ABSTRACT AND REFERENCES
INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2022.266990

INVESTIGATING THE IMPACT OF NETWORK TOPOLOGIES ON THE IOT-BASED WSN IN SMART HOME MONITORING SYSTEM (p. 6–14)

Shayma W. Nourildean
University of Technology, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-9452-4344

Yousra A. Mohammed
University of Technology, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-6432-0754

May T. Abdulhadi
Baghdad, Iraq
ORCID: https://orcid.org/0000-0003-2411-067X

The object of this research is to present IoT WSN-based smart home monitoring system, which allows users to monitor and manage all of their appliances and home equipment via the Internet using established protocols. IoT is described as the connection of equipment and appliances to the Internet in order to monitor, report, and perform certain tasks. Wireless Sensor Networks (WSN) are considered as a key component in the IoT model's implementation. This research presented the IoT WSN platform using Riverbed Modeler Simulation Program in order to examine the network performance for different Wireless Sensor topologies (Star, Tree and Mesh). This platform consists of a number of scenarios with a number of sensors in each scenario. Each sensor is represented by the ZigBee end device, which sensed and collected data about the smart home and sent the collected data to the controller, which is represented by the ZigBee coordinator. The controller sends the data to the server to be monitored by the users through any gateway (Wi-Fi) after logging in using a specific application with three routing topologies on the controller. The results showed that IoT WSN tree topology is the best topology if the throughput is considered for improvement at the expense of data dropped with acceptable delay. Star topology improves the network performance in terms of data dropped and throughput when the number of sensors was increased. Mesh topology achieved the smallest data dropped with low throughput. Due to their features, these results were effective because they indicated that the selection of suitable routing topology played an important role in improving the degradation of IoT WSN performance due to the interference of Wi-Fi and ZigBee network since they utilized the same frequency band (2.4 GHz).

Keywords: IoT, Riverbed, smart, Star, Tree, Mesh, ZigBee, throughput, delay, Wi-Fi.

References

1. Lavanya, P., Muthu Mayil, K. (2019). IoT - Based Wireless Sensors for Agriculture Monitoring. International Journal of Recent Technology and Engineering, 8 (2S4), 177–181. doi: https://doi.org/10.35940/ijrte.b1033.0782s419
2. Ma, L., Li, Z., Zheng, M. (2019). A Research on IoT Based Smart Home. 2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). doi: https://doi.org/10.1109/icmtma.2019.00033
3. Karray, F., Triki, M., Wassim Jmal, M., Abid, M., M. Obeid, A. (2018). WiRoTip: an IoT-based Wireless Sensor Network for Water Pipeline Monitoring. International Journal of Electrical and Computer Engineering (IJECE), 8 (5), 3250. doi: https://doi.org/10.11591/ijece.v8i5.pp3250-3258
4. Jothikumar, C., Ramana, K., Chakravarthy, V. D., Singh, S., Ra, I. H. (2021). An Efficient Routing Approach to Maximize the Lifetime of IoT-Based Wireless Sensor Networks in 5G and Beyond. Mobile Information Systems, 2021, 1–11. doi: https://doi.org/10.1155/2021/9160516
5. Agarwal, A., Singh, M., Singh, S., Singh, A., Singh, A. (2022). Wireless Sensor Network Based Internet of Things for Precision Agriculture. SSRN Electronic Journal. doi: https://doi.org/10.2139/ssrn.4031983
6. Haseeb, K., Ud Din, I., Almogren, A., Islam, N. (2020). An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture. Sensors, 20 (7), 2081. doi: https://doi.org/10.3390/s20072081
7. Roopa, G. K., Shetty, R. (2019). IOT & Wireless Sensor Networks in Precision Agriculture. International Journal of Science and Research (IJSR), 8 (1), 401–404.
8. Mendoza-Cano, O., Aquino-Santos, R., López-de la Cruz, J., Edwards, R. M., Khouakhi, A., Pattison, I. et al. (2021). Experiments of an IoT-based wireless sensor network for flood monitoring in Colima, Mexico. Journal of Hydroinformatics, 23 (3), 385–401. doi: https://doi.org/10.2166/hydro.2021.126
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: https://doi.org/10.1186/s40537-019-0268-2
10. Gabhane, J. P., Thakare, S., Craig, M. (2017). Smart Homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions. International Research Journal of Engineering and Technology (IRJET), 04 (05), 1965–1969.
11. Davidovic, B., Labus, A. (2016). A smart home system based on sensor technology. Facta Universitatis - Series: Electronics and Energetics, 29 (3), 451–460. doi: https://doi.org/10.2298/fuee1603451d
12. Sisavath, C., Yu, L. (2021). Design and implementation of security system for smart home based on IOT technology. Procedia Computer Science, 183, 4–13. doi: https://doi.org/10.1016/j.procs.2021.02.023
13. Salim, A., Ismail, A., Osamy, W., Khedr, A. M. (2021). Compressive sensing based secure data aggregation scheme for IoT based WSN applications. PLOS ONE, 16 (12), e0260634. doi: https://doi.org/10.1371/journal.pone.0260634
14. El-Sayed, H. H., Bayatti, H. A. (2021). Improving Network Lifetime in WSN for the application of IoT. Applied Mathematics & Information Sciences, 15 (4), 453–458. doi: https://doi.org/10.18576/amis/150407
15. Sharma, S., Verma, V. K. (2022). An Integrated Exploration on Internet of Things and Wireless Sensor Networks. Wireless Personal Communications, 124 (3), 2735–2770. doi: https://doi.org/10.1007/s11277-022-09487-3
16. Anandhavalli, A., Bhuvaneswari, A. (2018). IoT Based Wireless Sensor Networks – A Survey. International Journal of Computer Trends and Technology, 65 (1), 21–28. doi: https://doi.org/10.14445/22312803/ijctt-v65p104
17. Shafiq, M., Ashraf, H., Ullah, A., Masud, M., Azeem, M., Z. Jhanjhi, N., Humayun, M. (2021). Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN. Computers, Materials & Continua, 67 (3), 3505–3521. doi: https://doi.org/10.32604/cmc.2021.015533
18. Saleh, M. (2020). WSNs and IoT Their Challenges and applications for Healthcare and Agriculture: A Survey. Iraqi Journal for Electrical

and Electronic Engineering. The 3rd Scientific Conference of Electrical and Electronic Engineering Researches (SCEEER), 37–43. doi: https://doi.org/10.37917/ijeee.sceeer.3rd.6

19. Ghayvat, H., Mukhopadhyay, S., Gui, X., Suryadevara, N. (2015). WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors, 15 (5), 10350–10379. doi: https://doi.org/10.3390/s150510350
20. Coboi, A. E., Nguyen, V., Nguyen, M., Duy, N. T. (2021). An Analysis of ZigBee Technologies for Data Routing in Wireless Sensor Networks. ICSES Transactions on Computer Networks and Communications (ITCNC).
21. Ali, H., Chew, W. Y., Khan, F., Weller, S. R. (2017). Design and implementation of an IoT assisted real-time ZigBee mesh WSN based AMR system for deployment in smart cities. 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). doi: https://doi.org/10.1109/sege.2017.8052810
22. Vançin, S., Erdem, E. (2015). Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard. International Journal of Computer Networks and Applications (IJCNA), 2 (3), 135–143.
23. Nourildean, S. W., Hassib, M. D., Mohammed, Y. A. (2022). Internet of things based wireless sensor network: a review. Indonesian Journal of Electrical Engineering and Computer Science, 27 (1), 246. doi: https://doi.org/10.11591/ijeecs.v27.i1.pp246-261
24. Ameen, S. Y., Nourildean, S. W. (2013). Coordinator and router investigation in IEEE802.15.14 ZigBee wireless sensor network. 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE). doi: https://doi.org/10.1109/iceccpce.2013.6998748
25. Sharma, R., Vashisht, V., Singh, U. (2020). Modelling and simulation frameworks for wireless sensor networks: a comparative study. IET Wireless Sensor Systems, 10 (5), 181–197. doi: https://doi.org/10.1049/iet-wss.2020.0046
26. Wail Nourildean, S., Mohammed Salih, A. (2022). Internet of Things based Wireless Sensor Network - WiFi Coexistence in Medical Applications. 2022 8th International Engineering Conference on Sustainable Technology and Development (IEC). doi: https://doi.org/10.1109/iec54822.2022.9807574
27. Nourildean, S. W., Jasim, S. I., Abdulhadi, M. T., Jaber, M. M. (2022). Point coordination mechanism based mobile ad hoc network investigation against jammers. Eastern-European Journal of Enterprise Technologies, 5 (9 (119)), 45–53. doi: https://doi.org/10.15587/1729-4061.2022.265779

DOI: 10.15587/1729-4061.2022.268368

DEVELOPMENT OF A METHOD FOR ENSURING CONFIDENTIALITY AND AUTHENTICITY IN WIRELESS CHANNELS (p. 15–27)

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

Roman Korolev
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-7948-5914

Mykhailo Koval
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2130-2548

Khazail Rzayev
Azerbaijan Technical University, Baku, Azerbaijan
ORCID: https://orcid.org/0000-0001-9272-4302

Oleksandr Voitko
Institute of Troops (Forces) Support and Information Technologies The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4610-4476

Olena Akhiiezer
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: https://orcid.org/0000-0002-7087-9749

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

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

Elnur Baghirov
Fogito Tech LLC, Baku, Azerbaijan
ORCID: https://orcid.org/0000-0002-8312-5751

Musa Mammadov
Cybernet LLC, Baku, Azerbaijan
ORCID: https://orcid.org/0000-0002-2517-6577

The object of the research is the development of a method for ensuring the authenticity and integrity of data in wireless channels based on post-quantum cryptosystems. The development of modern digital technologies ensures the transition to smart technologies and the formation of Next Generation Networks. The formation of smart technologies, as a rule, uses wireless communication channel standards IEEE 802.11X, IEEE 802.15.4, IEEE 802.16, which use only authentication protocols and privacy mechanisms, which are formed on symmetric algorithms. In the conditions of the post-quantum period (the advent of a full-scale quantum computer), the stability of such algorithms is questioned. Such systems, as a rule, are formed on the basis of the synthesis of socio-cyber-physical systems and cloud technologies, which simplifies the conduct of Advanced Persistent Threat attacks, both on the internal circuit of execution systems and on external control systems. The creation of multi-circuit information protection systems allows for an objective assessment of the current state of the system as a whole and the formation of preventive measures to counter cyber threats. The proposed method of providing basic security services: confidentiality, integrity and authenticity based on crypto-code constructions takes into account the level of secrecy of information transmitted over wireless channels and/or stored in databases of socio-cyber-physical systems. The use of post-quantum algorithms – McEliece/Niederreiter crypto-code constructions on elliptic/modified elliptic/lossy/Low-density parity-check code provides the necessary level of stability in the post-quantum cryptoperiod (crypto-stability at the level of 10^{25}–10^{35} group operations), speed and probability of information (P_{err} not lower than 10^{-9}–10^{-12}). The proposed method of information exchange using wireless communication channels ensures their practical implementation on resource-limited devices (creating of CCC on the GF field (2^4–2^6).

Keywords: crypto-code constructions of McEliece and Niederreiter, smart technologies, security concept, multi-contour protection systems.

References

1. Merz, H., Hansemann, T., Hübner, C. (2009). Building Automation: Communication systems with EIB/KNX, LON und BACnet. Springer, 282. doi: https://doi.org/10.1007/978-3-540-88829-1
2. KNX Technical Manual. 2CKA001473B8668. Busch-Presence detector KNX / Busch-Watchdog Sky KNX (2017). Busch-Jaeger Elektro GmbH, 198. Available at: https://library.e.abb.com/public/ddedcbf7ab704705affb179ca91e0fa2/2CKA001473B8668_Prasenzmelder_6131_03_ABB_EN.pdf
3. Technical documentation on KNX devices (2006). ABB.
4. KNX Handbook Version 1.1 Revision 1 (2004). Konnex Association.
5. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual. Busch-Watchdog Sky KNX (2016). Busch-Jaeger Elektro GmbH, 648.
6. ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products (2016). ABB, 86. Available at: https://library.e.abb.com/public/d26bd890d3ef476fbc3a59a2fdca6116/Webinar%20ABB%20i-bus%20KNX%20-%20KNX%20Basics%20and%20Products.pdf
7. Manual for KNX Planning (2017). Siemens Switzerland Ltd, 100.
8. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation (2010). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 116.
9. Guide for Cybersecurity Event Recovery. NIST. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-184.pdf
10. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf
11. Guide to LTE Security. NIST Special Publication (SP) 800-187. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-187/draft/documents/sp800_187_draft.pdf
12. Kottapalli, N. (2011). Diameter and LTE Evolved Packet System. Corporate Headquarters, 10. Available at: http://go.radisys.com/rs/radisys/images/paper-lte-diameter-eps.pdf
13. Ventura, H. (2002). Diameter - Next generation's AAA protocol. Institutionen för Systemteknik, 66. Available at: https://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf
14. Vinay Kumar, S. B., Harihar, M. N. (2012). Diameter-Based Protocol in the IP Multimedia Subsystem. International Journal of Soft Computing and Engineering (IJSCE), 1 (6), 266–269. Available at: https://www.ijsce.org/wp-content/uploads/papers/v1i6/F0320121611.pdf
15. Qanbari, S., Mahdizadeh, S., Rahimzadeh, R., Behinaein, N., Dustdar, S. (2016). Diameter of Things (DoT): A Protocol for Real-Time Telemetry of IoT Applications. Lecture Notes in Computer Science, 207–222. doi: https://doi.org/10.1007/978-3-319-43177-2_14
16. Tschofenig, H. (2019). Diameter: new generation AAA protocol – design, practice, and applications. John Wiley & Sons, Ltd. doi: https://doi.org/10.1002/9781118875889
17. Ugrozy bezopasnosti yadra paketnoy seti 4G. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
18. Uyazvimosti protokola Diameter v setyakh 4G. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
19. Ashibani, Y., Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. Computers & Security, 68, 81–97. doi: https://doi.org/10.1016/j.cose.2017.04.005
20. Graja, I., Kallel, S., Guermouche, N., Cheikhrouhou, S., Hadj Kacem, A. (2018). A comprehensive survey on modeling of cyber-physical systems. Concurrency and Computation: Practice and Experience, 32 (15). doi: https://doi.org/10.1002/cpe.4850
21. Minahil, Ayub, M. F., Mahmood, K., Kumari, S., Sangaiah, A. K. (2021). Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. Digital Communications and Networks, 7 (2), 235–244. doi: https://doi.org/10.1016/j.dcan.2020.06.003
22. Inam ul haq, Wang, J., Zhu, Y., Maqbool, S. (2021). An efficient hash-based authenticated key agreement scheme for multi-server architecture resilient to key compromise impersonation. Digital Communications and Networks, 7 (1), 140–150. doi: https://doi.org/10.1016/j.dcan.2020.05.001
23. Darem, A., Alhashmi, A. A., Jemal, H. A. (2022). Cybersecurity Threats and Countermeasures of the Smart Home. Ecosystem. International Journal of Computer Science and Network Security, 22 (3), 303–311. doi: https://doi.org/10.22937/IJCSNS.2022.22.3.39
24. Munilla, J., Burmester, M., Barco, R. (2021). An enhanced symmetric-key based 5G-AKA protocol. Computer Networks, 198, 108373. doi: https://doi.org/10.1016/j.comnet.2021.108373
25. Generic authentication architecture (GAA); generic bootstrapping architecture (GBA). TS 33.220. 3GPP. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2280
26. HMAC: Keyed-Hashing for Message Authentication. Available at: https://www.ietf.org/rfc/rfc2104.txt
27. 3G Security; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation. TR 35.909. 3GPP. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2405
28. 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. doi: https://doi.org/10.15587/1729-4061.2018.150903
29. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18–26. doi: https://doi.org/10.15587/1729-4061.2016.75250
30. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multifactor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175
31. 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: http://doi.org/10.15587/978-617-7319-31-2
32. Bleykhut, R. (1986). Teoriya i praktika kodov, kontroliruyuschikh oshibki. Moscow: Mir, 576.
33. Naim, M., Ali-Pacha, H., Ali-Pacha, A., Hadj-Said, N. (2021). Lengthening the period of a Linear Feedback Shift Register. Journal of Engineering Technology and Applied Sciences. doi: https://doi.org/10.30931/jetas.778792

DOI: 10.15587/1729-4061.2022.269030

APPLICATION OF THE PRINCIPLE OF INFORMATION OBJECTS DESCRIPTION FORMALIZATION FOR THE DESIGN OF INFORMATION PROTECTION SYSTEMS (p. 28–37)

Vladimir Lutsenko
National Technical University «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7632-1730

Dmytro Progonov
National Technical University «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-1124-1497

The development of information independence of the State requires the introduction of the latest technologies for analyzing, storing, processing, and transmitting information. The focus of this work is improving information security systems with limited access, in particular the development of new methods of designing such systems, which are characterized by minimal influence of the subject-designer on the design process. The object of the study is the methodology and means of designing systems for restricting and controlling physical access, as well as access to information at objects of information activity and information and telecommunication systems of Ukraine.

To exclude the influence of the subject of the designer, it is necessary to improve the design process itself. In this paper, the possibility of creating an automatic design system based on the representation of protection objects in the form of objects of a common structure has been mathematically proved. Such a structure combines both telecommunication objects and objects of information activity. Changes in the legislative, regulatory, and technical bases of information protection necessary for the implementation of the proposed system have been determined, in particular, granting the State Communications Committee of Ukraine new powers that ensure the balance of interests of the customer of protection systems and executors. The possibility of formalizing the representation of data on arbitrary objects of protection is shown. This representation makes it possible to create open library semantic databases with incomplete data on the object of protection.

A theoretical base has been built that makes it possible to determine the correspondence between the set of threats to the information security of the object and the unambiguous corresponding list of countermeasures. At the same time, information protection projects are distinguished by evolution and uniformity of choice of a set of means of protection to any threats to objects of arbitrary complexity.

Keywords: databases with incomplete information, automatic designer of information security systems, object of protection of the general structure.

References

1. Wu, T., Zhang, R., Dai, P., Liu, S. (2018). Research on information system architecture of standardized organization based on data repository. 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). doi: https://doi.org/10.1109/itoec.2018.8740482
2. Grishina, N. V. (2007). Organizaciya kompleksnoy sistemy zashchity informacii. Moscow: Gelios ARV, 256.
3. Zakaria, K. N., Othman, S. H., Zainal, A. (2019). Review of Cybersecurity Audit Management and Execution Approaches. 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS). doi: https://doi.org/10.1109/icriis48246.2019.9073641
4. Karagiannis, S., Manso, M., Magkos, E., Ribeiro, L. L., Campos, L. (2021). Automated and On-Demand Cybersecurity Certification. 2021 IEEE International Conference on Cyber Security and Resilience (CSR). doi: https://doi.org/10.1109/csr51186.2021.9527958
5. Turner, R. C. (2022). Process Mining for Asymmetric Cybersecurity Audit. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). doi: https://doi.org/10.1109/csr54599.2022.9850298
6. Progonov, D., Yarysh, M. (2022). Analyzing the accuracy of detecting steganograms formed by adaptive steganographic methods when using artificial neural networks. Eastern-European Journal of Enterprise Technologies, 1 (9 (115)), 45–55. doi: https://doi.org/10.15587/1729-4061.2022.251350
7. Isazadeh, A., Karimpour, H. (2011). Formal Specification of Control Software Systems Using Behavioral Views. International Journal of Advanced Research in Computer Science, 2 (1), 62–67. Available at: http://www.ijarcs.info/index.php/Ijarcs/article/view/246/236
8. Mierlo, S. V., Vangheluwe, H. (2018). Introduction to statecharts modeling, simulation, testing, and deployment. 2018 Winter Simulation Conference (WSC). doi: https://doi.org/10.1109/wsc.2018.8632384
9. Hoffmann, J. L. C., Horstmann, L. P., Wagner, M., Vieira, F., de Lucena, M. M., Frohlich, A. A. (2022). Using Formal Methods to Specify Data-Driven Cyber-Physical Systems. 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE). doi: https://doi.org/10.1109/isie51582.2022.9831686
10. Eckhart, M., Ekelhart, A., Weippl, E. (2022). Automated Security Risk Identification Using AutomationML-Based Engineering Data. IEEE Transactions on Dependable and Secure Computing, 19 (3), 1655–1672. doi: https://doi.org/10.1109/tdsc.2020.3033150
11. Cha, S.-C., Yeh, K.-H. (2018). An ISO/IEC 15408-2 Compliant Security Auditing System with Blockchain Technology. 2018 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2018.8433185
12. Buddy System. Available at: https://www.securitylab.ru/software/234275.php
13. Budko, M., Vasylenko, V., Korolenko, M., Butochnov, O. (2002). Systema zakhystu informatsiyi vid NSD „RUBIZh". Praktychni aspekty realizatsiyi kontseptsii tsentralizovanoho upravlinnia bezpekoiu korporatyvnoi systemy. Pravove, normatyvne ta metrolohichne zabezpechennia system zakhystu informatsiyi v Ukraini, 4, 154–161.
14. Hodel, R. (2013). An Introduction to Mathematical Logic. Dover Publications, 512.
15. Shoenfield, J. (2018). Mathematical Logic. A K Peters/CRC Press, 356. doi: https://doi.org/10.1201/9780203749456

DOI: 10.15587/1729-4061.2022.269221

MANAGING SECURITY IN IOT BY APPLYING THE DEEP NEURAL NETWORK-BASED SECURITY FRAMEWORK (p. 38–50)

Nabeel Mahdy Haddad
Misan University, Amarah, Iraq
ORCID: https://orcid.org/0000-0003-1933-5225

Hayder Sabah Salih
Iraqi Ministry of Higher Education and Scientific Research, Baghdad, Iraq
ORCID: https://orcid.org/0000-0001-7983-1269

Ban Salman Shukur
Baghdad College, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-7351-0760

Sura Khalil Abd
Universiti Tenaga Nasional, Selangor, Malaysia
Dijlah University College, Doura, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-1593-4506

Mohammed Hasan Ali
Imam Ja'afar Al-sadiq University, Najaf, Iraq
ORCID: https://orcid.org/0000-0001-7963-0918

Rami Qais Malik
Al-Mustaqbal University College, Hila, Babylon, Iraq
ORCID: https://orcid.org/0000-0003-2518-9260

Security issues and Internet of Things (IoT) risks in several areas are growing steadily with the increased usage of IoT. The systems have developed weaknesses in computer and memory constraints in most IoT operating systems. IoT devices typically cannot operate complicated defense measures because of their poor processing capabilities. A shortage of IoT ecosystems is the most critical impediment to developing a secured IoT device. In addition, security issues create several problems, such as data access control, attacks, vulnerabilities, and privacy protection issues. These security issues lead to affect the originality of the data that cause to affects the data analysis. This research proposes an AI-based security method for the IoT environment (AI-SM-IoT) system to overcome security problems in IoT. This design was based on the edge of the network of AI-enabled security components for IoT emergency preparedness. The modules presented detect, identify and continue to identify the phase of an assault life span based on the concept of the cyberspace killing chain. It outlines each long-term security in the proposed framework and proves its effectiveness in practical applications across diverse threats. In addition, each risk in the borders layer is dealt with by integrating artificial intelligence (AI) safety modules into a separate layer of AI-SM-IoT delivered by services. It contrasted the system framework with the previous designs. It described the architectural freedom from the base areas of the project and its relatively low latency, which provides safety as a service rather than an embedded network edge on the internet-of-things design. It assessed the proposed design based on the administration score of the IoT platform, throughput, security, and working time.

Keywords: Internet of things, security, artificial intelligence, fog computing, wireless sensors, security threats.

References

1. Oniani, S., Marques, G., Barnovi, S., Pires, I. M., Bhoi, A. K. (2020). Artificial Intelligence for Internet of Things and Enhanced Medical Systems. Studies in Computational Intelligence, 43–59. doi: https://doi.org/10.1007/978-981-15-5495-7_3
2. Su, J., Chu, X., Kadry, S., S, R. (2020). Internet-of-Things-Assisted Smart System 4.0 Framework Using Simulated Routing Procedures. Sustainability, 12 (15), 6119. doi: https://doi.org/10.3390/su12156119
3. El-Latif, A. A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C., Venegas-Andraca, S. E. (2020). Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario. IEEE Transactions on Network and Service Management, 17 (1), 118–131. doi: https://doi.org/10.1109/tnsm.2020.2969863
4. Chakraborty, N., Li, J.-Q., Mondal, S., Luo, C., Wang, H., Alazab, M. et al. (2021). On Designing a Lesser Obtrusive Authentication Protocol to Prevent Machine-Learning-Based Threats in Internet of Things. IEEE Internet of Things Journal, 8 (5), 3255–3267. doi: https://doi.org/10.1109/jiot.2020.3025274
5. Manogaran, G., Mumtaz, S., Mavromoustakis, C. X., Pallis, E., Mastorakis, G. (2021). Artificial Intelligence and Blockchain-Assisted Offloading Approach for Data Availability Maximization in Edge Nodes. IEEE Transactions on Vehicular Technology, 70 (3), 2404–2412. doi: https://doi.org/10.1109/tvt.2021.3058689
6. Zheng, W., Muthu, B., Kadry, S. N. (2021). Research on the design of analytical communication and information model for teaching resources with cloud-sharing platform. Computer Applications in Engineering Education, 29 (2), 359–369. doi: https://doi.org/10.1002/cae.22375
7. Wang, W., Jackson Samuel, R. D., Hsu, C.-H. (2020). Prediction architecture of deep learning assisted short long term neural network for advanced traffic critical prediction system using remote sensing data. European Journal of Remote Sensing, 54 (sup2), 65–76. doi: https://doi.org/10.1080/22797254.2020.1755998
8. Rauf, H. T., Gao, J., Almadhor, A., Arif, M., Nafis, M. T. (2021). Enhanced bat algorithm for COVID-19 short-term forecasting using optimized LSTM. Soft Computing, 25 (20), 12989–12999. doi: https://doi.org/10.1007/s00500-021-06075-8
9. Mohamed Shakeel, P., Baskar, S., Sarma Dhulipala, V. R., Mishra, S., Jaber, M. M. (2018). RETRACTED ARTICLE: Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks. Journal of Medical Systems, 42 (10). doi: https://doi.org/10.1007/s10916-018-1045-z
10. Amudha, G., Narayanasamy, P. (2018). Distributed Location and Trust Based Replica Detection in Wireless Sensor Networks. Wireless Personal Communications, 102 (4), 3303–3321. doi: https://doi.org/10.1007/s11277-018-5369-2
11. Nguyen, T. N., Le, V. V., Chu, S.-I., Liu, B.-H., Hsu, Y.-C. (2021). Secure Localization Algorithms Against Localization Attacks in Wireless Sensor Networks. Wireless Personal Communications, 127 (1), 767–792. doi: https://doi.org/10.1007/s11277-021-08404-4
12. Malarvizhi Kumar, P., Choong Seon, H. (2021). RETRACTED ARTICLE: Internet of Things-Based Digital Video Intrusion for Intelligent Monitoring Approach. Arabian Journal for Science and Engineering. doi: https://doi.org/10.1007/s13369-021-05902-2
13. Manickam, A., Jiang, J., Zhou, Y., Sagar, A., Soundrapandiyan, R., Dinesh Jackson Samuel, R. (2021). Automated pneumonia detection on chest X-ray images: A deep learning approach with different optimizers and transfer learning architectures. Measurement, 184, 109953. doi: https://doi.org/10.1016/j.measurement.2021.109953
14. Sheron, P. S. F., Sridhar, K. P., Baskar, S., Shakeel, P. M. (2019). A decentralized scalable security framework for end-to-end authentication of future IoT communication. Transactions on Emerging Telecommunications Technologies, 31 (12). doi: https://doi.org/10.1002/ett.3815
15. Amudha, G. (2021). Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions. Wireless Personal Communications, 127 (1), 85–105. doi: https://doi.org/10.1007/s11277-021-08094-y
16. Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. Future Generation Computer Systems, 123, 1–13. doi: https://doi.org/10.1016/j.future.2021.01.028
17. Nguyen, T. N., Liu, B.-H., Nguyen, N. P., Dumba, B., Chou, J.-T. (2021). Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks. IEEE Transactions on Power Delivery, 36 (4), 2264–2273. doi: https://doi.org/10.1109/tpwrd.2021.3061358
18. Singh, S., Sharma, P. K., Yoon, B., Shojafar, M., Cho, G. H., Ra, I.-H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society, 63, 102364. doi: https://doi.org/10.1016/j.scs.2020.102364
19. Javaid, N., Sher, A., Nasir, H., Guizani, N. (2018). Intelligence in IoT-Based 5G Networks: Opportunities and Challenges. IEEE Communications Magazine, 56 (10), 94–100. doi: https://doi.org/10.1109/mcom.2018.1800036
20. Mao, B., Kawamoto, Y., Kato, N. (2020). AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things. IEEE Internet of Things Journal, 7 (8), 7032–7042. doi: https://doi.org/10.1109/jiot.2020.2982417

21. Mendhurwar, S., Mishra, R. (2019). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15 (4), 565–584. doi: https://doi.org/10.1080/17517575.2019.1600041
22. Mukherjee, A., Goswami, P., Yang, L., Sah Tyagi, S. K., Samal, U. C., Mohapatra, S. K. (2020). Deep neural network-based clustering technique for secure IIoT. Neural Computing and Applications, 32 (20), 16109–16117. doi: https://doi.org/10.1007/s00521-020-04763-4
23. Vimal, S., Khari, M., Crespo, R. G., Kalaivani, L., Dey, N., Kaliappan, M. (2020). Energy enhancement using Multiobjective Ant colony optimization with Double Q learning algorithm for IoT based cognitive radio networks. Computer Communications, 154, 481–490. doi: https://doi.org/10.1016/j.comcom.2020.03.004
24. Alqaralleh, B. A. Y., Vaiyapuri, T., Parvathy, V. S., Gupta, D., Khanna, A., Shankar, K. (2021). Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Personal and Ubiquitous Computing. doi: https://doi.org/10.1007/s00779-021-01543-2
25. Ahmed Jamal, A., Mustafa Majid, A.-A., Konev, A., Kosachenko, T., Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings. doi: https://doi.org/10.1016/j.matpr.2021.06.320
26. Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., Chen, J. (2020). A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. IEEE Transactions on Services Computing, 1–1. doi: https://doi.org/10.1109/tsc.2020.2964537
27. Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A., Alzahrani, B. A. (2020). Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications, 157, 102537. doi: https://doi.org/10.1016/j.jnca.2020.102537
28. Poniszewska-Maranda, A., Kaczmarek, D., Kryvinska, N., Xhafa, F. (2018). Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service system. Computing, 101 (11), 1661–1685. doi: https://doi.org/10.1007/s00607-018-0680-z
29. Zaidan, A. A., Zaidan, B. B. (2018). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artificial Intelligence Review, 53 (1), 141–165. doi: https://doi.org/10.1007/s10462-018-9648-9
30. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R. (2020). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. Transactions on Emerging Telecommunications Technologies, 32 (6). doi: https://doi.org/10.1002/ett.4112
31. Sultana, T., Wahid, K. A. (2019). IoT-Guard: Event-Driven Fog-Based Video Surveillance System for Real-Time Security Management. IEEE Access, 7, 134881–134894. doi: https://doi.org/10.1109/access.2019.2941978
32. Li, D., Deng, L., Liu, W., Su, Q. (2020). Improving communication precision of IoT through behavior-based learning in smart city environment. Future Generation Computer Systems, 108, 512–520. doi: https://doi.org/10.1016/j.future.2020.02.053
33. Edge-IIoTset Cyber Security Dataset of IoT & IIoT. Available at: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot

DOI: 10.15587/1729-4061.2022.269031

DEVISING AN APPROACH TO ANALYZE THE PARAMETERS FOR DETERMINING POTENTIAL PRE-MODIFIED FIRMWARE OF USB DEVICES (p. 51–58)

Yekaterina Zuyeva
Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-0762-6260

Anna Pyrkova
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0001-8483-451X

Abdizhapar Saparbayev
Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-4494-7568

Aiymzhan Makulova
Narxoz University, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0003-0144-0844

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

This paper reports the results of experiments and studies involving different types of devices that can implement a BadUSB scenario, for example, BadUSB, Rubber Ducky, which, when connected to a computer, impersonate a device with a Human Interface Device, emulating other devices such as a keyboard and mouse.

Given the problem of the lack of management tools for detecting preliminary modifications of USB devices against attacks based on the seizure of computer control, a software and hardware system is proposed as an object of study. It is implemented programmatically in the Arduino IDE environment, and physically it is made on the Arduino Mega board with Shield, which reads the parameters of the devices. It monitors the startup of USB devices and checks each device for pre-retrofitting by passing HID descriptors from the connected hardware. Having parsed the data using Python, the data are represented in the appropriate form for analysis, on the basis of which a decision is made by the system on the possible preliminary modification of the USB drive from which these data came. This is due to the detailed consideration and thorough analysis of data, data types, temporal characteristics of data transmitted along different channels. The technical characteristics and functionality of USB devices were investigated; the parameters transmitted at the moment when they are supplied with power were determined. The system can draw a conclusion based on the analysis according to its algorithm and block a suspicious USB device that has been connected and that can intercept control over the computer.

The results of the study could be used in the field of protection of information systems from attacks based on the seizure of control from external media. The designed solution increases the level of security of the system, making it possible to recognize a possibly pre-modified device at the connection stage.

Keywords: information protection, USB devices, HID, BadUSB, USB controllers, modification of USB devices.

References

1. Neuner, S., Voyiatzis, A. G., Fotopoulos, S., Mulliner, C., Weippl, E. R. (2018). USBlock: Blocking USB-Based Keypress Injection At-

tacks. Lecture Notes in Computer Science, 278–295. doi: https://doi.org/10.1007/978-3-319-95729-6_18
2. Yang, B., Qin, Y., Zhang, Y., Wang, W., Feng, D. (2016). TMSUI: A Trust Management Scheme of USB Storage Devices for Industrial Control Systems. Lecture Notes in Computer Science, 152–168. doi: https://doi.org/10.1007/978-3-319-29814-6_13
3. Johnson, P. C., Bratus, S., Smith, S. W. (2017). Protecting Against Malicious Bits On the Wire. Proceedings of the 33rd Annual Computer Security Applications Conference. doi: https://doi.org/10.1145/3134600.3134630
4. Ramadhanty, A. D., Budiono, A., Almaarif, A. (2020). Implementation and Analysis of Keyboard Injection Attack using USB Devices in Windows Operating System. 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE). doi: https://doi.org/10.1109/ic2ie50715.2020.9274631
5. Mueller, T., Zimmer, E., de Nittis, L. (2019). Using Context and Provenance to defend against USB-borne attacks. Proceedings of the 14th International Conference on Availability, Reliability and Security. doi: https://doi.org/10.1145/3339252.3339268
6. Karystinos, E., Andreatos, A., Douligeris, C. (2019). Spyduino: Arduino as a HID Exploiting the BadUSB Vulnerability. 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). doi: https://doi.org/10.1109/dcoss.2019.00066
7. Mohammadmoradi, H., Gnawali, O. (2018). Making Whitelisting-Based Defense Work Against BadUSB. ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment. Available at: http://www2.cs.uh.edu/~gnawali/papers/badusb-icsde2018.pdf
8. Ji, X., Le Guernic, G., Cuppens-Boulahia, N., Cuppens, F. (2018). USB Packets Filtering Policies and an Associated Low-Cost Simulation Framework. Lecture Notes in Computer Science, 732–742. doi: https://doi.org/10.1007/978-3-030-01950-1_44
9. Hernandez, G., Fowze, F., Tian, D. (Jing), Yavuz, T., Butler, K. R. B. (2017). FirmUSB. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. doi: https://doi.org/10.1145/3133956.3134050
10. Pyrkova, A., Zuyeva, Ye. (2019). Creating BADUSB devices and system safety analysis. Vestnik KazNITU, 5, 466–470. Available at: https://official.satbayev.university/download/document/12327/%D0%92%D0%95%D0%A1%D0%A2%D0%9D%D0%98%D0%9A-2019%20%E2%84%965.pdf
11. Zueva, E. A., Pyrkova, A. Yu. (2019). Nvestigation of USB devices using ducky script. Vestnik AUES, 3, 53–57. Available at: https://vestnik-aues.kz/frontend/web/uploads/magazine/pdf/1591966671_nFx8A8.pdf#page=55
12. Zueva Ye. (2020). Analysis of work of devices with BADUSB vulnerability. Vestnik KBTU, 17 (1), 141–146. Available at: https://kbtu.edu.kz/images/vesnik_1_2020.pdf

DOI: 10.15587/1729-4061.2022.269027

THE DEVELOPMENT OF A MANAGEMENT DECISION-MAKING METHOD BASED ON THE ANALYSIS OF INFORMATION FROM SPACE OBSERVATION SYSTEMS (p. 59–69)

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

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

Ihor Butko
Academician Yuriy Bugay International Scientific and Technical University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2859-0351

Mykola Butko
Chernihiv Polytechnic National University, Chernihiv, Ukraine
ORCID: https://orcid.org/0000-0002-4349-1298

Veronika Khudolei
Academician Yuriy Bugay International Scientific and Technical University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-6658-7065

Stanislav Kukhtyk
Academician Yuriy Bugay International Scientific and Technical University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2738-5866

The object of this study is the process of making a management decision based on the analysis of information from space surveillance systems.

Unlike the well-known ones, the method of making a management decision based on the analysis of information from space surveillance systems involves:

– segmentation of an optoelectronic image;

– determination and prediction of a priori probabilities of possible environmental states;

– an application for making a management decision of a combination of Bayes criteria and a minimum of variance.

Experimental studies have been carried out on making a management decision based on the analysis of information from space surveillance systems. To conduct experimental research on making a management decision based on the analysis of information from space surveillance systems, a model problem has been stated. As images from space surveillance systems, images obtained from the WorldView-2 spacecraft (USA) with a difference of four days were considered. The vegetation index was calculated, and the probabilities of degradation dynamics of plant segments were determined. It was established that the maximum value of the estimated functional is achieved when choosing a solution φ_1, which is optimal according to the Bayesian criterion and the criterion of minimum variance.

The quality of management decision-making was assessed by the well-known and developed methods. To assess the quality of management decision-making, the concepts of objectivity of the decision-making method and the selectivity of the decision-making method by known and developed method were introduced. It has been established that both methods are objective, and the improved method is more selective (the gain is 2.6 times). This becomes possible through the use of information from space surveillance systems.

Keywords: management decision, space surveillance system, image segmentation, state of the environment, forecasting.

References

1. Khater, E.-S. G., Ali, S. A., Afify, M. T., Bayomy, M. A., Abbas, R. S. (2022). Using of geographic information systems (GIS) to determine the suitable site for collecting agricultural residues. Scientific Reports, 12 (1). doi: https://doi.org/10.1038/s41598-022-18850-0
2. Horbulin, V. P. (2021). The use of space information in the system of geographic information provision of managerial decision-making on Ukraine's national security and defense issues. Visnyk of the National Academy of Sciences of Ukraine, 9, 3–11. doi: https://doi.org/10.15407/visn2021.09.003

3. Harrison, T., Strohmeyer, M. (2022). Commercial Space Remote Sensing and Its Role in National Security. CSIS BRIEFS. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220202_Harrison_Commercial_Space.pdf?VgV9.43i5ZGs8JDAYDtz0KNbkEnXpH21
4. Military Imaging and Surveillance Technology (MIST) (Archived). Available at: https://www.darpa.mil/program/military-imaging-and-surveillance-technology
5. Hosseini, S., Baziyad, H., Norouzi, R., Jabbedari Khiabani, S., Gidófalvi, G., Albadvi, A. et al. (2021). Mapping the intellectual structure of GIS-T field (2008–2019): a dynamic co-word analysis. Scientometrics, 126 (4), 2667–2688. doi: https://doi.org/10.1007/s11192-020-03840-8
6. Rashidi, K., Noorizadeh, A., Kannan, D., Cullinane, K. (2020). Applying the triple bottom line in sustainable supplier selection: A meta-review of the state-of-the-art. Journal of Cleaner Production, 269, 122001. doi: https://doi.org/10.1016/j.jclepro.2020.122001
7. Cherfi, A., Nouira, K., Ferchichi, A. (2018). Very Fast C4.5 Decision Tree Algorithm. Applied Artificial Intelligence, 32 (2), 119–137. doi: https://doi.org/10.1080/08839514.2018.1447479
8. Katranzhy, L., Podskrebko, O., Krasko, V. (2018). Modelling the dynamics of the adequacy of bank's regulatory capital. Baltic Journal of Economic Studies, 4(1), 188–194. doi: https://doi.org/10.30525/2256-0742/2018-4-1-188-194
9. Kachayeva, G. I., Mustafayev, A. G. (2018). The use of neural networks for the automatic analysis of electrocardiograms in diagnosis of cardiovascular diseases. Herald of Dagestan State Technical University. Technical Sciences, 45 (2), 114–124. doi: https://doi.org/10.21822/2073-6185-2018-45-2-114-124
10. Zhdanov, V. V. (2016). Experimental method to predict avalanches based on neural networks. Ice and Snow, 56 (4), 502–510. doi: https://doi.org/10.15356/2076-6734-2016-4-502-510
11. Kanev, A., Nasteka, A., Bessonova, C., Nevmerzhitsky, D., Silaev, A., Efremov, A., Nikiforova, K. (2017). Anomaly detection in wireless sensor network of the "smart home" system. 2017 20th Conference of Open Innovations Association (FRUCT). doi: https://doi.org/10.23919/fruct.2017.8071301
12. Sreeshakthy, M., Preethi, J. (2016). Classification of Human Emotion from Deap EEG Signal Using Hybrid Improved Neural Networks with Cuckoo Search. BRAIN: Broad Research in Artificial Intelligence and Neuroscience, 6 (3-4), 60–73. Available at https://doaj.org/article/4c120012c5d44b6abc4e2b389888c7a3
13. Chica, J., Zaputt, S., Encalada, J., Salamea, C., Montalvo, M. (2019). Objective assessment of skin repigmentation using a multilayer perceptron. Journal of Medical Signals & Sensors, 9 (2), 88. doi: https://doi.org/10.4103/jmss.jmss_52_18
14. Massel, L. V., Gerget, O. M., Massel, A. G., Mamedov, T. G. (2019). The Use of Machine Learning in Situational Management in Relation to the Tasks of the Power Industry. EPJ Web of Conferences, 217, 01010. doi: https://doi.org/10.1051/epjconf/201921701010
15. Abaci, K., Yamacli, V. (2019). Hybrid Artificial Neural Network by Using Differential Search Algorithm for Solving Power Flow Problem. Advances in Electrical and Computer Engineering, 19 (4), 57–64. doi: https://doi.org/10.4316/aece.2019.04007
16. Mishchuk, O. S., Vitynskyi, P. B. (2018). Neural Network with Combined Approximation of the Surface of the Response. Research Bulletin of the National Technical University of Ukraine "Kyiv Politechnic Institute," 2, 18–24. doi: https://doi.org/10.20535/1810-0546.2018.2.129022
17. Kazemi, M., Faezirad, M. (2018). Efficiency estimation using nonlinear influences of time lags in DEA Using Artificial Neural Networks. Management Journal, 10 (1), 17–34. doi: https://doi.org/10.22059/IMJ.2018.129192.1006898
18. Parapuram, G., Mokhtari, M., Ben Hmida, J. (2018). An Artificially Intelligent Technique to Generate Synthetic Geomechanical Well Logs for the Bakken Formation. Energies, 11 (3), 680. doi: https://doi.org/10.3390/en11030680
19. Prokoptsev, N. G., Alekseenko, A. E., Kholodov, Y. A. (2018). Traffic flow speed prediction on transportation graph with convolutional neural networks. Computer Research and Modeling, 10 (3), 359–367. doi: https://doi.org/10.20537/2076-7633-2018-10-3-359-367
20. Mennis, J., Liu, J. W. (2005). Mining Association Rules in Spatio-Temporal Data: An Analysis of Urban Socioeconomic and Land Cover Change. Transactions in GIS, 9 (1), 5–17. doi: https://doi.org/10.1111/j.1467-9671.2005.00202.x
21. Miller, H. J., Han, J. (Eds.) (2009). Geographic Data Mining and Knowledge Discovery. CRC Press, 486. doi: https://doi.org/10.1201/9781420073980
22. Manea, E., Di Carlo, D., Depellegrin, D., Agardy, T., Gissi, E. (2019). Multidimensional assessment of supporting ecosystem services for marine spatial planning of the Adriatic Sea. Ecological Indicators, 101, 821–837. doi: https://doi.org/10.1016/j.ecolind.2018.12.017
23. Cressie, N. (1993). Statistics for spatial data. John Wiley & Sons, Inc. doi: https://doi.org/10.1002/9781119115151
24. History and evolution of big data analytics. Available at https://www.sas.com/en_us/insights/analytics/big-data-analytics.html
25. Li, S. Zhi, Hu, Q., Deng, X. Hong, Cai, Z. Quan (2019). Reversible image watermarking based on texture analysis of grey level co-occurrence matrix. International Journal of Computational Science and Engineering, 19 (1), 83. doi: https://doi.org/10.1504/ijcse.2019.099642
26. De O. Bastos, L., Liatsis, P., Conci, A. (2008). Automatic texture segmentation based on k-means clustering and efficient calculation of co-occurrence features. 2008 15th International Conference on Systems, Signals and Image Processing. doi: https://doi.org/10.1109/iwssip.2008.4604387
27. Hung, C.-C., Song, E., Lan, Y. (2019). Image Texture, Texture Features, and Image Texture Classification and Segmentation. Image Texture Analysis, 3–14. doi: https://doi.org/10.1007/978-3-030-13773-1_1
28. Tian, Y., Li, Y., Liu, D., Luo, R. (2016). FCM texture image segmentation method based on the local binary pattern. 2016 12th World Congress on Intelligent Control and Automation (WCICA). doi: https://doi.org/10.1109/wcica.2016.7578571
29. Khudov, H., Makoveichuk, O., Butko, I., Gyrenko, I., Stryhun, V., Bilous, O., Shamrai, N. et al. (2022). Devising a method for segmenting camouflaged military equipment on images from space surveillance systems using a genetic algorithm. Eastern-European Journal of Enterprise Technologies, 3 (9 (117)), 6–14. doi: https://doi.org/10.15587/1729-4061.2022.259759
30. Jing, Z., Wei, D., Youhui, Z. (2012). An Algorithm for Scanned Document Image Segmentation Based on Voronoi Diagram. 2012 International Conference on Computer Science and Electronics Engineering. doi: https://doi.org/10.1109/iccsee.2012.144
31. Shanmugavadivu, P., Sivakumar, V. (2012). Fractal Dimension Based Texture Analysis of Digital Images. Procedia Engineering, 38, 2981–2986. doi: https://doi.org/10.1016/j.proeng.2012.06.348
32. Simon, P., V, U. (2020). Deep Learning based Feature Extraction for Texture Classification. Procedia Computer Science, 171, 1680–1687. doi: https://doi.org/10.1016/j.procs.2020.04.180
33. Khudov, H., Makoveichuk, O., Khizhnyak, I., Oleksenko, O., Khazhanets, Y., Solomonenko, Y. et al. (2022). Devising a method

for segmenting complex structured images acquired from space observation systems based on the particle swarm algorithm. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 6–13. doi: https://doi.org/10.15587/1729-4061.2022.255203

34. Berezina, S., Solonets, O., Lee, K., Bortsova, M. (2021). An information technique for segmentation of military assets in conditions of uncertainty of initial data. Information Processing Systems, 4 (167), 6–18. doi: https://doi.org/10.30748/soi.2021.167.01
35. Ruban, I., Khudov, H., Makoveichuk, O., Chomik, M., Khudov, V., Khizhnyak, I. et al. (2019). Construction of methods for determining the contours of objects on tonal aerospace images based on the ant algorithms. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 25–34. doi: https://doi.org/10.15587/1729-4061.2019.177817
36. Mittal, H., Pandey, A. C., Saraswat, M., Kumar, S., Pal, R., Modwel, G. (2021). A comprehensive survey of image segmentation: clustering methods, performance parameters, and benchmark datasets. Multimedia Tools and Applications, 81 (24), 35001–35026. doi: https://doi.org/10.1007/s11042-021-10594-9
37. Khudov, H., Makoveichuk, O., Khudov, V., Maliuha, V., Andriienko, A., Tertyshnik, Y. et al. (2022). Devising a method for segmenting images acquired from space optical and electronic observation systems based on the Sine-Cosine algorithm. Eastern-European Journal of Enterprise Technologies, 5 (9 (119)), 17–24. doi: https://doi.org/10.15587/1729-4061.2022.265775
38. Butko, I. (2021). Model and method of making management decisions based on the analysis of geospatial information. Advanced Information Systems, 5 (2), 42–48. doi: https://doi.org/10.20998/2522-9052.2021.2.07
39. Mashtalir, V., Ruban, I., Levashenko, V. (Eds.) (2020). Advances in Spatio-Temporal Segmentation of Visual Data. Studies in Computational Intelligence. doi: https://doi.org/10.1007/978-3-030-35480-0
40. Khudov, H., Makoveichuk, O., Misiuk, D., Pievtsov, H., Khizhnyak, I., Solomonenko, Y. et al. (2022). Devising a method for processing the image of a vehicle's license plate when shooting with a smartphone camera . Eastern-European Journal of Enterprise Technologies, 1 (2 (115), 6–21. doi: https://doi.org/10.15587/1729-4061.2022.252310
41. Khudov, H., Makoveychuk, O., Butko, I., Khizhnyak, I. (2021). A Model for Prediction of Geospatial Data in Systems for Processing Geospatial Information. Systems of Arms and Military Equipment, 2 (66), 123–28. doi: https://doi.org/10.30748/soivt.2021.66.16
42. Box, G. E. P., Jenkins, G. M., Reinsel, G. C. (1994). Time Series Analysis: Forecasting and Control. Englewood Cliffs, NJ: Prentice Hall. Available at https://www.worldcat.org/title/28888762
43. Brockwell, P. J., Davis, R. A. (2009). Time Series: Theory and Methods. Springer, 580. doi: https://doi.org/10.1007/978-1-4419-0320-4
44. Khudov, G. V. (2003). Features of optimization of two-alternative decisions by joint search and detection of objects. Problemy Upravleniya i Informatiki (Avtomatika), 5, 51–59. Available at https://www.researchgate.net/publication/291431400_Features_of_optimization_of_two-alternative_decisions_by_joint_search_and_detection_of_objects
45. Satellite Imagery. Available at https://www.maxar.com/products/satellite-imagery
46. Ronneberger, O., Fischer, P., Brox, T. (2015). U-Net: Convolutional Networks for Biomedical Image Segmentation. Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015, 234–241. doi: https://doi.org/10.1007/978-3-319-24574-4_28

DOI: 10.15587/1729-4061.2022.266801

CLASSIFYING WIRELESS SIGNAL MODULATION SORTING USING CONVOLUTIONAL NEURAL NETWORK (p. 70–79)

Ekhlas Hamza
University of Technology - Iraq, Baghdad, Iraq
ORCID: https://orcid.org/0000-0003-4351-3685

Sameir Aziez
University of Technology - Iraq, Baghdad, Iraq
ORCID: https://orcid.org/0000-0003-0136-3869

Fadia Hummadi
Al-Khwarizmi College of Engineering, University of Baghdad, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-8179-5305

Ahmad Sabry
Al-Nahrain University, Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-2736-5582

Deep learning has recently been used for this issue with superior results in automatic modulation classification. Previous studies state that it is challenging to categorize a variety of modulation formats using traditional approaches; however, modulation classification is a crucial component of non-cooperative communication in wireless communication. The deep learning network was applied to solve the issue and get decent outcomes. This work uses a deep learning convolutional neural network (DLCNN) to classify three analog and eight digital modulation techniques by generating channel-impaired and synthetic waveforms as training data. The obtained DLCNN is tested by over-the-air indicators and a Software Define Radio(SDR) platform. The trained DLCNN estimates the modulation kind of each frame by taking 1024 samples of channel-impaired signals. The method includes generating several frames of 4-arry pulse amplitude modulation (PAM4) that are impaired with sampling time drift, Additive white Gaussian noise (AWGN), center frequency, and Rician multipath fading. The DLCNN predicts real inputs when receiving a signal with complex samples of baseband. Before updating the network coefficients and on all iterations, the data store transforms data from files and records it. This network takes about 50 minutes to train using in-memory data and 110 minutes to train using disk data. The evaluation of the trained DLCNN is carried out by obtaining the classification accuracy for the test frames. The obtained outcome demonstrates that the developed network can achieve an accuracy of about 94.3 % in roughly 12 epochs for such types of waveforms, which elapsed about 26 minutes for training. This will increase the efficiency of spectrum usage and detect the modulation type of the wireless communication receivers.

Keywords: wireless communications, digital modulation, deep learning convolutional neural network classifiers.

References

1. Huynh-The, T., Pham, Q.-V., Nguyen, T.-V., Nguyen, T. T., Ruby, R., Zeng, M., Kim, D.-S. (2021). Automatic Modulation Classification: A Deep Architecture Survey. IEEE Access, 9, 142950–142971. doi: https://doi.org/10.1109/access.2021.3120419
2. Xu, Y., Li, D., Wang, Z., Guo, Q., Xiang, W. (2018). A deep learning method based on convolutional neural network for automatic modulation classification of wireless signals. Wireless Networks, 25 (7), 3735–3746. doi: https://doi.org/10.1007/s11276-018-1667-6
3. Al-Shoukry, S., M. Jawad, B. J., Musa, Z., Sabry, A. H. (2022). Development of predictive modeling and deep learning classifica-

tion of taxi trip tolls. Eastern-European Journal of Enterprise Technologies, 3 (3 (117)), 6–12. doi: https://doi.org/10.15587/1729-4061.2022.259242

4. Jwaid, W. M., Al-Husseini, Z. S. M., Sabry, A. H. (2021). Development of brain tumor segmentation of magnetic resonance imaging (MRI) using U-Net deep learning. Eastern-European Journal of Enterprise Technologies, 4 (9(112)), 23–31. doi: https://doi.org/10.15587/1729-4061.2021.238957
5. Shijer, S. S., Sabry, A. H. (2021). Analysis of performance parameters for wireless network using switching multiple access control method. Eastern-European Journal of Enterprise Technologies, 4 (9 (112)), 6–14. doi: https://doi.org/10.15587/1729-4061.2021.238457
6. Zhang, H., Wang, Y., Xu, L., Aaron Gulliver, T., Cao, C. (2020). Automatic Modulation Classification Using a Deep Multi-Stream Neural Network. IEEE Access, 8, 43888–43897. doi: https://doi.org/10.1109/access.2020.2971698
7. Zhou, Y., Lin, T., Zhu, Y. (2020). Automatic Modulation Classification in Time-Varying Channels Based on Deep Learning. IEEE Access, 8, 197508–197522. doi: https://doi.org/10.1109/access.2020.3034942
8. Clement, J. C., Indira, N., Vijayakumar, P., Nandakumar, R. (2020). Deep learning based modulation classification for 5G and beyond wireless systems. Peer-to-Peer Networking and Applications, 14 (1), 319–332. doi: https://doi.org/10.1007/s12083-020-01003-3
9. Perenda, E., Rajendran, S., Bovet, G., Pollin, S., Zheleva, M. (2022). Evolutionary Optimization of Residual Neural Network Architectures for Modulation Classification. IEEE Transactions on Cognitive Communications and Networking, 8 (2), 542–556. doi: https://doi.org/10.1109/tccn.2021.3137519
10. Zhou, R., Liu, F., Gravelle, C. W. (2020). Deep Learning for Modulation Recognition: A Survey With a Demonstration. IEEE Access, 8, 67366–67376. doi: https://doi.org/10.1109/access.2020.2986330
11. Ujan, S., Navidi, N., Landry, R. J. (2020). Hierarchical Classification Method for Radio Frequency Interference Recognition and Characterization in Satcom. Applied Sciences, 10 (13), 4608. doi: https://doi.org/10.3390/app10134608
12. Zheng, S., Qi, P., Chen, S., Yang, X. (2019). Fusion Methods for CNN-Based Automatic Modulation Classification. IEEE Access, 7, 66496–66504. doi: https://doi.org/10.1109/access.2019.2918136
13. Ji, K., Chang, S., Huang, S., Chen, H., Jia, S., Lu, H. (2021). Modulation Classification of Active Attack Signals for Internet of Things Using GP-CNN Network. 2021 IEEE International Conference on Communications Workshops (ICC Workshops). doi: https://doi.org/10.1109/iccworkshops50388.2021.9473800
14. Al-Nuaimi, D. H., Akbar, M. F., Salman, L. B., Abidin, I. S. Z., Isa, N. A. M. (2021). AMC2N: Automatic Modulation Classification Using Feature Clustering-Based Two-Lane Capsule Networks. Electronics, 10 (1), 76. doi: https://doi.org/10.3390/electronics10010076

DOI: 10.15587/1729-4061.2022.267892

SOFTWARE PROTOTYPE DEVELOPMENT FOR NON-CENTRALIZED OBJECTS OF WIND FLOW AMPLIFICATION (p. 80–88)

Gaukhar Alina
Abylkas Saginov Karaganda Technical University, Karaganda, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-7697-4667

Nurlan Tashatov
L. N. Gumilyov Eurasian National University, Nur-Sultan, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-3271-2163

Galina Tatkeyeva
S. Seifullin Kazakh Agro Technical University, Nur-Sultan, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0115-6344

Madi Bauyrzhanuly
S. Seifullin Kazakh Agro Technical University, Nur-Sultan, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-6425-1402

Dinara Kaibassova
Abylkas Saginov Karaganda Technical University, Karaganda, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-8410-7758

Margulan Nurtay
Abylkas Saginov Karaganda Technical University, Karaganda, Republic of Kazakhstan
ORCID: https://orcid.org/0000-0002-0786-6195

This research is devoted to the development of software to increase the efficiency of autonomous wind-generating substations using panel structures, which will allow the use of wind energy to generate electricity with minimal losses and for the life support of buildings and structures. In the course of the work, a software and hardware system with a functional diagram for experimental measurements was developed. The paper also describes the process of modeling wind generation, collecting and transmitting real-time data to a web server via the HTTPS protocol. Due to the intensive development of wind energy in Kazakhstan, there is a need to apply methods to improve the energy generation process. In particular, the use of hardware and software to monitor and make decisions on optimizing the power generation process will help solve the problem of limited economic and labor resources. The results of the experiments revealed that the automatic control of the shield structures allows specialists to increase the effectiveness of the energy generation process by 25 % and, thus, a non-linear relationship between the power of the generated energy, the speed and direction of wind has been revealed. It should also be noted that the results obtained in the course of this research make it possible to solve the problem of saving electricity in the cities of Kazakhstan, since so far there are only large-scale wind farms, which is not always available in simple urban conditions. Moreover, the software developed during the study will allow autonomous control and analysis of the behavior of the wind farm, taking into account various weather conditions. In the future, the methods of data analysis will be applied to the data obtained via the process of modeling.

A script for receiving and transmitting real-time data with wind speed and direction sensors has been developed.

Keywords: wind energy, Internet of Things, software, real time, Django, process monitoring.

References

1. Megantoro, P., Pramudita, B. A., Vigneshwaran, P., Yurianta, A., Winarno, H. A. (2021). Real-time monitoring system for weather and air pollutant measurement with HTML-based UI application. Bulletin of Electrical Engineering and Informatics, 10 (3), 1669–1677. doi: https://doi.org/10.11591/eei.v10i3.3030
2. Tomilova, N., Tomilov, A., Kaibassova, D., Kalinin, A., Amirov, A., Nurtay, M. (2022). Digital models of stabilizing the hydraulic mode of heat supply systems. Journal of Theoretical and Applied Information Technology, 100 (2), 322–335. Available at: http://www.jatit.org/volumes/Vol100No2/3Vol100No2.pdf
3. Navulur, S., S. C. S. Sastry, A., N. Giri Prasad, M. (2017). Agricultural Management through Wireless Sensors and Internet of

Things. International Journal of Electrical and Computer Engineering (IJECE), 7 (6), 3492. doi: https://doi.org/10.11591/ijece.v7i6.pp3492-3499

4. Megantoro, P., Prastio, R. P., Kusuma, H. F. A., Abror, A., Vigneshwaran, P., Priambodo, D. F., Alif, D. S. (2022). Instrumentation system for data acquisition and monitoring of hydroponic farming using ESP32 via Google Firebase. Indonesian Journal of Electrical Engineering and Computer Science, 27 (1), 52. doi: https://doi.org/10.11591/ijeecs.v27.i1.pp52-61
5. Chaudhuri, T., Nyamati, V., Jayavel, K. (2018). Design and implementation of IoT framework for Home Automation and Monitoring. 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference On. doi: https://doi.org/10.1109/i-smac.2018.8653724
6. Robson, W., Ernawati, I., Nugrahaeni, C. (2021). Design of Multisensor Automatic Fan Control System Using Sugeno Fuzzy Method. Journal of Robotics and Control (JRC), 2 (4). doi: https://doi.org/10.18196/jrc.2496
7. Das, B., Jain, P. C. (2017). Real-time water quality monitoring system using Internet of Things. 2017 International Conference on Computer, Communications and Electronics (Comptelix). doi: https://doi.org/10.1109/comptelix.2017.8003942
8. Peng, Y., Shi, Y., Li, J., Hu, Y. (2022). Optimal Scheduling of 5G Base Station Energy Storage Considering Wind and Solar Complementation. 2022 4th Asia Energy and Electrical Engineering Symposium (AEEES). doi: https://doi.org/10.1109/aeees54426.2022.9759744
9. Volk, R., Stallkamp, C., Herbst, M., Schultmann, F. (2021). Regional rotor blade waste quantification in Germany until 2040. Resources, Conservation and Recycling, 172, 105667. doi: https://doi.org/10.1016/j.resconrec.2021.105667
10. Bezrukikh, P. P., Bezrukikh, P. P. Jr., Karabanov, S. M. (2020). On the Electricity Generation Balances Worldwide and in Russia. Vestnik MEI, 4 (4), 21–28. doi: https://doi.org/10.24160/1993-6982-2020-4-21-28
11. Butterfield, B. L., Bullen, D. B. (2022). Questioning a Green New Deal–Bulk materials requirements for an all-renewable economy in the United States. Energy Research & Social Science, 86, 102424. doi: https://doi.org/10.1016/j.erss.2021.102424
12. Al Mubarok, A. G., Djatmiko, W., Yusro, M. (2018). Design of Arduino-based small wind power generation system. E3S Web of Conferences, 67, 01006. doi: https://doi.org/10.1051/e3sconf/20186701006
13. Mahmuddin, F., Yusran, A. M., Klara, S. (2017). On the use of an Arduino-based controller to control the charging process of a wind turbine. AIP Conference Proceedings. doi: https://doi.org/10.1063/1.4976284
14. Liu, Q., Sun, X. (2012). Research of Web Real-Time Communication Based on Web Socket. International Journal of Communications, Network and System Sciences, 05 (12), 797–801. doi: https://doi.org/10.4236/ijcns.2012.512083
15. Skvorc, D., Horvat, M., Srbljic, S. (2014). Performance evaluation of Websocket protocol for implementation of full-duplex web streams. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). doi: https://doi.org/10.1109/mipro.2014.6859715
16. Ferdiansyah, N., Rahayu, D. A., Permala, R. (2019). Comparation of postgresql, mariadb and mongodb capabilities in processing lapan satellite ais data. Pengembangan Iptek Litbangyasa Pesawat Terbang, Roket Dan Satelit. doi: https://doi.org/10.30536/p.siptekgan.2019.v23.23
17. Rubio, D. (2017). Introduction to the Django Framework. Beginning Django, 1–29. doi: https://doi.org/10.1007/978-1-4842-2787-9_1
18. Shyam, A., Mukesh, N. (2020). A Django Based Educational Resource Sharing Website: Shreic. Journal of Scientific Research, 64 (01), 138–152. doi: https://doi.org/10.37398/jsr.2020.640134_

АНОТАЦІЇ

INFORMATION AND CONTROLLING SYSTEM

DOI: 10.15587/1729-4061.2022.266990

ДОСЛІДЖЕННЯ ВПЛИВУ МЕРЕЖЕВИХ ТОПОЛОГІЙ НА БЕЗДРОТОВІ СЕНСОРНІ МЕРЕЖІ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ В СИСТЕМІ МОНІТОРИНГУ РОЗУМНОГО БУДИНКУ (с. 6–14)

Shayma W. Nourildean, Yousra A. Mohammed, May T. Abdulhadi

Метою даного дослідження є представлення системи моніторингу розумного будинку на базі бездротових сенсорних мереж на основі Інтернету речей, що дозволяє користувачам контролювати і управляти всіма своїми побутовими приладами та обладнанням через Інтернет за встановленими протоколами. Інтернет речей описується як підключення обладнання та побутової техніки до Інтернету з метою моніторингу, звітування та виконання певних завдань. Бездротові сенсорні мережі (БСМ) розглядаються як ключовий компонент при реалізації моделі Інтернету речей. У роботі представлена платформа БСМ IP з використанням програми моделювання Riverbed Modeler для вивчення продуктивності мережі для різних топологій бездротових датчиків (зірка, дерево та решітка). Дана платформа складається з ряду сценаріїв з декількома датчиками в кожному сценарії. Кожен датчик представлений кінцевим пристроєм ZigBee, який зчитує та збирає дані розумного будинку та надсилає зібрані дані на контролер, що представлений координатором ZigBee. Контролер надсилає дані на сервер для моніторингу користувачами через будь-який шлюз (Wi-Fi) після входу в систему за допомогою певної програми з трьома топологіями маршрутизації на контролері. Результати показали, що деревоподібна топологія БСМ IP є найкращою топологією, якщо розглядати можливість поліпшення пропускної здатності за рахунок втрат даних з прийнятною затримкою. Зіркоподібна топологія підвищує продуктивність мережі з точки зору втрат даних та пропускної здатності при збільшенні кількості датчиків. Решітчата топологія забезпечує найменший обсяг втрат даних за низької пропускної здатності. Завдяки своїм особливостям ці результати були ефективними, оскільки вони показали, що вибір відповідної топології маршрутизації зіграв важливу роль у поліпшенні продуктивності БСМ IP, зниження якої спричинене перешкодами з боку мережі Wi-Fi та ZigBee, оскільки вони використовували один і той самий діапазон частот (2,4 ГГц).

Ключові слова: Інтернет речей, Riverbed, розумний, зірка, дерево, решітка, ZigBee, пропускна здатність, затримка, Wi-Fi.

DOI: 10.15587/1729-4061.2022.268368

РОЗРОБКА МЕТОДУ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА АВТЕНТИЧНОСТІ У БЕЗДРОТОВИХ КАНАЛАХ (с. 15–27)

С. П. Євсеєв, Р. В. Корольов, М. В. Коваль, Х. Н. Рзаєв, О. В. Войтко, О. Б. Ахієзер, А. В. Гребенюк, С. В. Мілевський, Elnur Baghirov, Musa Mammadov

Об'єктом дослідження є розробка методу забезпечення автентичності та цілісності даних в бездротових каналів на основі постквантових криптосистем. Розвиток сучасних цифрових технологій забезпечує перехід на смарт-технології та формування Next Generation Network-мереж. Формування смарт-технологій, як правило використовує бездротові стандарти каналів зв'язку IEEE 802.11X, IEEE 802.15.4, IEEE 802.16, в яких використовуються лише протоколи автентичності та механізми конфіденціальності, які формуються на симетричних алгоритмах. В умовах постквантового періоду (появи повномасштабного квантового комп'ютера) стійкість таких алгоритмів ставиться під сумнів. Такі системи, як правило формуються на основі синтезу соціокіберфізичних систем та хмарних технологій, що спрощує проведення Advanced Persistent Threat-атак, як на внутрішній конур систем виконання, так і на зовнішній системи управління. Створення багатоконтурних систем захисту інформації дозволяє забезпечити об'єктивну оцінку потокового стану системи в цілому та формування превентивних заходів протидії кіберзагрозам. Запропонований метод забезпечення основних послуг безпеки: конфіденційності, цілісності та автентичності на основі крипто-кодових конструкцій враховує рівень секретності інформації яка передається бездротовими каналами та/або зберігається в базах даних соціокіберфізичних систем. Використання постквантових алгоритмів – крипто-кодових конструкцій Мак-Еліса/Нідеррайтера на еліптичних/модифікованих еліптичних/збиткових/ Low-density parity-check code-кодах забезпечує в постквантовий криптоперіод необхідний рівень стійкості (криптостійкість на рівні 10^{25}–10^{35} групових операцій), швидкості та вірогідності інформації ($P_{пом}$ не нижче 10^{-9}–10^{-12}). Запропонований метод обміну інформації з використанням бездротових каналах зв'язку забезпечує їх практичну реалізацію на ресурсообмежених пристроях (побудова ККК на полем GF (2^4–2^6).

Ключові слова: крипто-кодові конструкції Мак-Еліса та Нідеррайтера, смарт-технології, концепція безпеки, багатоконтурні системи захисту.

DOI: 10.15587/1729-4061.2022.269030

ЗАСТОСУВАННЯ ПРИНЦИПУ ФОРМАЛІЗАЦІЇ ОПИСУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ДЛЯ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ (с. 28–37)

В. М. Луценко, Д. О. Прогонов

Розбудова інформаційної незалежності Держави потребує впровадження новітніх технологій аналізу, зберігання, обробки та передачі інформації. Увага даної роботи спрямована на вдосконалення систем захисту інформації з обмеженим доступом, зокрема

розробці новітніх методів проектування таких систем, які відрізняються мінімальним впливом суб'єкта-проектувальника на процес проектування. Об'єктом дослідження є методика і засіб проектування систем обмеження та контролю фізичного доступу, а також доступу до інформації на об'єктах інформаційної діяльності та інформаційно-телекомунікаційних системах України.

Для виключення впливу суб'єкта проектанта необхідно вдосконалити сам процес проектування. В даній роботі математично доведено можливість створення автоматичної системи проектування, заснованої на представленні об'єктів захисту у вигляді об'єктів загальної структури. Така структура поєднує в собі як телекомунікаційні об'єкти, так і об'єкти інформаційної діяльності. Визначено зміни в законодавчій, нормативній та технічній базах захисту інформації, необхідні для впровадження запропонованої системи, зокрема надання Держкомзв'язку України нових повноважень, що забезпечують баланс інтересів замовника систем захисту і виконавців. Показана можливість формалізації представлення даних про довільні об'єкти захисту. Дане представлення дозволяє створювати відкриті бібліотечні семантичні бази даних при неповних даних щодо об'єкту захисту.

Створена теоретична база, яка дозволяє визначати відповідність між множиною загроз інформаційній безпеці об'єкта і однозначним відповідним переліком протидій. При цьому проекти захисту інформації відрізняються еволюційністю і єдиністю вибору множини засобів захисту будь-яким загрозам для об'єктів довільної складності.

Ключові слова: бази даних при неповній інформації, автоматичний проектувальник систем безпеки інформації, об'єкт захисту загальної структури.

DOI: 10.15587/1729-4061.2022.269221

УПРАВЛІННЯ БЕЗПЕКОЮ В IoT ІЗ ЗАСТОСУВАННЯМ ФРЕЙМВОРКА БЕЗПЕКИ НА ОСНОВІ ГЛИБОКОЇ НЕЙРОННОЇ МЕРЕЖІ (с. 38–50)

Nabeel Mahdy Haddad, Hayder Sabah Salih, Ban Salman Shukur, Sura Khalil Abd, Mohammed Hassan Ali, Rami Qais Malik

Проблеми безпеки та ризики Інтернету речей (IoT) у кількох областях неухильно зростають у міру розширення використання IoT. У більшості операційних систем Інтернету речей у системах з'явилися недоліки, пов'язані з обмеженнями комп'ютерів та пам'яті. Пристрої IoT зазвичай не можуть використовувати складні заходи захисту через їх погані обчислювальні можливості. Недостача екосистем IoT є найбільшою перешкодою для розробки захищеного пристрою IoT. Крім того, проблеми з безпекою створюють низку проблем, таких як контроль доступу до даних, атаки, уразливості та проблеми із захистом конфіденційності. Ці проблеми безпеки впливають на оригінальність даних, що впливає аналіз даних. У цьому дослідженні пропонується заснований на ШІ метод забезпечення безпеки середовища IoT (AI-SM-IoT) для подолання проблем безпеки IoT. Цей дизайн був заснований на межі мережі компонентів безпеки за допомогою ШІ для забезпечення готовності до надзвичайних ситуацій IoT. Представлені модулі виявляють, ідентифікують та продовжують ідентифікувати фазу тривалості нападу на основі концепції ланцюжка вбивств у кіберпросторі. Він описує кожну довгострокову безпеку в запропонованій структурі та доводить її ефективність у практичних застосуваннях за різних загроз. Крім того, кожен ризик на прикордонному рівні усувається шляхом інтеграції модулів безпеки штучного інтелекту (ШІ) в окремий рівень AI-SM-IoT, що надається службами. Він вирізняє структуру системи від попередніх проектів. У ньому описувалася архітектурна свобода від базових областей проекту та його відносно низька затримка, яка забезпечує безпеку як послугу, а не вбудований мережний кордон у дизайні Інтернету речей. Він оцінив запропонований дизайн на основі оцінки адміністрування платформи IoT, пропускної спроможності, безпеки та робочого часу.

Ключові слова: Інтернет речей, безпека, штучний інтелект, туманні обчислення, бездротові датчики, загрози безпеці.

DOI: 10.15587/1729-4061.2022.269031

РОЗРОБКА ПІДХОДУ ДО АНАЛІЗУ ПАРАМЕТРІВ ВИЗНАЧЕННЯ МОЖЛИВОЇ ПОПЕРЕДНЬО МОДИФІКОВАНОЇ ПРОШИВКИ USB-ПРИСТРОЇВ (с. 51–58)

Yekaterina Zuyeva, Anna Pyrkova, Abdizhapar Saparbayev, Aiymzhan Makulova, Gulzinat Ordabayeva

Наведено результати експериментів та досліджень з різними типами пристроїв, які можуть здійснювати BadUSB-сценарій, наприклад: BadUSB, Rubber Ducky, які при підключенні до комп'ютера видають себе за пристрій з Human Interface Device, емулюючи інші пристрої, такі як клавіатура та миша.

При проблемі відсутності інструментів управління виявлення попередніх модифікацій USB-пристроїв від атак, заснованих на захопленні управління комп'ютером, в якості об'єкту дослідження пропонується програмно-апаратний комплекс. Програмно він реалізований серед Arduino IDE, а фізично він виконаний на платі Arduino Mega с Shield, що зчитує параметри пристроїв. Він відстежує запуск USB-пристроїв і перевіряє кожен пристрій на факт попередньої модифікованості шляхом передачі дескрипторів HID з обладнання, що підключається. Розпарсувавши дані за допомогою Python, дані подаються у відповідному вигляді для аналізу, на підставі чого приймається рішення системою про можливу попередню модифікацію USB-носія, з якого ці дані надійшли. Це відбувається завдяки детальному розгляду та копіткому аналізу даних, типів даних, тимчасових характеристик даних, що передаються у різних каналах. Було досліджено технічні характеристики та функціональні можливості USB-пристроїв, визначено параметри, що передаються в момент, коли їм подають живлення. Комплекс може робити висновок на підставі аналізу за своїм алгоритмом та блокувати підозрілий USB-пристрій, який був підключений та який може перехопити керування комп'ютером.

Результати дослідження можна використовувати у сфері захисту інформаційних систем від атак, заснованих на захопленні управління із зовнішніх носіїв. Створене рішення підвищує рівень безпеки роботи системи, дозволяючи розпізнати можливо попередньо модифікований пристрій на етапі підключення.

Ключові слова: захист інформації, USB-пристрої, HID, BadUSB, контролери USB, модифікація USB-пристроїв.

DOI: 10.15587/1729-4061.2022.269027

РОЗРОБКА МЕТОДУ ПРИЙНЯТТЯ УПРАВЛІНСЬКОГО РІШЕННЯ НА ОСНОВІ АНАЛІЗУ ІНФОРМАЦІЇ З КОСМІЧНИХ СИСТЕМ СПОСТЕРЕЖЕННЯ (с. 59–69)

Г. В. Худов, О. М. Маковейчук, І. М. Бутко, М. П. Бутко, В. Ю. Худолей, С. В. Кухтик

Об'єктом дослідження є процес прийняття управлінського рішення на основі аналізу інформації з космічних систем спостереження.

На відміну від відомих, метод прийняття управлінського рішення на основі аналізу інформації з космічних систем спостереження передбачає:

– сегментування оптико-електронного зображення;

– визначення та прогнозування апріорних ймовірностей можливих станів середовища;

– застосування для прийняття управлінського рішення комбінації критеріїв Байєса та мінімуму дисперсії.

Проведені експериментальні дослідження щодо прийняття управлінського рішення на основі аналізу інформації з космічних систем спостереження. Для проведення експериментальних досліджень щодо прийняття управлінського рішення на основі аналізу інформації з космічних систем спостереження сформульовано модельна задача. У якості зображень з космічних систем спостереження розглянуто зображення, що отримані з космічного апарату WorldView-2 (США) з різницею у чотири доби. Розраховано вегетаційний індекс та визначені ймовірності деградаційної динаміки рослинних сегментів. Встановлено, що максимальне значення оціночного функціоналу досягається при виборі рішення ϕ_1, яке є оптимальним за байєсовським критерієм та критерієм мінімуму дисперсії.

Проведено оцінювання якості прийняття управлінського рішення відомими та розробленим методом. Для оцінювання якості прийняття управлінського рішення відомими та розробленим методом введені поняття об'єктивності методу прийняття рішення та селективності методу прийняття рішення. Встановлено, що обидва метода є об'єктивними та удосконалений метод є більш селективним (виграш складає 2,6 разів). Це стає можливим завдяки використанню інформації космічних систем спостереження.

Ключові слова: управлінське рішення, космічна система спостереження, сегментування зображення, стан середовища, прогнозування.

DOI: 10.15587/1729-4061.2022.266801

КЛАСИФІКАЦІЯ СОРТУВАННЯ МОДУЛЯЦІЇ СИГНАЛУ БЕЗПРОВІДНОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ ЗВЕРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ (с. 70–79)

Ekhlas Hamza, Sameir Aziez, Fadia Hummadi, Ahmad Sabry

Глибоке навчання нещодавно використовувалося для цієї проблеми та показало чудові результати автоматичної класифікації модуляції. Попередні дослідження стверджують, що складно класифікувати різноманітні формати модуляції, використовуючи традиційні підходи; однак класифікація модуляції є важливим компонентом некооперативного зв'язку при використанні бездротового зв'язку. Мережа глибокого навчання була застосована для вирішення проблеми та отримання гідних результатів. У цій роботі використовується згорткова нейронна мережа з глибоким навчанням (ЗГМГН) для класифікації трьох аналогових та восьми методів цифрової модуляції шляхом створення спотворених каналів та синтетичних сигналів як навчальних даних. Отримана ЗГМГН тестується за допомогою ефірних індикаторів та платформи Software Define Radio (SDR). Навчена ЗГМГН оцінює вид модуляції кожного кадру, взявши 1024 вибірки сигналів із спотвореннями каналу. Спосіб включає генерацію декількох кадрів амплітудної модуляції імпульсів з чотирма рядами (PAM4), які погіршуються через дрейф часу дискретизації, адитивного білого гаусівського шуму (AWGN), центральної частоти і багатопроменевого завмирання Райса. ЗГМГН передбачає реальні вхідні дані прийому сигналу зі складними вибірками основний лінії частот. Перед оновленням мережевих коефіцієнтів та на всіх ітераціях сховище даних перетворює дані з файлів та записує їх. Для навчання мережі з використанням даних у пам'яті потрібно близько 50 хвилин, а для навчання з використанням даних з диска – 110 хвилин. Оцінка навчання ЗГМГН здійснюється шляхом отримання точності класифікації для тестових кадрів. Отриманий результат показує, що розроблена мережа може досягти точності близько 94,3 % приблизно за 12 епох для таких типів сигналів, навчання яких пішло близько 26 хвилин. Це підвищить ефективність використання спектра та визначить тип модуляції приймачів бездротового зв'язку.

Ключові слова: бездротовий зв'язок, цифрова модуляція, класифікатори нейронних згорткових мереж з глибоким навчанням.

DOI: 10.15587/1729-4061.2022.267892

РОЗРОБКА ПРОТОТИПУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ НЕЦЕНТРАЛІЗОВАНИХ ОБ'ЄКТІВ ПОСИЛЕННЯ ВІТРОВОГО ПОТОКУ (с. 80–88)

Gaukhar Alina, Nurlan Tashatov, Galina Tatkeyeva, Madi Bauyrzhanuly, Dinara Kaibassova, Margulan Nurtay

Дане дослідження присвячене розробці програмного забезпечення для підвищення ефективності автономних вітрогенеруючих підстанцій з використанням панельних конструкцій, що дозволить використовувати енергію вітру для вироблення електроенергії

з мінімальними втратами і для життєзабезпечення будівель та споруд. В ході роботи розроблено програмно-апаратний комплекс із функціональною схемою для проведення експериментальних вимірювань. У статті також описується процес моделювання вітрогенерації, збору та передачі даних у режимі реального часу на веб-сервер за протоколом HTTPS. У зв'язку з інтенсивним розвитком вітроенергетики у Казахстані існує необхідність застосування методів удосконалення процесу вироблення енергії. Зокрема, використання технічних та програмних засобів контролю та прийняття рішень щодо оптимізації процесу вироблення електроенергії допоможе вирішити проблему обмежених економічних і трудових ресурсів. Результати експериментів показали, що автоматичне управління щитовими конструкціями дозволяє фахівцям підвищити ефективність процесу вироблення енергії на 25 % і, таким чином, виявлена нелінійна залежність між потужністю вироблюваної енергії, швидкістю та напрямком вітру. Слід також зазначити, що результати, отримані в ході даного дослідження, дозволяють вирішити проблему економії електроенергії в містах Казахстану, оскільки поки існують лише масштабні вітряні електростанції, що не завжди доступно в простих міських умовах. Більш того, розроблене в ході дослідження програмне забезпечення дозволить здійснювати автономне управління та аналізувати поведінку вітроелектростанції з урахуванням різних погодних умов. Надалі методи аналізу даних будуть застосовані до даних, отриманих у процесі моделювання.

Розроблено сценарій прийому та передачі даних з датчиків швидкості і напрямку вітру в режимі реального часу.

Ключові слова: вітроенергетика, Інтернет речей, програмне забезпечення, реальний час, Django, моніторинг процесів.