A. (2019). Features of working areas of multilateration systems. The Aviation Herald, 1 (1), 10–16. Available at: https://bgaa.by/sites/default/files/inline-files/aviacionnyy-vestnik-zhurnal-no1-19_12.pdf
26. Schäfer, M., Lenders, V., Martinovic, I. (2013). Experimental Analysis of Attacks on Next Generation Air Traffic Communication. Lecture Notes in Computer Science, 253–271. doi: https://doi.org/10.1007/978-3-642-38980-1_16
27. Enclosure Kit for USRP B200/B210. Available at: https://www.ettus.com/all-products/USRP-B200-Enclosure/
28. Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., Brumley, D. (2012). GPS software attacks. Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12. doi: https://doi.org/10.1145/2382196.2382245
29. Saybel', A. G. (1958). Osnovy teorii tochnosti radiotehnicheskih metodov mestoopredeleniya. Moscow: Oborongiz, 56.
30. P-19MA. Available at: https://www.aerotechnica.ua/en/p-19ma-en.html

DOI: 10.15587/1729-4061.2021.240344

DEVISING A METHOD FOR IMPROVING CRYPTO RESISTANCE OF THE SYMMETRIC BLOCK CRYPTOSYSTEM RC5 USING NONLINEAR SHIFT FUNCTIONS (p. 17–29)

Andrii Sahun
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5151-9203

Vladyslav Khaidurov
Institute of Engineering Thermophysics of the Institute of Engineering Thermophysics of NAS of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4805-8880

Valeriy Lakhno
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9695-4543

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

Vitalii Chubaievskyi
Kyiv National University of Trade and Economics, Kyiv, Ukraine
National Police of Ukraine, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-8078-2652

Olena Kryvoruchko
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7661-9227

Alona Desiatko
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2284-3418

This paper analyzes ways to improve the cryptographic strength of the symmetric block cipher RC5. The task to enhance the stability of the classic RC5 cipher is explained by the fact that it is part of various open cryptographic libraries and is frequently used in practice. Several methods have been considered, applying which theoretically contributes to improving the stability of cryptographic transformations. It is found that unlike other alternatives (increasing the number of rounds, the length of the key, and the encryption block), the use of nonlinear shift functions does not increase the computational complexity of the RC5 algorithm. The study result has helped build an analytical model that was implemented in the form of the MATLAB (USA) software application. The software

interface provides the ability to manually change the encryption parameters of the RC5 crypto algorithm. The resulting upgrade of the RC5 crypto algorithm has been tested on different sets of input data during encryption and decryption. The resulting modification also does not lead to an increase in the calculation time but makes it possible to improve the resistance to hacking the encrypted data by several orders of magnitude (2^{10}), provided that differential analysis methods are used and the number of rounds is 14. For one of the nonlinear functions used, resistance to the differential cryptoanalysis used increased by 2^{12} times already in the eleventh round of encryption. The reliability of the improved cryptosystem has been confirmed by the absence of statistical correlation between the blocks of incoming messages and output blocks, the absence of collisions at which it is possible to obtain the same sequences of bits at the output with different messages at the input. The resulting algorithm could be applied in computer systems with low computing performance.

Keywords: nonlinear function, symmetric cryptosystem, shift function, RC5, block cipher, cryptoanalysis.

References

1. Recommendation X.200 (07/94). Available at: https://www.itu.int/rec/T-REC-X.200-199407-I
2. Understanding Layer 2 Encryption. Technical Whitepaper (2013). SafeNet. Available at: https://newberrygroup.com/wp-content/uploads/2017/10/understanding-layer-2-encryption-wp-en-v2-dec022013-web.pdf
3. Rivest, R. L. (1995). The RC5 encryption algorithm. Lecture Notes in Computer Science, 86–96. doi: https://doi.org/10.1007/3-540-60590-8_7
4. OpenSSL. Cryptography and SSL/TLS Toolkit. Available at: https://www.openssl.org/
5. RSA® BSAFE® Crypto-J JSAFE and JCE Software Module 6.2.4 Security Policy Level 1 (2020). Available at: http://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3172.pdf
6. Blozva, A., Kydyralina, L. M., Matus, Y. V., Osypova, T. Y., Sauanova, K., Brzhanov, R. T., Shalabayeva, M. (2021). IoT Devices Integration and Protection in available Infrastructure of a University computer Network. Journal of Theoretical and Applied Information Technology, 99 (8), 1820–1833. Available at: http://www.jatit.org/volumes/Vol99No8/11Vol99No8.pdf
7. Luzhetskyi, V., Horbenko, I. (2015). Metody shyfruvannia na osnovi perestanovky blokiv zminnoi dovzhyny. Zakhyst informatsiyi, 17 (2), 169–175.
8. Biryukov, A., Khovratovich, D. (2009). Related-Key Cryptanalysis of the Full AES-192 and AES-256. Lecture Notes in Computer Science, 1–18. doi: https://doi.org/10.1007/978-3-642-10366-7_1
9. Garfinkel, S. (1994). PGP: Pretty Good Privacy: Pretty Good Privacy. O'Reilly Media, 432.
10. Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). Lecture Notes in Computer Science, 191–204. doi: https://doi.org/10.1007/3-540-58108-1_24
11. Biryukov, A., Kushilevitz, E. (1998). Improved cryptanalysis of RC5. Advances in Cryptology – EUROCRYPT'98, 85–99. doi: https://doi.org/10.1007/bfb0054119
12. Furlong, M., Heys, H. (2005). A timing attack on the CIKS-1 block cipher. Canadian Conference on Electrical and Computer Engineering, 2005. doi: https://doi.org/10.1109/ccece.2005.1556916
13. Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. Lecture Notes in Computer Science, 386–397. doi: https://doi.org/10.1007/3-540-48285-7_33
14. Kaliski, B. S., Yin, Y. L. (1995). On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm. Lecture Notes in Computer Science, 171–184. doi: https://doi.org/10.1007/3-540-44750-4_14
15. Knudsen, L. R., Meier, W. (1997). Differential cryptanalysis of RC5. European Transactions on Telecommunications, 8 (5), 445–454. doi: https://doi.org/10.1002/ett.4460080503
16. Aggregate Statistics (2021). RC5-72 / Overall Project Stats. Available at: https://stats.distributed.net/projects.php?project_id=8
17. Panasenko, S. P. (2009). Algoritmy shifrovaniya. Spetsial'niy spravochnik. Sankt-Peterburg: BHV, 576.
18. Welchman, G. (1982). The Hut Six Story: Breaking the Enigma Codes. Harmondsworth: Allen Lane.

DOI: 10.15587/1729-4061.2021.241638

DEVELOPMENT OF A METHOD FOR ASSESSING THE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON THE LOTKA-VOLTERRA MODEL (p. 30–47)

Serhii Yevseiev
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-1647-6444

Serhii Pohasii
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-4540-3693

Stanislav Milevskyi
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-5087-7036

Oleksandr Milov
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0001-6135-2120

Yevgen Melenti
Yaroslav Mudryi National Law University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-2955-2469

Ivan Grod
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine
ORCID: https://orcid.org/0000-0002-0678-1456

Denis Berestov
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-3918-2978

Ruslan Fedorenko
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9433-5458

Oleg Kurchenko
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-3507-2392

The paper presents the results of the development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. Security models of cyber-physical systems are proposed: "predator-prey" taking into account the computing capabilities and focus of targeted cyberattacks, "predator-prey" taking into account the possible competition of attackers in relation to the "prey", "predator-prey" taking into account the relationships between "prey species" and "predator species", "predator-prey" taking into account the relationship between "prey species" and

"predator species". Based on the proposed approach, the coefficients of the Lotka-Volterra model α=0.39, β=0.32, γ=0.29, ϕ=0.27 were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the protection system, and also allow determining the financial and computing capabilities of the attacker based on the identified threats.

The proposed method for assessing the security of cyber-physical systems is based on the developed threat classifier, allows assessing the current security level and provides recommendations regarding the allocation of limited protection resources based on an expert assessment of known threats. This approach allows offline dynamic simulation, which makes it possible to timely determine attackers' capabilities and form preventive protection measures based on threat analysis. In the simulation, actual bases for assessing real threats and incidents in cyber-physical systems can be used, which allows an expert assessment of their impact on both individual security services and security components (cyber security, information security and security of information).

The presented simulation results do not contradict the graphical results of the classical Lotka-Volterra model, which indicates the adequacy of the proposed approach for assessing the security of cyber-physical systems.

Keywords: critical infrastructure, security system, threat classifier, Lotka-Volterra model, simulation method, security level.

References

1. IoT Security Maturity Model: Description and Intended Use (2018). Available at: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf
2. IoT Security Maturity Model: Practitioner's Guide (2019). Available at: https://iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf
3. Global'noe issledovanie tendentsiy informatsionnoy bezopasnosti na 2017. Available at: https://www.pwc.ru/ru/publications/gsiss-2017.html
4. Otchet Antifishinga o zaschischennosti sotrudnikov v 2020 godu (2021). Available at: https://antiphish.ru/tpost/88km7s0a01-otchyot-antifishinga-o-zaschischennosti
5. Gartner nazvala 10 glavnyh trendov v sfere kiberbezopasnosti v 2021 godu. Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8_%D0%B2_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#.2AGartner_.D0.BD.D0.B0.D0.B7.D0.B2.D0.B0.D0.BB.D0.B0_10_.D0.B3.D0.BB.D0.B0.D0.B2.D0.BD.D1.8B.D1.85_.D1.82.D1.80.D0.B5.D0.BD.D0.B4.D0.BE.D0.B2_.D0.B2_.D1.81.D1.84.D0.B5.D1.80.D0.B5_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.B2_2021_.D0.B3.D0.BE.D0.B4.D1.83
6. 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. doi: https://doi.org/10.15587/978-617-7319-31-2
7. Hryshchuk, R., Yevseiev, S. (2016). The synergetic approach for providing bank information security: the problem formulation. Ukrainian Scientific Journal of Information Security, 22 (1), 64–74. doi: https://doi.org/10.18372/2225-5036.22.10456
8. Hryshchuk, R. V. (2010). Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiu metodamy teoriy dyferentsialnykh ihor ta dyferentsialnykh peretvoren. Zhytomyr: Ruta, 280.
9. Hryshchuk, R. V., Danyk, Yu. H.; Danyk, Yu. H. (Ed.) (2016). Osnovy kibernetychnoi bezpeky. Zhytomyr: ZhNAEU, 636.
10. Petrov, O., Lahno, V. (2016). Povyshenie informatsionnoy bezopasnosti avtomatizirovannyh sitsem obrabotki dannyh na transporte. Information Technology in Selected Areas of Management. Krakow, 65–78.
11. Model' zrelosti bezopasnosti interneta veschey: tolchok k razvitiyu bezopasnyh sistem. Available at: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/
12. Trubetskov, D. I. (2011). Phenomenon of Lotka–Volterra mathematical model and similar models. Izvestiya VUZ. Applied Nonlinear Dynamics, 19 (2), 69–88. doi: https://doi.org/10.18500/0869-6632-2011-19-2-69-88
13. Bratus', A. S., Novozhilov, A. S., Platonov, A. P. Dinamicheskie sistemy i modeli biologii. Available at: https://avmaksimov.ucoz.ru/_ld/1/109_-Bratus_A-Novoz.pdf
14. Dormidontov, A. V., Mironova, L. V., Mironov, V. S. (2018). Possibility of the mathematical model of counteraction application to the assessment of transport infrastructure security level. Civil Aviation High Technologies, 21 (3), 67–77. doi: https://doi.org/10.26467/2079-0619-2018-21-3-67-77
15. Kononovich, I. V. (2014). Dynamics of the number of information security incidents. Informatics and Mathematical Methods in Simulation, 4 (1), 35–43. Available at: http://immm.opu.ua/files/archive/n1_v4_2014/n1_v4_2014.pdf
16. Kononovich, I., Mayevskiy, D., Podobniy, R. (2015). Models of system of the cibersecurity providing with delay of reaction on incidents. Informatics and Mathematical Methods in Simulation, 5 (4), 339–346. Available at: http://immm.opu.ua/files/archive/n4_v5_2015/n4_v5_2015.pdf
17. Lippert, K. J., Cloutier, R. (2021). Cyberspace: A Digital Ecosystem. Systems, 9 (3), 48. doi: https://doi.org/10.3390/systems9030048
18. Mazurczyk, W., Drobniak, S., Moore, S. (2016). Towards a Systematic View on Cybersecurity Ecology. Combatting Cybercrime and Cyberterrorism, 17–37. doi: https://doi.org/10.1007/978-3-319-38930-1_2
19. Gorman, S. P., Kulkarni, R. G., Schintler, L. A., Stough, R. R. A Predator Prey Approach to the Network Structure of Cyberspace. Available at: https://www.researchgate.net/publication/255679706_A_predator_prey_approach_to_the_network_structure_of_cyberspace
20. Crandall, J. R., Ensafi, R., Forrest, S., Ladau, J., Shebaro, B. (2008). The ecology of Malware. Proceedings of the 2008 Workshop on New Security Paradigms - NSPW '08. doi: https://doi.org/10.1145/1595676.1595692
21. Fink, G. A., Haack, J. N., McKinnon, A. D., Fulp, E. W. (2014). Defense on the Move: Ant-Based Cyber Defense. IEEE Security & Privacy, 12 (2), 36–43. doi: https://doi.org/10.1109/msp.2014.21
22. Wu, L., Wang, Y. (2011). Estimation the parameters of Lotka–Volterra model based on grey direct modelling method and its application. Expert Systems with Applications, 38 (6), 6412–6416. doi: https://doi.org/10.1016/j.eswa.2010.09.013
23. Diz-Pita, É., Otero-Espinar, M. V. (2021). Predator–Prey Models: A Review of Some Recent Advances. Mathematics, 9 (15), 1783. doi: https://doi.org/10.3390/math9151783
24. Minaev, V. A., Sychev, M. P., Vayts, E. V., Gracheva, Yu. V. (2016). Matematicheskaya model' «hischnik-zhertva» v sisteme informatsionnoy bezopasnosti. Informatsiya i bezopasnost', 19 (3), 397–400. Available at: https://elibrary.ru/item.asp?id=27186929

25. 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. doi: https://doi.org/10.21303/2461-4262.2021.001615
26. 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. doi: https://doi.org/10.15587/1729-4061.2021.233533
27. Ya dogonyayu, ty ubegaesh'. Chto takoe model' Lotki-Vol'terry i kak ona pomogaet biologam. Available at: https://nplus1.ru/material/2019/12/04/lotka-volterra-model
28. 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. doi: https://doi.org/10.15587/1729-4061.2020.205702
29. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Available at: https://www.iso.org/standard/54534.html
30. An Introduction to Factor Analysis of Information Risk (FAIR). Available at: https://www.yumpu.com/en/document/read/7271140/an-introduction-to-factor-analysis-of-information-risk-fair
31. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NISTIR. doi: https://doi.org/10.6028/nist.ir.8105
32. Lohachab, A., Lohachab, A., Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, 9, 100174. doi: https://doi.org/10.1016/j.iot.2020.100174
33. Ugrozy bezopasnosti yadra paketnoy seti 4G (2017). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
34. Uyazvimosti protokola Diameter v setyah 4G (2018). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
35. Godovoy otchet o podverzhennosti kiberatakam sotrudnikov kompaniy v Rossii i SNG. Available at: https://welcome.tiger-optics.ru/антифишинг-годовой-отчет?_ga=2.171180576.1827066423.1631692491-524698473.1631692491

DOI: 10.15587/1729-4061.2021.242849

DEVELOPMENT OF A HASH ALGORITHM BASED ON CELLULAR AUTOMATA AND CHAOS THEORY (p. 48–55)

Yuriy Dobrovolsky
Y. Fedkovich Chernivtsi National University, Chernovtsy, Ukraine
ORCID: https://orcid.org/0000-0002-1248-3615

Dmytro Hanzhelo
Y. Fedkovich Chernivtsi National University, Chernovtsy, Ukraine
ORCID: https://orcid.org/0000-0002-0836-4568

Mariia Hanzhelo
Y. Fedkovich Chernivtsi National University, Chernovtsy, Ukraine
ORCID: https://orcid.org/0000-0002-6312-740X

Denis Trembach
Y. Fedkovich Chernivtsi National University, Chernovtsy, Ukraine
ORCID: https://orcid.org/0000-0001-8095-4186

Georgy Prokhorov
Y. Fedkovich Chernivtsi National University, Chernovtsy, Ukraine
ORCID: https://orcid.org/0000-0001-7810-2785

Information security, reliability of data transfer are today an important component of the globalization of information technology. Therefore, the proposed work is devoted to highlighting the results of the design and development of a hacking-resistant algorithm to ensure the integrity of information transfer via digital technology and computer engineering. To solve such problems, cryptographic hashing functions are used. In particular, elements of deterministic Chaos were introduced into the developed cyclic hashing algorithm. The investigation analyzes in detail the strengths and weaknesses of known hashing algorithms. They are shown to have disadvantages. The main ones are a large number of matches (Hamming (x, y) and the presence of a weak avalanche effect, which lead to a significant decrease in the reliability of the algorithm for hacking. The designed hashing algorithm uses an iterative Merkley-Damgard structure, augmented by the input message to a length multiple of 512 bits. Processing in blocks of 128-bit uses cellular automata with mixed rules of 30, 105 and 90, 150 and takes into account the dependence of the generation of the initial vector on the incoming message. This allows half of the 10,000 pairs of arbitrary messages to have an inverse Hamming distance of 0 to 2. The proposed algorithm is four times slower than the well-known family of "secure hash algorithms." However, computation speed is not a critical requirement for a hash function. Decreasing the sensitivity to the avalanche effect allows the generation time to be approximately halved. Optimization of the algorithm, as well as its testing was carried out using new technologies of the Java programming language (version 15). Suggestions and recommendations for improving this approach to data hashing are given also.

Keywords: hashing algorithm, chaos theory, cellular automata, compression function, transformation function.

References

1. Toffoli, T., Margolis, N. (1987). Cellular Automata Machines. Cambridge: MIT Press. doi: http://doi.org/10.7551/mitpress/1763.001.0001
2. Jeon, J.-Ch. (2013). Analysis of hash functions and cellular automata based schemes. International Journal of Security and Applications, 7 (3), 303–316. Available at: http://article.nadiapub.com/IJSIA/vol7_no3/28.pdf
3. Paar, C., Pelzl, J. (2010). Understanding cryptography. Berlin-Heidelberg: Springer-Verlag. doi: https://doi.org/10.1007/978-3-642-04101-3
4. Pasyeka, M., Pasieka, N., Bestylnyy, M., Sheketa, V. (2019). Analysis of the use of the highly effective implementation of the sha-512 hash functions for the development of software systems. Cybersecurity: Education, Science, Technique, 3 (3), 112–121. doi: http://doi.org/10.28925/2663-4023.2019.3.112121
5. Kuznetsov, O. O., Horbenko, Yu. I., Onopriienko, V. V., Stelnyk, I. V., Mialkovskyi, D. V. (2019). The study of cryptographic hashing algorithms used in modern blockchain systems. Radiotekhnika, 3 (198), 54–74. doi: http://doi.org/10.30837/rt.2019.3.198.05
6. Pro zatverdzhennia Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy (2017). Postanova Pravlinnia Natsionalnoho banku Ukrainy No. 95. 28.09.2017. Available at: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
7. DSTU 7564: 2014 "Informatsionnye tekhnologii. Kriptograficheskaia zaschita informatsii. Funktsiia kheshirovaniia" (2014). Priniatii prikazom Ministerstva ekonomicheskogo razvitiia i torgovli Ukrainy No. 1431. 02.12.2014. Available at: https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-7564-2014.pdf

8. Tiwari, H., Asawa, K. (2012). A secure and efficient cryptographic hash function based on NewFORK-256. Egyptian Informatics Journal, 13(3), 199–208. doi: http://doi.org/10.1016/j.eij.2012.08.003
9. El Moumni, S., Fettach, M., & Tragha, A. (2019). High throughput implementation of SHA3 hash algorithm on field programmable gate array (FPGA). Microelectronics Journal, 93, 104615. doi: http://doi.org/10.1016/j.mejo.2019.104615
10. Hasheminejad, A., Rostami, M. J. (2019). A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. Optik, 184, 205–213. doi: http://doi.org/10.1016/j.ijleo.2019.03.065
11. Hao, W., Liming, Z., Haowei, M., Xingang, Z., Jinping, C. (2020). Perceptual Hash algorithm for GF-2 image using SIFT and SVD[J]. Bulletin of Surveying and Mapping, 8, 44–49. doi: https://doi.org/10.13474/j.cnki.11-2246.2020.0246
12. Xue, Wang, Liu, Lv, Wang, Zeng. (2019). An RISC-V Processor with Area-Efficient Memristor-Based In-Memory Computing for Hash Algorithm in Blockchain Applications. Micromachines, 10 (8), 541. doi: http://doi.org/10.3390/mi10080541
13. Li, Y. (2016). Collision analysis and improvement of a hash function based on chaotic tent map. Optik, 127 (10), 4484–4489. doi: http://doi.org/10.1016/j.ijleo.2016.01.176
14. Tao, F., Qian, W. (2019). Image hash authentication algorithm for orthogonal moments of fractional order chaotic scrambling coupling hyper-complex number. Measurement, 134, 866–873. doi: http://doi.org/10.1016/j.measurement.2018.11.079
15. Sodhi, G. K., Gaba, G. S., Kansal, L., Bakkali, M. E., Tubbal, F. E. (2019). Implementation of message authentication code using DNA-LCG key and a novel hash algorithm. International Journal of Electrical and Computer Engineering (IJECE), 9 (1), 352–358. doi: http://doi.org/10.11591/ijece.v9i1.pp352-358
16. Sumagita, M., Riadi, I. (2018). Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application. International Journal of Cyber-Security and Digital Forensics, 7 (4), 373. Available at: https://link.gale.com/apps/doc/A603050342/AONE?u=anon~26dfe3b7&sid=bookmark-AONE&xid=80bc955a
17. Safaei Mehrabani, Y. (2018). Synthesis of an Application Specific Instruction Set Processor (ASIP) for RIPEMD-160 Hash Algorithm. International Journal of Electronics Letters, 7 (2), 154–165. doi: http://doi.org/10.1080/21681724.2018.1477182
18. Mittelbach, A. Fischlin, M. (2021). The Theory of Hash Functions and Random Oracles. Springer International Publishing. doi: http://doi.org/10.1007/978-3-030-63287-8
19. Georgacopoulou, C. (1986). An investigation of hashing algorithms and their performance. Bradford.
20. Liu, Y. (2020). Modelling Urban Development with Geographical Information Systems and Cellular Automata. CRC Press. doi: http://doi.org/10.1201/9781420059908
21. Ch, J. (2013). Analysis of hash functions and cellular automata based schemes. International Journal of Security and Applications, 7 (3), 303–316. Available at: http://article.nadiapub.com/IJSIA/vol7_no3/28.pdf
22. Belfedhal, A. E., Faraoun, K. M. (2015). Building Secure and Fast Cryptographic Hash Functions Using Programmable Cellular Automata. Journal of Computing and Information Technology, 23 (4), 317–328. doi: http://doi.org/10.2498/cit.1002639
23. Martinez, G. (2013), A Note on Elementary Cellular Automata Classification. Journal of Cellular Automata, 8 (3-4), 233–259. Available at: https://arxiv.org/pdf/1306.5577.pdf
24. Vergili, I., Yucel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen n x n S-Boxes. Turkish Journal of Electrical Engineering and Computer Science, 9, 137–145. Available at: https://journals.tubitak.gov.tr/elektrik/issues/elk-01-9-2/elk-9-2-3-0008-1.pdf
25. Mironov, I. (2005). Hash functions: Theory, attacks, and applications. Available at: https://www.microsoft.com/en-us/research/publication/hash-functions-theory-attacks-and-applications/
26. Li, W., Packard, N. (1990). The Structure of the Elementary Cellular Automata Rule Space. Complex Systems, 4, 281–297.
27. Wolfram, S. (2002). A New Kind of Science. Champaign: Wolfram Media, 1192.
28. Wolfram, S. (2002). Cellular Automata and Complexity. Westview Press.
29. Pieprzyk, J. (1993). Design of hashing algorithms. Springer-Verlag.
30. Belfedhal, A. E., Faraoun, K. M. (2015). Building Secure and Fast Cryptographic Hash Functions Using Programmable Cellular Automata. Journal of Computing and Information Technology, 23 (4), 317–328. doi: http://doi.org/10.2498/cit.1002639
31. Ostapov, S. E. Yevseiev, S. P., Korol, O. H. (2013). Tekhnolohii zakhystu informatsii. Kharkiv: Vyd. KhNEU, 476. Available at: http://kist.ntu.edu.ua/textPhD/tzi.pdf

DOI: 10.15587/1729-4061.2021.242993

ANALYSIS OF NETWORK SECURITY ORGANIZATION BASED ON SD-WAN TECHNOLOGY (p. 56–69)

Gulzinat Ordabayeva
Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-9952-1620

Abdizhapar Saparbayev
Kainar Academy, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-4494-7568

Bibinur Kirgizbayeva
Kazakh National Agrarian Research University,
Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-9233-6131

Gulzat Dzhsupbekova
M. Auezov South Kazakhstan State University,
Shyment, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-1727-0966

Nazira Rakhymbek
M. Auezov South Kazakhstan State University,
Shyment, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-4229-2286

A Software-Defined Network (SDN) on a Wide Area Network (WAN) is a computer network that is controlled and created by software.

SD-WAN is an emerging research area that has received a lot of attention from industry and government. This technology offers tremendous opportunities to support the creation of consolidated data centers and secure networks. This is an innovation that allows the network to be monitored and programmed so that it can respond to network events caused by security breaches.

This solution provides network security, offers a single network management console, and provides complete control over the network architecture. Also controls security in the cloud software-defined infrastructure (SDI), such as dynamically changing the network configuration when forwarding packets, blocking, redirecting, changing Media Access Control (MAC) or Internet Protocol (IP) addresses, limiting the packet flow rate etc.

Using SD-WAN technology, it is possible to reduce the cost of dedicated bandwidth channels, achieve a high-quality Virtual Private Network (VPN), and the ability to automatically select a channel for certain channels.

The main advantages of SD-WAN are the management of an unlimited number of devices from a single center, reducing the cost of deploying branch infrastructure.

According to the results of the survey, 7 % of respondents use SD-WAN for security solutions, 14 % at the piloting stage.

As a result of the research, it was revealed that by 2024, to increase the flexibility and support of cloud applications, more than 60 % of SD-WAN customers will implement the SASE (Secure Access Service Edge) architecture, which is 30 % more than in 2020 and the main concept-application security and cloud functions.

Keywords: OpenFlow, Software defined wide area network (SD-WAN), architecture, DDoS attack, WAN network.

References

1. Laponina, O. R., Sizov, M. R. (2017). Laboratory bench for testing the integration capabilities of SDN networks and traditional networks. International Journal of Open Information Technologies, 5 (9).
2. Mukhizi, S., Mutkhanna, A. S., Kirichek, R. V, Kucheriavii, A. E. (2019). Issledovanie modelei balansirovki nagruzki v programmno-konfiguriruemykh setiakh. Elektrosviaz, 1, 23–29
3. Sallent, O., Perez-Romero, J., Ferrus, R., Agusti, R. (2017). On Radio Access Network Slicing from a Radio Resource Management Perspective. IEEE Wireless Communications, 24 (5), 166–174. doi: http://doi.org/10.1109/mwc.2017.1600220wc
4. OpenFlow Management and Configuration Protocol (OF-CONFIG 1.2). ONF TS-016. Available at: https://www.opennetworking.org/wp-content/uploads/2013/02/of-config-1.2.pdf Last accessed: 15.08.2021
5. Google's Inter-Datacenter WAN Using SDN and OpenFlow. Available at: https://opennetworking.org/sdn-resources/customer-case-studies/google/
6. OpenFlow. Available at: https://lvk.cs.msu.su/~sveta/SDN_OpenFlow_basics_lecture1_v2.pdf Last accessed: 15.08.2021
7. Tok, M. S., Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. Computers & Security, 109, 102394. doi: http://doi.org/10.1016/j.cose.2021.102394
8. Huang, X., Zeng, M., Xie, K. (2021). Intelligent traffic control for QoS optimization in hybrid SDNs. Computer Networks, 189, 107877. doi: http://doi.org/10.1016/j.comnet.2021.107877
9. Pamplin, S. (2021). SD-WAN revolutionises IoT and edge security. Network Security, 2021 (8), 14–15. doi: http://doi.org/10.1016/s1353-4858(21)00090-8
10. Tok, S., Demirci, M. (2021). An Investigation of Topology Poisoning Attacks in Software Defined Networks Through Exploiting Link Layer Discovery Protocol, 589–608. Uludağ University Journal of The Faculty of Engineering, . doi: http://doi.org/10.17482/uumfd.769939
11. Polat, H., Polat, O., Cetin, A. (2020). Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. Sustainability, 12 (3), 1035. doi: http://doi.org/10.3390/su12031035
12. Olivier, F., Carlos, G., Florent, N. (2015). New Security Architecture for IoT Network. Procedia Computer Science, 52, 1028–1033. doi: http://doi.org/10.1016/j.procs.2015.05.099
13. Khorsandroo, S., Sánchez, A. G., Tosun, A. S., Arco, J., Doriguzzi-Corin, R. (2021). Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. Computer Networks, 192, 107981. doi: http://doi.org/10.1016/j.comnet.2021.107981
14. Dayal, N., Srivastava, S. (2021). SD-WAN Flood Tracer: Tracking the entry points of DDoS attack flows in WAN. Computer Networks, 186, 107813. doi: http://doi.org/10.1016/j.comnet.2021.107813
15. Smelianskii, R. L. (2014). Tekhnologii SDN i NFV: novye vozmozhnosti dlia telekommunikatsii. Vestnik Sviazi, 1, 43–47. Available at: https://www.arccn.ru/media/1132/ Last accessed: 29.08.2021
16. Galich, S. V., Deogenov, M. S., Kartashevskii, V. G., Pasiuk, A. O., Semenov, E. S. (2016). Issledovanie proizvoditelnosti PKS-kontrollera OpenDaylight na setiakh raznykh masshtabov. Izvestiia IUFU. Tekhnicheskie nauki, 9, 121–133.
17. Fouladi, R. F., Ermiş, O., Anarim, E. (2020). A DDoS attack detection and defense scheme using time-series analysis for SDN. Journal of Information Security and Applications, 54, 102587. doi: http://doi.org/10.1016/j.jisa.2020.102587
18. Cui, Y., Qian, Q., Xing, H., Li, S. (2020). LNAD: Towards Lightweight Network Anomaly Detection in Software-Defined Networking. 2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 855–860. doi: http://doi.org/10.1109/hpcc-smartcity-dss50907.2020.00113
19. Pourvahab, M., Ekbatanifard, G. (2019). An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. IEEE Access, 7, 99573–99588. doi: http://doi.org/10.1109/access.2019.2930345
20. ONF TR-502: SDN Architecture (2014). Open Networking Foundation. Available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf Last accessed: 20.08.2021
21. Queiroz, W., Capretz, M. A. M., Dantas, M. (2019). An approach for SDN traffic monitoring based on big data techniques. Journal of Network and Computer Applications, 131, 28–39. doi: http://doi.org/10.1016/j.jnca.2019.01.016
22. Lee, S., Kim, J., Woo, S., Yoon, C., Scott-Hayward, S., Yegneswaran, V. et. al. (2020). A comprehensive security assessment framework for software-defined networks. Computers & Security, 91, 101720. doi: http://doi.org/10.1016/j.cose.2020.101720
23. Rana, D. S., Dhondiyal, S. A., Chamoli, S. K. (2019). Software Defined Networking (SDN) Challenges, issues and Solution. International Journal of Computer Sciences and Engineering, 7 (1), 884–889. doi: http://doi.org/10.26438/ijcse/v7i1.884889
24. Critical Capabilities for WAN Edge Infrastructure. Available at: https://www.gartner.com/doc/reprints?id=1-1XWDQO33&ct==191210&st=sb Last accessed: 24.08.2021
25. Guo, Z., Feng, W., Liu, S., Jiang, W., Xu, Y., Zhang, Z.-L. (2019). RetroFlow: Maintaining Control Resiliency and Flow Programmability for Software-Defined WANs. IEEE/ACM International Symposium on Quality of Service (IWQoS '19). Phoenix, New York. doi: http://doi.org/10.1145/3326285.3329036
26. Malakhov, S. V., Tarasov, V.N. (2015). Teoreticheskoe i eksperimentalnoe issledovanie zaderzhki v programmnogo-kofiguriruemykh setiakh. Infokommunikatsionnye tekhnologii, 4, 409–413.
27. Maltsev, A. (2018). Postroenie zaschischennoi i adaptiruemoi seti SD-WAN. Available at: https://www.osp.ru/lan/2018/04/13054564 Last accessed: 29.08.2021
28. Tanha, M. (2019). Resilient Controller Placement Problems in Software Defined Wide-Area Networks. University of Victoria, 130.

29. Kodavanty, V., Sen, S., Kamsetty, S., Arumugam, P. V. (2019). Pat. No. US 2019/0207844 A1 USA. Determining routing decisions in a software – defined wide area network. Pub. Date: 04.07.2019.
30. Golani, K., Goswami, K., Bhatt, K., Park, Y. (2018). Fault Tolerant Traffic Engineering in Software-defined WAN. 2018 IEEE Symposium on Computers and Communications (ISCC). doi: http://doi.org/10.1109/iscc.2018.8538606
31. Sarychev, D. (2021). Kak obespechit bezopasnost programmno-opredeliaemykh setei (SD-WAN). Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/Secure-SD-WAN Last accessed: 05.09.2021
32. SD-WAN Market Recorded 39 Percent Growth for 1H 2021, According to Dell'Oro Group. Available at: https://www.delloro.com/news/sd-wan-market-recorded-39-percent-growth-for-1h-2021/ Last accessed: 05.09.2021
33. Galiev, A. (2021). Kak «Kazteleport» v razy sokratil izderzhki na vydelennye kanaly s pomoschiu SD-WAN. Available at: https://profit.kz/articles/14657/Kak-AO-Kazteleport-v-razi-sokratil-izderzhki-na-videlennie-kanali-s-pomoschu-SD-WAN/ Last accessed: 05.09.2021
34. BI Group modernizirovala set s pomoschiu resheniia SD-WAN ot Fortinet (2021). Available at: https://profit.kz/articles/14700/BI-Group-modernizirovala-set-s-pomoschu-resheniya-SD-WAN-ot-Fortinet/ Last accessed: 05.09.2021
35. Razbor rynka SD-WAN: kakie suschestvuiut resheniia i komu oni nuzhny (2019). Available at: https://safe.cnews.ru/articles/2019-11-06_razbor_rynka_sdwan_kakie_sushchestvuyut Last accessed: 06.09.2021
36. Rukovodstvo po sredstvu zaschity SD-WAN dlia rukovoditelei v sfere setevykh tekhnologii. Available at: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ru_ru/eBook-The-Network-Leaders-Guide-to-Secure-SD-WAN.pdf Last accessed: 06.09.2021

DOI: 10.15587/1729-4061.2021.242357

ANALYZING THE CODE STRUCTURES OF MULTIDIMENSIONAL SIGNALS FOR A CONTINUOUS INFORMATION TRANSMISSION CHANNEL (p. 70–81)

Liubov Berkman
State University of Telecommunications, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-6772-1596

Olexandr Turovsky
National Aviation University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4961-0876

Liudmyla Kyrpach
State University of Telecommunications, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-9210-922X

Oksana Varfolomeeva
State University of Telecommunications, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2294-4518

Volodymyr Dmytrenko
State University of Telecommunications, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4540-7248

Oleksii Pokotylo
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-1136-5123

One of the directions to improve the efficiency of modern telecommunication systems is the transition to the use of multidimensional signals for continuous channels of information transmission. As a result of studies carried out in recent years, it has been established that it is possible to ensure high quality of information transmission in continuous channels by combining demodulation and decoding operations into a single procedure that involves the construction of a code construct for a multidimensional signal.

This paper considers issues related to estimating the possibility to improve the efficiency of continuous information transmission channel by changing the signal distance of the code structure.

It has been established that the code structures of such types as a hierarchical code construct of signals, a hierarchical code construct of signals with Euclidean metric, a reversible code construct of signals, a reversible code construct of signals with Euclidean metric have the potential, when used, to increase the speed of information transmission along a continuous channel. With a signal distance reduced by 10 percent or larger, it could increase by two times or faster.

The estimation of the effect of reducing a signal distance on the efficiency of certain types of code structures was carried out. It has been established that the hierarchical reversible code construct, compared to the hierarchical code construct, provides a win of up to two or more times in the speed of information transmission with a halved signal distance. Implementing the modulation procedure has no fundamental difficulties, on the condition that for each code of the code construct the encoding procedure is known when using binary codes. The results reported here make it possible to build an acceptably complex demodulation procedure according to the specified types of code structures.

Keywords: continuous transmission channel, multidimensional signal, signal code construct, signal distance.

References

1. Hemming, R. V. (1998). Teoriya kodirovaniya i teoriya informatsii. Moscow: «Radio i svyaz'», 176.
2. Kasami, T. (1978). Teoriya kodirovaniya. Moscow: Mir, 576.
3. Morelos-Saragosa, R. (2006). Iskusstvo pomekhoustoychivogo kodirovaniya. Metody, algoritmy, primenenie. Moscow: Tekhnosfera, 320.
4. Polushin, P. A. (2007). Izbytochnost' signalov v radiosvyazi. Moscow: Radiotekhnika, 256.
5. Varbanets, S. P. (2013). Teoriya kodirovaniya. Odessa: ONU, 43.
6. Seletkov, V. L. (2010). Obschaya struktura lineynoy sistemy pomekhoustoychivogo kodirovaniya. Visti vyshchykh uchbovykh zakladiv. Radioelektronika, 53 (12), 24–31. doi: https://doi.org/10.20535/s0021347010120034
7. Di Renzo, M., Haas, H., Ghrayeb, A., Sugiura, S., Hanzo, L. (2014). Spatial Modulation for Generalized MIMO: Challenges, Opportunities, and Implementation. Proceedings of the IEEE, 102 (1), 56–103. doi: https://doi.org/10.1109/jproc.2013.2287851
8. Wong, C. W., Wong, T. F., Shea, J. M. (2011). Secret-Sharing LDPC Codes for the BPSK-Constrained Gaussian Wiretap Channel. IEEE Transactions on Information Forensics and Security, 6 (3), 551–564. doi: https://doi.org/10.1109/tifs.2011.2139208
9. Micheli, G., Neri, A. (2020). New Lower Bounds for Permutation Codes Using Linear Block Codes. IEEE Transactions on Information Theory, 66 (7), 4019–4025. doi: https://doi.org/10.1109/tit.2019.2957354
10. Chen, P., Shi, L., Fang, Y., Cai, G., Wang, L., Chen, G. (2018). A Coded DCSK Modulation System Over Rayleigh Fading Channels. IEEE Transactions on Communications, 66 (9), 3930–3942. doi: https://doi.org/10.1109/tcomm.2018.2827032

11. Jochym-O'Connor, T., Yoder, T. J. (2021). Four-dimensional toric code with non-Clifford transversal gates. Physical Review Research, 3 (1). doi: https://doi.org/10.1103/physrevresearch.3.013118
12. Freudenberger, J., Ghaboussi, F., Shavgulidze, S. (2013). New Coding Techniques for Codes over Gaussian Integers. IEEE Transactions on Communications, 61 (8), 3114–3124. doi: https://doi.org/10.1109/tcomm.2013.061913.120742
13. Park, J., Kim, I., Song, H.-Y. (2017). Interpretation of polar codes with Plotkin construction based on Gaussian approximation. 2017 Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA). doi: https://doi.org/10.1109/iwsda.2017.8097085
14. Gnatyuk, S., Kinzeryavyy, V., Iavich, M., Prysiazhnyi, D., Yubuzova, K. (2018). High-performance reliable block encryption algorithms secured against linear and differential cryptanalytic attacks. Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshop. Kyiv, 2104, 657–668. Available at: http://ceur-ws.org/Vol-2104/paper_220.pdf
15. Fogel, A., Koeyer, I., Secrist, C., Sipherd, A., Hafen, T., Fricke, M. (2021). The Revised Relational Coding System. doi: https://doi.org/10.13140/RG.2.2.27439.46245
16. Batenkov, K. A. (2014). Continuous channel modeling in shape of some space transformation operators. SPIIRAS Proceedings, 1 (32), 171–198. doi: https://doi.org/10.15622/sp.32.11
17. Boiko, J. M. (2014). Improvements Encoding Energy Benefit in Protected Telecommunication Data Transmission Channels. Communications, 2 (1), 7. doi: https://doi.org/10.11648/j.com.20140201.12
18. Boiko, J., Pyatin, I., Eromenko, O., Stepanov, M. (2020). Method of the adaptive decoding of self-orthogonal codes in telecommunication. Indonesian Journal of Electrical Engineering and Computer Science, 19 (3), 1287. doi: https://doi.org/10.11591/ijeecs.v19.i3.pp1287-1296
19. Gorcin, A. (2013). Multidimensional Signal Analysis for Wireless Communications Systems. Graduate Theses and Dissertations. Available at: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=5877&context=etd
20. Joo, H.-S., Kim, K.-H., No, J.-S., Shin, D.-J. (2017). New PTS Schemes for PAPR Reduction of OFDM Signals Without Side Information. IEEE Transactions on Broadcasting, 63 (3), 562–570. doi: https://doi.org/10.1109/tbc.2017.2711141
21. Shamasundar, B., Chockalingam, A. (2020). Constellation Design for Media-Based Modulation Using Block Codes and Squaring Construction. IEEE Journal on Selected Areas in Communications, 38 (9), 2156–2167. doi: https://doi.org/10.1109/jsac.2020.3000828
22. Vameghestahbanati, M., Marsland, I., Gohary, R. H., Yanikomeroglu, H. (2020). Hypercube-Based Multidimensional Constellation Design for Uplink SCMA Systems. 2020 IEEE International Conference on Communications Workshops (ICC Workshops). doi: https://doi.org/10.1109/iccworkshops49005.2020.9145403
23. Bloh, E. L., Zyablov, V. V. (1976). Obobschennye kaskadnye kody. Moscow: Svyaz', 240.
24. Bleyhut, R. (1986). Teoriya i praktika kodov, kontroliruyuschih oshibki. Moscow: Mir, 576.
25. Levina, B. R. (1979). Statisticheskaya teoriya svyazi i ee prakticheskie prilozheniya. Moscow: Svyaz', 376.
26. Klark, D., Keyn, D. (1987). Kodirovanie s ispravleniem oshibok v sistemah tsifrovoy svyazi. Moscow: Radio i svyaz', 392.
27. Danielsen, L. E. (2012). On the Classification of Hermitian Self-Dual Additive Codes Over GF(9). IEEE Transactions on Information Theory, 58 (8), 5500–5511. doi: https://doi.org/10.1109/tit.2012.2196255
28. Norden, A. P. (2016). Elementarnoe vvedenie v geometriyu Lobachevskogo. Moscow: Lenan, 220.
29. Kokseter, G., Mozer, Dzh. (1980). Porozhdayuschie elementy i opredelyayuschie sootnosheniya diskretnyh grupp. Moscow: Nauka, 240.
30. Zhurakovskyi, B. Iu. (2019). Research of the use of new antijamming codes for channels with elimination. Visnyk Derzhavnoho universytetu informatsiyno-komunikatsiynykh tekhnolohiy, 10 (2), 93–96. Available at: http://nbuv.gov.ua/UJRN/vduikt_2012_10_2_18
31. Banket, V. L., Prokopov, S. D. (2000). Metod opredeleniya svobodnogo rasstoyaniya invariantnyh signal'no-kodovyh konstruktsiy. Pratsi UNDIRT, 1 (21), 39–44. Available at: https://biblio.suitt.edu.ua/bitstream/handle/123456789/1711/Банкет%2с%20Прокопов.pdf?sequence=1&isAllowed=y
32. Polak, S. C. (2019). Semidefinite Programming Bounds for Constant-Weight Codes. IEEE Transactions on Information Theory, 65 (1), 28–38. doi: https://doi.org/10.1109/tit.2018.2854800
33. Zhang, H., Zhang, X., Ge, G. (2012). Optimal Ternary Constant-Weight Codes With Weight 4 and Distance 5. IEEE Transactions on Information Theory, 58 (5), 2706–2718. doi: https://doi.org/10.1109/tit.2011.2179412
34. Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., Odarchenko, R. (2020). 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
35. 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
36. 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

DOI: 10.15587/1729-4061.2021.242795

DEVELOPMENT OF THE CLASSIFIER BASED ON A MULTILAYER PERCEPTRON USING GENETIC ALGORITHM AND CART DECISION TREE (p. 82–90)

Liudmyla Dobrovska
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4055-6834

Olena Nosovets
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-1288-3528

The problem of developing universal classifiers of biomedical data, in particular those that characterize the presence of a large number of parameters, inaccuracies and uncertainty, is urgent. Many studies are aimed at developing methods for analyzing these data, among them there are methods based on a neural network (NN) in the form of a multilayer perceptron (MP) using GA.

The question of the application of evolutionary algorithms (EA) for setting up and learning the neural network is considered.

Theories of neural networks, genetic algorithms (GA) and decision trees intersect and penetrate each other, new developed neural networks and their applications constantly appear.

An example of a problem that is solved using EA algorithms is considered. Its goal is to develop and research a classifier for the diagnosis of breast cancer, obtained by combining the capabilities of the multilayer perceptron using the genetic algorithm (GA) and the CART decision tree.

The possibility of improving the classifiers of biomedical data in the form of NN based on GA by applying the process of appropriate preparation of biomedical data using the CART decision tree has been established.

The obtained results of the study indicate that these classifiers show the highest efficiency on the set of learning and with the minimum reduction of Decision Trees; increasing the number of contractions usually degrades the simulation result. On two datasets on the test set, the simulation accuracy was ≈83–87 %.

The experiments carried out have confirmed the effectiveness of the proposed method for the synthesis of neural networks and make it possible to recommend it for practical use in processing data sets for further diagnostics, prediction, or pattern recognition.

Keywords: neural network, multilayer perceptron using a genetic algorithm, CART decision tree.

References

1. Dobrovska, L., Dobrovska, I. (2015). Teoriia ta praktyka neironnykh merezh. Kyiv: NTUU «KPI», 395.
2. Dobrovska, L., Dobrovska, I. (2017). Design of the universal classif2ier as a RBF network based on the CART solution tree. Eastern-European Journal of Enterprise Technologies, 4 (4 (88)), 63–71. doi: http://doi.org/10.15587/1729-4061.2017.108976
3. Farizawani, A., Puteh, M., Marina, Y., Rivaie, A. (2020). A review of artificial neural network learning rule based on multiple variant of conjugate gradient approaches. Journal of Physics: Conference Series, 1529, 022040. doi: http://doi.org/10.1088/1742-6596/1529/2/022040
4. Yao, X. (1993). A review of evolutionary artificial neural networks. International Journal of Intelligent Systems, 8 (4), 539–567. doi: http://doi.org/10.1002/int.4550080406
5. Dutta, P., Kumar, A. (2018). Modeling and Optimization of a Liquid Flow Process using an Artificial Neural Network-Based Flower Pollination Algorithm. Journal of Intelligent Systems, 29 (1), 787–798. doi: http://doi.org/10.1515/jisys-2018-0206
6. Venkatesan, D., Kannan, K., Saravanan, R. (2008). A genetic algorithm-based artificial neural network model for the optimization of machining processes. Neural Computing and Applications, 18 (2), 135–140. doi: http://doi.org/10.1007/s00521-007-0166-y
7. Castillo, P., Arenas, M., Castillo-Valdivieso, J., Merelo, J., Prieto, A., 7. Romero, G. (2003). Artificial Neural Networks Design using Evolutionary Algorithms. Advances In Soft Computing. London: Springer, 43–52. doi: http://doi.org/10.1007/978-1-4471-3744-3_5
8. Ding, S., Xu, L., Su, C.,Zhu, H. (2010). Using Genetic Algorithms to Optimize Artificial Neural Networks. Journal Of Convergence Information Technology, 5 (8), 54–62. doi: http://doi.org/10.4156/jcit.vol5.issue8.6
9. Jaafra, Y., Luc Laurent, J., Deruyver, A., Saber Naceur, M. (2019). Reinforcement learning for neural architecture search: A review. Image and Vision Computing, 89, 57–66. doi: http://doi.org/10.1016/j.imavis.2019.06.005
10. Baker, B., Gupta, O., Naik, N., Raskar, R. (2021). Designing neural network architectures using reinforcement learning. Int. Conf. Learn. Represent. San Juan. Available at: https://arxiv.org/abs/1611.02167
11. Miikkulainen, R., Liang, J., Meyerson, E., Rawal, A., Fink, D., Francon, O. et al. (2019). Evolving Deep Neural Networks. Artificial Intelligence In The Age Of Neural Networks And Brain Computing. Elsevier, 293–312. doi: http://doi.org/10.1016/b978-0-12-815480-9.00015-3
12. Real, E., Aggarwal, A., Huang, Y., Le, Q. V. (2019). Regularized Evolution for Image Classifier Architecture Search. Proceedings of the AAAI Conference on Artificial Intelligence, 33, 4780–4789. doi: http://doi.org/10.1609/aaai.v33i01.33014780
13. Matteucci, M. (2006). ELeaRNT: Evolutionary Learning of Rich Neural Network Topologies. Computer Science. doi: http://doi.org/10.21236/ada456062
14. Luo, R., Tian, F., Qin, T., Chen, E., Liu, T. (2018). Neural Architecture Optimization. Conference And Workshop On Neural Information Processing Systems, 7827–7838.
15. Sariev, E., Germano, G. (2019). Bayesian regularized artificial neural networks for the estimation of the probability of default. Quantitative Finance, 20 (2), 311–328. doi: http://doi.org/10.1080/14697688.2019.1633014
16. Kim, H. B., Jung, S. H., Kim, T. G., Park, K. H. (1996). Fast learning method for back-propagation neural network by evolutionary adaptation of learning rates. Neurocomputing, 11 (1), 101–106. doi: http://doi.org/10.1016/0925-2312(96)00009-4
17. Michel, D., Navarro, D. (2021). Genetic Operators and Their Impact on the Training of Deep Neural Networks. Metaheuristics In Machine Learning: Theory And Applications. Cham: Springer, 97–124. doi: http://doi.org/10.1007/978-3-030-70542-8_5
18. UCI Machine Learning Repository: Data Sets. Available at: http://archive.ics.uci.edu/ml/datasets.php Last accessed: 22.09.2021

DOI: 10.15587/1729-4061.2021.243153

DESIGN AND IMPLEMENTATION OF THE DISTRIBUTED DOSIMETRIC SYSTEM BASED ON THE PRINCIPLES OF IOT (p. 91–100)

Vitalii Terokhin
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID:https://orcid.org/0000-0001-7653-4488

Mykola Stervoyedov
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0003-0136-6437

Oleg Ridozub
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-9385-5627

This paper describes the architecture and components of the distributed information and management system for collecting, processing, storing, and distributing data on a radiometric and dosimetric experiment using the principle of the Internet of Things. Data exchange between elements in the system, as well as the analysis of the received information, involves active application of the ThingSpeak cloud service. Two-way communication with the cloud with a 15-second loop has been implemented. Data are processed in the MATLAB (America) environment, integrated into the cloud. The developed hardware and software solutions demonstrate an increased accuracy of measurements due to the use of promising cadmium telluride (CdZnTe) detectors, modern microcontroller and micro communication technology, and a new algorithm for correcting the dependence of detector sensitivity on radiation energy. Measurement with correction by the method of average charge pulse amplitude is carried out in the energy range from 60 keV to 3 MeV. The resolution of the spectrometric channel is 6.5 % at the peak of 662 keV of full absorption from the reference source, Cesium (Cs – 137).

The module for a laboratory sensor network, designed to measure the dose of ionizing radiation, has a built-in spectrometric analog-digital converter, microcontroller control, and a communication unit. Constructing the diagrams demonstrates the operation of the interrupt handler in the form of a series of events occurring when requests arrive from a Web server. The peculiarity of the system is the absence of intermediate devices that make it possible to establish a connection with the Internet.

The developed system, equipment, algorithms, and programs are used for experimental studies of radiation and nuclear-physical processes. Elements of the system were useful for remote laboratory work by students.

Keywords: information management system, UML diagrams, Internet of Things, CdZnTe radiation detector.

References

1. Batura, T. V., Murzin, F. A., Semich, D. F. (2014). Cloud technologies: basic models, applications, concepts and development tendencies. Programmnye produkty i sistemy, 3 (107), 64–72. doi: http://doi.org/10.15827/0236-235x.107.064-072
2. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29 (7), 1645–1660. doi: http://doi.org/10.1016/j.future.2013.01.010
3. Ridozub, O., Terokhin, V., Stervoyedov, N., Fomin, S. (2019). Sensor node for wireless radiation monitoring network. Bulletin of V.N. Karazin Kharkiv National University, Series «Mathematical Modeling. Information Technology. Automated Control Systems», 44, 88–93. doi: http://doi.org/10.26565/2304-6201-2019-44-09
4. Finance, G. (2012). What actor should I use for scheduled use cases? Available at: http://www.umlchannel.com/en/uml/item/24-use-case-actor-system-timer/24-use-case-actor-system-timer Last accessed: 10.10.2020
5. Kutnii, V. E., Rybka, A. V., Davydov, L. N. et. al. (2021). Detektory ioniziruiuschikh izluchenii na osnove tellurida kadmiia – tsinka. Kharkiv: Tipografiia Madrid, 352.
6. Terokhin, V., Styervoyeodov, M., Ridozub, O., Fomin, S. (2020). Intelektualniy vuzol of sensory framing of radio monitoring. Materials of the conference CMNT – 2020. Kharkiv, 49–51.
7. Adame, T., Bel, A., Bellalta, B., Barcelo, J., Oliver, M. (2014). IEEE 802.11AH: the WiFi approach for M2M communications. IEEE Wireless Communications, 21 (6), 144–152. doi: http://doi.org/10.1109/mwc.2014.7000982
8. Somov, A. S. (2019). Sbor i vizualizatsiia dannykh s pomoschiu platformy interneta veschei Libelium Waspmote. Moscow: Skolkovskii institut nauki i tekhnologii, 30.
9. Kumar, S., Tiwari, P., Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6 (1). doi: http://doi.org/10.1186/s40537-019-0268-2
10. MATLAB – MathWorks – MATLAB & Simulink. Available at: https://www.mathworks.com/products/matlab.html
11. Hryhorieva, L. I., Tomili, Yu. A., Rozhkov, I. M. (2008). Ionizuiuche vyprominiuvannia ta yoho vplyv na liudynu. Mykolaiv: MDHU im. Petra Mohyly, 208.
12. Owens, A. (2019). Semiconductor Radiation Detectors. CRC Press, 494. doi: http://doi.org/10.1201/b22251
13. Zakharchenko, A. A., Nakonechnii, D. V., Shliakhov, I. N., Rybka, A. V., Kutnii, V. E., Khazhmuradov, M. A. (2019). Simulation of energy dependence of CdTe (CdZnTe) gamma-radiation detectors sensitivity. Tekhnologiia i Innovatsii, 44, 245–247.

АНОТАЦІЇ

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2021.242935

РОЗРОБКА МЕТОДУ ВИЗНАЧЕННЯ КООРДИНАТ ПОВІТРЯНИХ ОБ'ЄКТІВ РАДІОЛОКАЦІЙНИМИ СТАНЦІЯМИ З ДОДАТКОВИМ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ МУЛЬТИЛАТЕРАЦІЇ (с. 6–16)

Г. В. Худов, П. Є. Минко, Ш. М. Іхсанов, О. С. Дьяконов, О. В. Коваленко, Ю. С. Соломоненко, Є. М. Дроб, О. М. Харун, С. Д. Черкашин, О. В. Сердюк

Проведені експериментальні дослідження щодо підтвердження порушень в роботі приймачів ADS-B. Експериментальні дослідження порушень в роботі приймачів ADS-B проведені з використанням приймача FlightAware Piaware. Наведені приклади порушень в роботі приймачів ADS-B. Встановлено, що експериментально виявлені порушення в роботі приймачів ADS-B можуть привести до зниження точності визначення координат повітряних об'єктів при сумісному застосуванні радіолокаційної станції та технології мультилатерації.

Розроблено метод визначення координат повітряного об'єкта радіолокаційною станцією з додатковим використанням технології мультилатерації. Розроблений метод передбачає наступні етапи: введення вихідних даних, розрахунок відстаней між пунктами прийому та повітряним об'єктом, розрахунок вектору нев'язок, розрахунок матриці часткових похідних з урахуванням оцінок координат повітряного об'єкту на попередній ітерації, обчислення поправки, розрахунок уточнених координат повітряного об'єкта. На відміну від відомих, удосконалений метод визначення координат повітряного об'єкту радіолокаційною станцією додатково використовує технологію мультилатерації.

Проведено оцінювання точності визначення координат повітряних об'єктів радіолокаційною станцією з додатковим використанням технології мультилатерації. Встановлено, що додаткове використання технології мультилатерації дозволить забезпечити зменшення похибки визначення координат повітряного об'єкту в середньому від 1,58 до 2,39 разів у порівнянні з використанням лише автономної радіолокаційної станції.

Ключові слова: радіолокаційна станція, технологія мультилатерації, повітряний об'єкт, метод визначення, середньоквадратична помилка.

DOI: 10.15587/1729-4061.2021.240344

РОЗРОБКА МЕТОДУ ПІДВИЩЕННЯ КРИПТОСТІЙКОСТІ СИМЕТРИЧНОЇ БЛОКОВОЇ КРИПТОСИСТЕМИ RC5 З ВИКОРИСТАННЯМ НЕЛІНІЙНИХ ФУНКЦІЙ ЗСУВУ (с. 17–29)

А. В. Сагун, В. В. Хайдуров, В. А. Лахно, І. Р. Опірський, В. І. Чубаєвський, О. В. Криворучко, А. М. Десятко

В роботі проаналізовані шляхи підвищення криптостійкості симетричного блочного шифру RC5. Проблема підвищення стійкості класичного шифру RC5 пояснюється тим, що він є частиною різних відкритих криптографічних бібліотек та частим його використанням на практиці. Розглянуто декілька методів, використання яких теоретично сприяє покращення стійкості криптографічних перетворень. Встановлено, що на відміну від інших альтернатив (збільшення числа раундів, довжини ключа та блоку шифрування), використання нелінійних функцій зсуву не підвищує обчислювальну складність алгоритму RC5. В результаті проведених досліджень було отримано аналітичну модель, яка була реалізована у вигляді програмного додатку Matlab (США). В інтерфейсі програмного продукту передбачена можливість ручної зміни параметрів шифрування крипто алгоритму RC5. Отримана модернізація криптоалгоритму RC5 протестована на різних наборах вхідних даних для шифрування та дешифрування графічних і. Отримана модифікація також не призводить до збільшення часу обчислень, але дозволяє збільшити стійкість до зламу зашифрованих даних до декількох порядків (2^{10}) за умови використання методів диференційного аналізу, і кількості раундів=14. Для однієї з використаних нелінійних функцій стійкість до використаного диференційного криптоаналізу збільшилася в 2^{12} рази вже на одинадцятому раунді шифрування. В якості нелінійних зсувних функцій було використано п'ять функцій. Надійність вдосконаленої криптосистеми підтверджується відсутністю статистичної кореляції між блоками вхідних повідомлень та вихідними блоками відсутністю колізій, при яких можна отримати однакові послідовності бітів на виході при різних повідомленнях на вході. Отриманий алгоритм може бути застосований в комп'ютерних системах з невисокою обчислювальною продуктивністю.

Ключові слова: нелінійна функція, симетрична криптосистема, функція зсуву, RC5, блочний шифр, криптоаналіз.

DOI: 10.15587/1729-4061.2021.241638

РОЗРОБКА МЕТОДУ ОЦІНКИ БЕЗПЕКИ КІБЕРФІЗІЧЕСКІХ СИСТЕМ НА ОСНОВІ МОДЕЛІ ЛОТКИ-ВОЛЬТЕРРИ (с. 30–47)

С. П. Євсеєв, С. С. Погасій, С. В. Мілевський, О. В. Мілов, Є. О. Меленті, О. В. Шмато, І. М. Грод, Д. С. Берестов, Р. М. Федоренко, О. А. Курченко

У статті відображені результати розробки методу оцінки безпеки кіберфізичних систем на основі моделі Лотки-Вольтери. Запропоновано моделі безпеки кіберфізичних систем: "хижак-жертва" з урахуванням обчислювальних можливостей і спрямованості цільових кібератак, "хижак-жертва" з урахуванням можливої конкуренції зловмисників по відношенню до "жертви", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків". На основі запропонованого підходу отримані коефіцієнти моделі Лотки-Вольтери α=0,39, β=0,32, γ=0,29, ϕ=0,27, які враховують синергізм і гибридность сучасних загроз, фінансування на формування та вдосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника по виявленим загрозам.

Пропонований метод оцінки безпеки кіберфізичних систем ґрунтується на базі розробленого класифікатора загроз, дозволяє оцінити поточний рівень безпеки і в динаміці формувати рекомендації щодо розподілу обмежених ресурсів захисту на основі експертної оцінки відомих загроз. Такий підхід дозволяє проводити динамічне моделювання в оф-лайн режимі, що дозволяє на основі аналізу загроз своєчасно визначити можливості зловмисників і сформувати превентивні заходи захисту. При імітаційному моделюванні можуть використовуватися фактичні бази оцінки реальних загроз і інцидентів на кіберфізичні системи, що дозволяє провести експертну оцінку їх впливу як на окремі послуги безпеки, так і на складові безпеки (кібербезпека, інформаційну безпеку та безпеку інформації).

Представлені результати імітаційного моделювання не суперечать графічним результатами класичної моделі Лотки-Вольтер, що свідчить про адекватність запропонованого підходу з оцінки безпеки кіберфізичних систем.

Ключові слова: критична інфраструктура, система безпеки, класифікатор загроз, модель Лотки-Вольтери, методологія моделювання, рівень безпеки.

DOI: 10.15587/1729-4061.2021.242849

РОЗРОБКА АЛГОРИТМУ ХЕШ-ФУНКЦІЇ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ І ТЕОРІЇ ХАОСА (с. 48–55)

Ю. Г. Добровольський, Д. В. Ганжелло, М. Г. Ганжелло, Д. В. Трембач, Г. В. Прохоров

Захист інформації, надійність передачі даних, є сьогодні важливою складовою глобалізації інформаційних технологій. Тому пропонована робота присвячена висвітленню результатів проектування та розроблення стійкого до злому алгоритму, призначеного для забезпечення цілісності інформації, що передається і приймається засобами цифрової техніки і комп'ютерної інженерії. Для вирішення таких завдань використовуються криптографічні функції хешування. Зокрема, у розроблений циклічний алгоритм хешування внесено елементи детермінованого Хаосу. У дослідженні детально проаналізовані сильні і слабкі сторони відомих алгоритмів хешування. Показано, що вони мають певні недоліки. Основні з них, це велика кількість не збігів (відстаней Хемінга (Hamming (x, y) і наявність лавинного ефекту, які призводять до істотного зниження надійності та стійкості алгоритму до злому. Спроектований алгоритм хешування використовує ітеративну структуру Мерклі-Дамгарда, доповнену вхідним повідомленням до довжини кратної 512 біт. Додаткова обробка блоками по 128-біт використовує клітинні автомати зі змішаними правилами 30, 105 і 90, 150 і враховує залежність від вхідного повідомлення генерації початкового вектора. Це дозволяє половині з 10 тисяч пар довільних повідомлень мати відстань Хеммінга від 0 до 2. Запропонований алгоритм працює в чотири рази повільніше відомого сімейства «Безпечний хеш-алгоритм». Однак швидкість обчислення не є критичним вимогам, які ставляться до хеш-функції. Зменшення чутливості до лавинному ефекту дозволяє зменшити час генерації хеш-функції приблизно вдвічі. Оптимізація алгоритму, а також його тестування проводилося з використанням нових технологій мови програмування Java (версія 15). Наведено припущення і рекомендації щодо вдосконалення даного підходу до хешування даних.

Ключові слова: алгоритм хешування, теорія хаосу, клітинні автомати, функція стиснення, функція трансформації.

DOI: 10.15587/1729-4061.2021.242993

АНАЛІЗ ОРГАНІЗАЦІЇ БЕЗПЕКИ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ SD-WAN (с. 56–69)

Gulzinat Ordabayeva, Abdizhapar Saparbayev, Bibinur Kirgizbayeva, Gulzat Dzhsupbekova, Nazira Rakhymbek

Програмно-визначувана мережа (Software-Defined Network – SDN) у глобальній мережі (Wide Area Network – WAN) – це комп'ютерна мережа, яка керується та створюється програмним забезпеченням.

SD-WAN – область дослідження, що розвивається, яка привернула велику увагу промисловості та уряду. Ця технологія містить величезні можливості підтримки створення консолідованих центрів обробки даних та безпечних мереж. Це нововведення, яке дозволяє контролювати та програмувати мережу таким чином, щоб вона могла реагувати до мережевих подій, спричинених порушеннями безпеки.

Це рішення забезпечує безпеку мереж, пропонує єдину консоль для управління мережею та надає повний контроль над архітектурою мережі. Також контролює безпеку у хмарному середовищі програмно-визначуваної інфраструктури (Software Defined Infrastructure, SDI), як динамічна зміна конфігурації мережі при пересиланні пакетів, блокуванні, перенаправленні, змін Media Access Control (MAC) або Internet Protocol (IP) адреси, обмеження швидкості потоку пакетів і т.д.

Використовуючи технологію SD-WAN, можна скоротити витрати на виділені канали з пропускною здатністю, досягти якісної віртуальної приватної мережі (Virtual Private Network, VPN), можливість автоматичного вибору каналу по певних каналах.

Основні переваги SD-WAN – керування необмеженою кількістю пристроїв із єдиного центру, скорочення витрат на розгортання інфраструктури філій.

За результатами опитування 7 % респондентів використовують SD-WAN для вирішення безпеки, 14 % на стадії пілотування.

В результаті досліджень було виявлено, що до 2024 року для підвищення гнучкості та підтримки хмарних додатків понад 60 % клієнтів SD-WAN впровадять архітектуру SASE (прикордонний сервіс безпечного доступу – Secure Access Service Edge), яка на 30 % більша за 2020 і основна Концепція – безпека додатків та хмарних функцій.

Ключові слова: OpenFlow, Software defined wide area network (SD-WAN), архітектура, DDoS-атака, WAN-мережа.

DOI: 10.15587/1729-4061.2021.242357

АНАЛІЗ КОДОВИХ КОНСТРУКЦІЙ БАГАТОВИМІРНИХ СИГНАЛІВ ДЛЯ БЕЗПЕРЕРВНОГО КАНАЛУ ПЕРЕДАЧІ ІНФОРМАЦІЇ (с. 70–81)

Л. Н. Беркман, О. Л. Туровський, О. Г. Варфоломієва, Л. А. Кирпач, В. В. Дмитренко, О. І. Покотило

Одним з напрямків підвищення ефективності роботи сучасних телекомунікаційних систем є перехід до використання багатовимірних сигналі для безперервних каналів передачі інформації. В результаті проведених в останні роки досліджень встановлено, що за-

безпечити високу якість передачі інформації в безперервних каналах можна методом об'єднання операцій демодуляції і декодування в єдину процедуру, яка передбачає створення кодової конструкції багатовимірного сигналу.

Безпосередньо розглянуті питання оцінки можливості зміною сигнальної відстані кодової конструкції, підвищити ефективність роботи безперервного каналу передачі інформації.

Встановлено, що кодові конструкції типу: ієрархічна кодова конструкція сигналів; ієрархічна кодова конструкція сигналів з евклідовою метрикою; перестановочна кодова конструкції сигналів; перестановочна кодова конструкції сигналів з евклідовою метрикою, при їх застосуванні мають потенційну можливість до підвищення швидкості передачі інформації через безперервний канал. Вона, при зменшені сигнальної відстані від 10 і більше відсотків, може досягати до двох і більше разів.

Здійснено оцінку впливу зменшення сигнальної відстані на ефективність роботи окремих типів кодових конструкцій. Встановлено, що ієрархічна переставна кодова конструкція в порівнянні з ієрархічної кодовою конструкцією, забезпечує виграш до двох і більше разів в швидкості передачі інформації при зменшені сигнальної відстані в два рази. Реалізація процедури модуляції не має принципових труднощів при умові, що для кожного коду кодової конструкції відома процедура кодування при застосування двійкових кодів. Отримані результати дозволяють побудувати достатньо прийняту по складності процедуру демодуляції відповідно визначених типів кодових конструкцій.

Ключові слова: безперервний канал передачі, багатовимірний сигнал, кодова конструкція сигналу, сигнальна відстань.

DOI: 10.15587/1729-4061.2021.242795

РОЗРОБКА КЛАСИФІКАТОРА НА ОСНОВІ БАГАТОШАРОВОГО ПЕРСЕПТРОНУ З ВИКОРИСТАННЯМ ГЕНЕТИЧНОГО АЛГОРИТМУ ТА ДЕРЕВА РОЗВ'ЯЗКІВ CART (с. 82–90)

Л. М. Добровська, О. К. Носовець

Проблема розробки універсальних класифікаторів біомедичних даних, зокрема тих, які характеризують наявність великої кількості параметрів, неточність та невизначеність, є актуальною. Багато досліджень спрямовано на розробку методів аналізу цих даних, серед них є методи на основі нейронної мережі (НМ) у вигляді багатошарового персептрону (БП) з використанням ГА.

Розглядається питання застосування еволюційних алгоритмів (ЕА) для налаштування і навчання НМ.

Теорії НМ, генетичних алгоритмів (ГА) та Дерев рішень перетинаються та проникають одна в одну, постійно з'являються нові розвинені НМ та їх застосунки.

Розглянуто приклад завдання, яке вирішується за допомогою ЕА. Його мета – розробити та дослідити класифікатор для діагностики захворювань на рак молочної залози, одержаний шляхом поєднання можливостей багатошарового персептрону з використанням генетичного алгоритму (ГА) та Дерева розв'язків CART.

Встановлено можливість вдосконалення класифікаторів біомедичних даних у вигляді НМ на основі ГА шляхом застосування процесу відповідної підготовки біомедичних даних із використанням Дерева розв'язків CART.

Отримані результати дослідження свідчать про те, що ці класифікатори показують найвищу ефективність на множині тестування та при мінімальному скороченні Дерева розв'язків; збільшення кількості скорочень зазвичай погіршує результат моделювання. На двох наборах даних на множині тестування точність моделювання склала ≈83–87 %.

Проведені експерименти підтвердили ефективність запропонованого методу синтезу НМ і дозволяють рекомендувати його для використання на практиці при обробці наборів даних для подальшої діагностики, прогнозування або розпізнавання образів.

Ключові слова: нейронна мережа, багатошаровий персептрон з використанням генетичного алгоритму, дерево розв'язків CART.

DOI: 10.15587/1729-4061.2021.243153

РОЗРОБКА ТА РЕАЛІЗАЦІЯ РОЗПОДІЛЕНОЇ ДОЗИМЕТРИЧНОЇ СИСТЕМИ НА ОСНОВІ ПРИНЦИПІВ IOT (с. 82–90)

В. Л. Терьохін, Н. Г. Стервоєдов, О. В. Рідозуб

Описано архітектуру та складові елементи розподіленої інформаційно–управляючої системи для збору, обробки, зберігання та розповсюдження даних радіометричного і дозиметричного експерименту за принципом Інтернету речей. Обмін даними між елементами в системі і аналіз отриманої інформації здійснюється з активним застосуванням хмарного сервісу ThingSpeak. Реалізовано двосторонній обмін даними зі хмарою з циклом 15 секунд. Обробка даних проводиться в середовищі MATLAB (Америка), який є інтегрований в хмару. Розроблені апаратні і програмні рішення мають підвищену точність вимірювань за рахунок застосування перспективних телурид кадмію (CdZnTe) детекторів, сучасної мікроконтролерної і микрокомунікаційної техніки і нового алгоритму корекції залежності чутливості детектору від енергії випромінювання. Вимірювання з корекцією методом середньої амплітуди імпульсів заряду здійснюється в діапазоні енергій від 60 keV до 3 MeV. Роздільна здатність спектрометричного каналу складає 6,5 % на піку 662 keV повного поглинання від еталонного джерела Цезій (Cs – 137).

Модуль лабораторної сенсорної мережі, який розроблено для вимірювання дози іонізуючого випромінювання, має вбудований спектрометричний аналого-цифровий перетворювач, мікроконтролерне керування і комунікаційний блок. Створення діаграм демонструє роботу обробника переривань у вигляді ряду подій, що відбуваються при надходженні запитів з веб-серверу. Особливістю системи є відсутність проміжних пристроїв, що дозволяють встановлювати підключення с мережею Інтернет.

Розроблені система, апаратура, алгоритми і програми використовується для експериментальних досліджень радіаційних і ядерно-фізичних процесів. Елементи системи виявилися корисними для дистанційного виконання лабораторних робіт студентами.

Ключові слова: інформаційно-управляюча система, UML діаграми, Інтернет речей, CdZnTe детектор випромінювання.