applied sciences

MDPI

Editorial

Wireless Communication: Applications Security and Reliability—Present and Future

Ireneusz Kubiak

Department of Electromagnetic Compatibility, Military Communication Institute—National Research Institute, 05-130 Zegrze Poludniowe, Poland; i.kubiak@wil.waw.pl

Abstract: Information security is of great importance nowadays. This is related to the widespread use of new technologies in the development of long-distance communications and the use of increasingly "faster" signals. Information security can be considered in many areas of information processing, including wireless systems and wired systems that are based on electronic devices. Each of such devices is a source of electromagnetic disturbances but may also be sensitive to such disturbances. This Special Issue titled "Wireless Communication: Applications, Security, and Reliability" covers a broad spectrum of information security related to cybersecurity, cryptography, and electromagnetic protection. In each case, the information protection solutions used must keep up with the development of technologies used in information processing. The broad thematic area of this Special Issue was intended to encourage scientists and researchers to present their research results and the goals that this research was intended to serve. At the same time, it could allow for the exchange of knowledge and experience gained during the work on information security.

Keywords: MIMO; 5G; cyberattack; security; side-channel attack; cognitive radio; quantitative metrics

check for updates

Citation: Kubiak, I. Wireless Communication: Applications Security and Reliability—Present and Future. *Appl. Sci.* **2024**, *14*, 3865. https://doi.org/10.3390/app14093865

Received: 9 February 2024
Accepted: 28 April 2024
Published: 30 April 2024

1. Introduction

Wireless communication is an indispensable element of our lives. We use it in many areas of telephone communications, the Internet, bank payments, and access control. New wireless technologies not only make our everyday lives easier but also have a huge impact on information security, our safety, and our health. Hence the need to carry out activities at many levels aimed at ensuring communication security and reliability by using solutions resistant to electromagnetic infiltration, in particular sources of sensitive emission related to graphic information, cybercrime, and cryptographic attacks. In each case, there are devices that should ensure the secure transmission of information. However, the development of the used technologies and their unlimited implementation in newer devices increase their sensitivity to external factors. These factors may be intentionally generated electromagnetic fields, disturbing the operation of devices, or even destroying them.

This Special Issue titled "Wireless Communication: Applications, Security, and Reliability" covered all the above-mentioned topic areas. This made it possible to present, from a broad perspective, in one place most issues related to the use of wireless communications [1,2], possible threats [3,4], proposed solutions to increase the level of information [5], and biological safety [6].

2. The Present Issue

This Special Issue consists of seventeen papers covering a broad range of topics related to the applications of wireless communication, cryptography, cybersecurity, and electromagnetic immunity, from cognitive radio and channel acquisition to pseudo-random generators, attack detection, and electromagnetic eavesdropping.

Wideband communication in different frequency bands, efficient use of spectrum, channel sensing and acquisition, protection of information in the aspect of electromagnetic

emissions, and the selection of test methods for new IT devices from the point of view of immunity from electromagnetic fields were particularly interesting for the authors.

The authors of the articles paid attention to many aspects of wireless communication, existing threats, and solutions whose application increases the level of information security. The issues discussed in detail showed how important elements are communication reliability [7–9], information security [10,11], and resistance to various types of external attacks—cyberattacks [12,13], cryptographic attacks [14,15], or electromagnetic attacks [16–19].

In [20], an interesting research problem in edge computing is explored. In particular, the dynamics of delay and reliability caused by VNF parallelization and BVNF deployment are modeled and formulated. The authors also designed an approximation algorithm to solve the formulated problem. In [21], a novel topology construction method for a UAV swarm network that takes into account the criterion of topology duration in addition to other important criteria such as network throughput, end-to-end delay, and node energy consumption is proposed. The paper aims to formulate the topology construction of a swarm network as an optimization problem and solve it using a double-head clustering method that considers group similarity of movement, intra- and inter-cluster distance, node forwarding delay, and energy strategy. The proposed method is designed to be effective in constructing network topologies for large-scale UAV swarm scenarios. In [22], the scalability and performance of SDN-based large-scale Wi-Fi networks are examined. To assess Wi-Fi networks on SDN, the TCP and UDP protocols were used. Using a testbed comprised of Mininet-Wi-Fi and a Ryu Controller, Wi-Fi over SDN and its functionality and scalability were investigated. [23] introduces a mathematical model for P2P networks to study the effect of two different attacks on these systems. In [24], an algorithm that improves compression efficiency by combining CAS map and MAC to remove header bits of CAS map-based compression algorithms is proposed. Using the proposed method shows that the occurrence of compressed messages exceeding 4 bytes is reduced by up to 75.9% compared to the Triple ID method. In [25], a method to compare the OWL-based and XML-based approaches to represent and query cognitive radio capabilities using quantitative metrics is proposed. In order to prove the feasibility and correctness of the method, a proof-of-concept system for the method is developed. Two types of metrics, matching quality metrics and performance metrics, were collected by the system with progressively less complete background knowledge representations and different-sized sets of devices and queries. In [26], the feasibility of Li-Fi communication by considering Red Sea parameters was explored, including a high salinity and growing turbidity. These parameters have a huge impact on blocking the entire Li-Fi communication with little increase. The experimental results show that the Li-Fi signals are affected less by salinity and more by turbidity but are found to be sufficiently strong to be used for communication in the Red Sea. In wireless communications [27], high-security defense systems such as Low Probability of Detection (LPD), Low Probability of Interception (LPI), or Low Probability of Exploitation (LPE) communication algorithms are examined. There is a proposed noise signaling system in the transmission medium that represents a type of security at the physical level that will modify the input/output data that will be conventionally modulated in a noise-like form. In [28], a theoretical study of the numerical calculation of mutual information for finite-alphabet-based transmissions over doubly correlated MIMO fading channels was presented. The main objective was to examine the appropriateness of the saddle point method. The proposed solution gives considerable accuracy in estimating the average mutual information with reduced complexity, which may facilitate the practical application of mutual information. In [29], empirical results of a REM design using interpolating methods are presented. The presented experimentally measured data and their interpretation are important in the context of RF source localization. In [30], a low-complexity NUC demapping algorithm, i.e., the SCSR algorithm, is proposed. SCSR algorithm creates the subsets based on the quadrant of 2D-NUC received symbol or the sign of the I/Q component after 1D-NUC received symbol is decomposed. Moreover, the condensation characteristic is used to further reduce the number of constellation points contained in the

subsets. In [31], a realistic use case for Wi-Fi misbehavior, i.e., BYOD policies with tethering, is considered. The selfish attack considered (CCA modification) is plausible, gives benefits to the attacker, and harms well-behaved users. The presented detection mechanism is based on a well-thought-out observation rule along with a sequential analysis technique to eliminate false alarms. In [32], an algorithm for relay selection in cooperative MIMO networks is presented. In [33], a method of colorizing images obtained in the process of electromagnetic infiltration is presented. In the method for creating LUTs, an exponential function was proposed with parameters that make it possible to change the position of the function course on the axis of pixel amplitude values of the image subjected to colorization and to change its width. Appropriate selection of these parameters makes it possible to expose the appropriate values of the image pixel amplitudes and thus to highlight the important data contained in the image. In [34], an issue related to the correct determination of the number *BCorr* of the reproduced image lines on the basis of the recorded revealing emission signal was presented. Determining the correct *BCorr* value is very important when it is necessary to further process the image using the coherent summation method in order to improve its quality, i.e., improve the signal-to-noise (SNR) parameter. In [35], an issue related to the correct determination of the line length of the reconstructed image on the basis of the recorded revealing emission signal was considered. The correct line length ensures that the graphic elements contained in the image remain vertical. For this purpose, an algorithm for estimating the line length of the reconstructed image was proposed. The algorithm for estimating the line length of the reconstructed image uses three methods of determining the line length of the image for a given accuracy. At the same time, criteria were indicated that must be met to determine the correct length of the image line for the assumed accuracy of estimation. In [36], preliminary results of the analysis of the possibility of using the Fourier and the CZT transforms to determine image rastering parameters in the process of electromagnetic infiltration were presented. Particular attention was paid to the accuracy of determining the line length of the reconstructed image based on the accuracy of determining the value of the horizontal sync frequency of the eavesdropped display. The precision of the determination of the line length of the image is of great importance in the case of further processing of the reconstructed image, e.g., in accordance with the coherent summation algorithm to improve the SNR value.

3. Future

Wireless communications are a constantly developing field. New solutions that increase communication possibilities over longer and longer distances, with higher quality of services, higher speed, and, ultimately, greater reliability, are looked for. All this requires a lot of research, new solutions, and implementation. At the same time, the search for solutions that make people's lives easier must be inextricably linked to ensuring their information security as well as their lives and health. These are challenges for the future on which work must focus. We cannot forget about the possibilities of using artificial intelligence, which is also increasingly boldly entering the area of services provided using wireless communications. Artificial intelligence is also starting to appear in intentional electromagnetic attacks on wireless infrastructure. Graphical display of processed information reconstructed based on revealing emissions is the first level of such attacks. Fast and reliable reproduction of information using electromagnetic fields can become a serious threat. Another interesting area of research is ensuring the cryptographic protection of transmitted information. Quantum cryptology using quantum computers is enjoying great interest. Using such computers, you can quickly perform certain calculations that cannot be performed in real time on ordinary computers based on silicon semiconductors.

As we can see, wireless communication is related to a number of important issues that must be developed in parallel to ensure its security. These are tasks for the future, but not the distant future.

Acknowledgments: First of all, I would like to thank all researchers who submitted articles to this Special Issue for their excellent contributions. I am also grateful to all reviewers who helped in the evaluation of the manuscripts and made very valuable suggestions to improve the quality of the contributions. I would like to acknowledge the editorial board of *Applied Sciences*, who invited me to guest edit this Special Issue. I am also grateful to the *Applied Sciences* Editorial Office staff, who worked thoroughly to maintain the rigorous peer-review schedule and timely publication.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Cirjulina, D.; Babajans, R.; Capligins, F.; Kolosovs, D.; Litvinenko, A. Experimental Study on Colpitts Chaotic Oscillator-Based Communication System Application for the Internet of Things. *Appl. Sci.* **2024**, *14*, 1180. [CrossRef]
2. Roh, S.; Nguyen, T.D.; Lee, J.S. Applications of Nanomaterials in RFID Wireless Sensor Components. *Appl. Sci.* **2024**, *14*, 1216. [CrossRef]
3. Afreen, H.; Kashif, M.; Shaheen, Q.; Alfaifi, Y.H.; Ayaz, M. IoT-Based Smart Surveillance System for High-Security Areas. *Appl. Sci.* **2023**, *13*, 8936. [CrossRef]
4. Almazroi, A.A.; Liaqat, M.; Ali, R.L.; Gani, A. SLMAS: A Secure and Light Weight Mutual Authentication Scheme for the Smart Wheelchair. *Appl. Sci.* **2023**, *13*, 6564. [CrossRef]
5. Martin, R.; Lopez, B.; Vidal, I.; Valera, F.; Nogales, B. Service for Deploying Digital Twins of QKD Networks. *Appl. Sci.* **2024**, *14*, 1018. [CrossRef]
6. Razek, A. Assessment and Categorization of Biological Effects and Atypical Symptoms Owing to Exposure to RF Fields from Wireless Energy Devices. *Appl. Sci.* **2023**, *13*, 1265. [CrossRef]
7. Huang, Y.; Martinez, J.-F.; Diaz, V.H.; Sendra, J. A Novel Topology Control Approach to Maintain the Node Degree in Dynamic Wireless Sensor Networks. *Sensors* **2014**, *14*, 4672–4688. [CrossRef] [PubMed]
8. Chrysikos, T.; Gourna, S.; Skouroliakou, A. RF Coverage Design for the Implementation of a Broadband Monitoring Service in the Context of 5G-Enabled Smart Cities. *Information* **2023**, *14*, 156. [CrossRef]
9. Razaque, A.; Elleithy, K.M. Energy-Efficient Boarder Node Medium Access Control Protocol for Wireless Sensor Networks. *Sensors* **2014**, *14*, 5074–5117. [CrossRef]
10. Anh Le, D.T.; Nguyen, H.; Jang, J.M. An Experimental Demonstration of 2D-Multiple-Input-Multiple- Output-Based Deep Learning for Optical Camera Communication. *Appl. Sci.* **2024**, *14*, 1003. [CrossRef]
11. Alexan, W.; ElBeltagy, M.; Aboshousha, A. RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System. *Symmetry* **2022**, *14*, 443. [CrossRef]
12. Song, I.; Jeon, S.; Kim, D.; Lee, M.G.; Seo, J.T. GENICS: A Framework for Generating Attack Scenarios for Cybersecurity Exercises on Industrial Control Systems. *Appl. Sci.* **2024**, *14*, 768. [CrossRef]
13. Ali, O.; Nguyen, T.-L.; Mohammed, O.A. Assessment of Cyber-Physical Inverter-Based Microgrid Control Performance under Communication Delay and Cyber-Attacks. *Appl. Sci.* **2024**, *14*, 997. [CrossRef]
14. Lopez-Garcia, D.A.; Torreglosa, J.P.; Vera, D.; Sanchez-Raya, M. Binary-Tree-Fed Mixnet: An Efficient Symmetric Encryption Solution. *Appl. Sci.* **2024**, *14*, 966. [CrossRef]
15. Mohsenabad, H.N.; Tut, M.A. Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset. *Appl. Sci.* **2024**, *14*, 1044. [CrossRef]
16. Choi, D.H.; Lee, E.; Yook, J.G. Reconstruction of Video Information Through Leakaged Electromagnetic Waves 523 from Two VDUs Using a Narrow Band-Pass Filter. *IEEE Access* **2022**, *10*, 40307–40315. [CrossRef]
17. Aydın, H. TEMPEST Attacks and Cybersecurity. *Int. J. Eng. Technol.* **2019**, *5*, 552.
18. Zhang, N.; Lu, Y.; Cui, Q.; Wang, Y. Investigation of unintentional video emanations from a VGA connector in the desktop Computers. *IEEE Trans. Electromagn. Compat.* **2017**, *59*, 1826–1834. [CrossRef]
19. Przybysz, A.; Grzesiak, K.; Kubiak, I. Electromagnetic Safety of Remote Communication Devices—Videoconference. *Symmetry* **2021**, *13*, 323. [CrossRef]
20. Han, Y.; Liang, J.; Lin, Y. Joint Deployment Optimization of Parallelized SFCs and BVNFs in Multi-Access Edge Computing. *Appl. Sci.* **2023**, *13*, 7261. [CrossRef]
21. Zhou, R.; Zhang, X.; Song, D.; Qin, K.; Xu, L. Topology Duration Optimization for UAV Swarm Network under the System Performance Constraint. *Appl. Sci.* **2023**, *13*, 5602. [CrossRef]
22. Ali, M.; Jehangiri, A.I.; Alramli, O.I.; Ahmad, Z.; Ghoniem, R.M.; Ala'anzy, M.A.; Saleem, R. Performance and Scalability Analysis of SDN-Based Large-Scale Wi-Fi Networks. *Appl. Sci.* **2023**, *13*, 4170. [CrossRef]
23. Sánchez-Patiño, N.; Gallegos-Garcia, G.; Rivero-Angeles, M.E. Teletraffic Analysis of DoS and Malware Cyber Attacks on P2P Networks under Exponential Assumptions. *Appl. Sci.* **2023**, *13*, 4625. [CrossRef]
24. Piao, J.; Jin, S.; Seo, D.H.; Woo, S.; Chung, J.G. MAC-Based Compression Ratio Improvement for CAN Security. *Appl. Sci.* **2023**, *13*, 2654. [CrossRef]
25. Chen, Y.; Kokar, M.M.; Moskal, J.; Chowdhury, K.R. Metrics-Based Comparison of OWL and XML for Representing and Querying Cognitive Radio Capabilities. *Appl. Sci.* **2022**, *12*, 11946. [CrossRef]

26. Alatawi, A.S. A Testbed for Investigating the Effect of Salinity and Turbidity in the Red Sea on White-LED-Based Underwater Wireless Communication. *Appl. Sci.* **2022**, *12*, 9266. [CrossRef]
27. Choi, J.; Park, D.; Kim, S. Seungyoung Ahn, Implementation of a Noise-Shaped Signaling System through Software-Defined Radio. *Appl. Sci.* **2022**, *12*, 641. [CrossRef]
28. Liu, Y.; Zhang, J.; Zhang, D. Saddle Point Approximation of Mutual Information for Finite-Alphabet Inputs over Doubly Correlated MIMO Rayleigh Fading Channels. *Appl. Sci.* **2021**, *11*, 4700. [CrossRef]
29. Kaniewski, P.; Romanik, J.; Golan, E.; Zubel, K. Spectrum Awareness for Cognitive Radios Supported by Radio Environment Maps: Zonal Approach. *Appl. Sci.* **2021**, *11*, 2910. [CrossRef]
30. Wang, H.; Li, M.; Wang, C. A Universal Low-Complexity Demapping Algorithm for Non-Uniform Constellations. *Appl. Sci.* **2020**, *10*, 8572. [CrossRef]
31. Cho, J. Detection of Misconfigured BYOD Devices in Wi-Fi Networks. *Appl. Sci.* **2020**, *10*, 7203. [CrossRef]
32. Na, Y.-Y.; Lee, W.-S.; Paek, M.-J.; Song, H.-K.; Hwang, D.; You, Y.-H. Adaptive Relay Selection Scheme by Using Compound Channel. *Appl. Sci.* **2020**, *10*, 5614. [CrossRef]
33. Kubiak, I.; Przybysz, A. Pseudo-Coloring as an Effective Tool to Improve the Readability of Images Obtained in an Electromagnetic Infiltration Process. *Appl. Sci.* **2023**, *13*, 9496. [CrossRef]
34. Kubiak, I.; Przybysz, A.; Grzesiak, K. Number of Lines of Image Reconstructed from a Revealing Emission Signal as an Important Parameter of Rasterization and Coherent Summation Processes. *Appl. Sci.* **2023**, *13*, 447. [CrossRef]
35. Kubiak, I.; Przybysz, A. Measurements and Correctness Criteria for Determining the Line Length of the Data Image Obtained in the Process of Electromagnetic Infiltration. *Appl. Sci.* **2022**, *12*, 10384. [CrossRef]
36. Kubiak, I.; Przybysz, A. Fourier and Chirp-Z Transforms in the Estimation Values Process of Horizontal and Vertical Synchronization Frequencies of Graphic Displays. *Appl. Sci.* **2022**, *12*, 5281. [CrossRef]