ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 9, No. 2, 2024

FEATURES OF BUILDING WIRELESS COMPUTER NETWORKS TO INCREASE NOISE IMMUNITY

Mykola Voloshyn, Maksym Oleksiv

Lviv Polytechnic National University, 12, Bandera Str, Lviv, 79013, Ukraine.
Authors' e-mails: mykola.i.voloshyn@lpnu.ua, maksym.v.oleksiv@lpnu.ua

https://doi.org/10.23939/acps2024.02.

Submitted on 10.09.2024

***Abstract*: The paper analyzes existing types of wireless computer networks, technologies, standards, and potential types of interference. Based on this analysis, a classification of wireless information transmission methods has been proposed, taking into account their parameters and task specificity. The primary issues affecting interference resistance in wireless networks have been highlighted. Technical features, advantages, and limitations of each type have been examined, along with their suitability for various scenarios and operational environments. Additionally, the paper offers an overview of innovative trends and emerging research areas aimed at enhancing interference resistance in the rapidly evolving field of wireless network technology.**

***Index Terms*: wireless computer networks, local area network, computer equipment, interference, interference immunity.**

I. INTRODUCTION

Information and communication technologies (ICT) [1] enable processing, reception, and transmission of information between devices and systems over various distances. Wireless computer networks are crucial in ICT, facilitating reliable and efficient communication from personal to large-scale corporate networks.

Advances in bioengineering, nanowire manufacturing, and radio technologies have introduced new paradigms in wireless networks, varying in scalability, size, and environmental placement. This diversity allows tailored applications based on specific needs. Wireless network implementation relies on standards dictating interaction, information transfer protocols, and compatibility. These networks are popular for their ease of deployment and cost-effectiveness but face challenges like interference and security issues. Interference resistance ensures reliable information transmission and is key in network evaluation.

This study aims to analyze wireless network types, unify them by technological and standard-based characteristics, and compare existing interference types to advance wireless network security research.

II. LITERATURE REVIEW OF PROBLEM STATEMENT

Wireless computer networks communicate using micro or radio waves without cables. This technology enhances how information is organized and allows for rapid scaling of existing networks, making it widely used across various business segments, from medicine to the military.

A wireless network comprises hardware and software components. Hardware handles signal transmission, reduces interference, and maintains coverage, while software manages signal formation, amplification, transmission, and ensures information security [2]. It also detects and corrects malfunctions and counters interference. Information security is achieved through data encoding and decoding, preventing unauthorized access. Security protocols, algorithms, and signal modulation provide noise immunity and control internal operations. AI tools enhance these networks, managing tasks like loss prediction, signal spectrum management, content caching, and information processing [3-4].

Typing and classification of wireless networks depend on parameters like transmission method, client distance, and management method. Work [5] classifies networks by location (local, global), management (centralized, decentralized), and organization (selection, routing). Work [6] compares wireless and wired networks on installation, mobility, node visibility, network visibility, speed, bandwidth, and security. Paper [7] categorizes networks by signal range: up to 10 meters (Bluetooth, IrDA, ZigBee, UWB), 100 meters (Wi-Fi), 50 km (WiMAX), and more than 50 km (GCS, GPRS, LTE, UMTS).

The increasing use of embedded wireless systems leads to greater interference and slower data transmission. Urban areas can have multiple Wi-Fi access points within range, while rural areas may have overlapping channels from neighboring access points, slowing data transfers. Additional interference sources include cordless phones, microwave ovens, FCC Part 15 devices, and amateur radio. Research [8] discusses Wi-Fi and Bluetooth protocols, their frequencies, band plans, interference issues, and optimization techniques.

Publications on wireless networks often focus on popular types like Wi-Fi and Bluetooth, with little material on less common networks and their interference mitigation. This highlights the need for further analysis of all wireless network types and continued research to establish stable classification and improve interference immunity. The purpose of this paper is to analyze and

unify known types of wireless networks and their interference immunity methods. This involves a comparative characterization of wireless network types, analysis of technologies used, their inherent interference, and proposing ways to increase interference resistance during deployment.

III. SCOPE OF WORK AND OBJECTIVES

The purpose of this paper is to analyze and unify the known types of wireless networks and the interference immunity methods that are inherent in them. To achieve this, we will divide this task into subtasks. First of all, it is necessary to conduct a comparative characterization of wireless network types and underlying technologies in terms of their physical characteristics and capabilities. Secondly, it is to conduct a comprehensive analysis of the types of technologies used and their inherent interference. And, thirdly, it is to formulate and propose ways to increase interference resistance when deploying wireless networks.

IV. CHARACTERISTICS AND CLASSIFICATION OF WIRELESS NETWORK TECHNOLOGIES

Nanonetworks are short-range networks of nanomachines using electromagnetic and molecular communication. The IEEE P1906.1 standard provides a framework for these communications, including metrics for performance. BitSimulator models wireless nanonetworks using TS-OOK [9-10]. The Internet of Bio-Nano Things (IoNT) uses tiny devices for data collection, benefiting biomedical applications [11-13].

Nanonetworks consist of devices like nanotransmitters, nanoreceivers, nanosensors, nanorobots, nanocontrollers, and nanorouters. Molecular communication is useful where electromagnetic waves are inefficient, but molecular diffusion can cause issues. Fig. 1. illustrates molecular diffusion, where molecules move from a high concentration area to a lower one, spreading randomly and preventing stable transmission.

A Wireless Body Area Network (WBAN) enables users to exchange biosignals via sensor nodes, requiring low power, security, and low latency. The IEEE 802.15.6 standard defines its physical and MAC layers [14-15]. WBANs can cause interference when overlapping, especially when exceeding available frequencies, leading to inter-network interference, as it is shown in Fig. 2.

Wireless Personal Area Network (WPAN) connects devices around a workspace using a wireless medium, like wireless mice, wearables, Bluetooth devices, and security systems. IEEE 802.15.4 forms the basis for the ZigBee protocol [16-17], while IEEE 802.15.1 (Bluetooth) supports wireless connections in a personal workspace [18]. Devices like Bluetooth and IEEE 802.15.4 can interfere with WLANs. Interference can be mitigated by increasing frequency distance or using 5 GHz for WLAN [19].

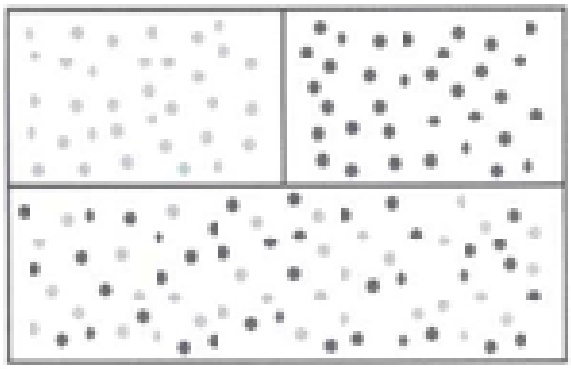

Fig. 1. Molecular diffusion

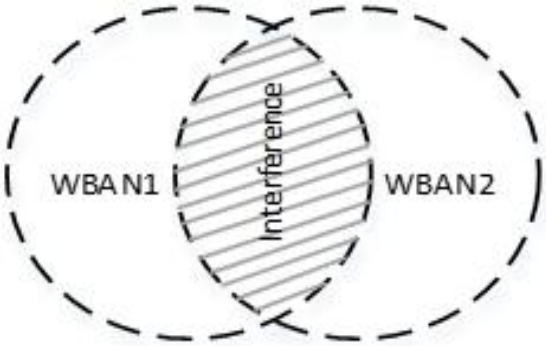

Fig. 2. WBAN interference

A Wireless Local Area Network (WLAN) connects devices within a limited area using Wi-Fi, transmitting IP data. Components include wireless devices, access points, and an Internet provider. WLANs range from a few meters to several hundred meters, affected by router power and environmental interference. WLAN power ranges from 1 to 250 mW, while IEEE 802.15.4 operates at 1 mW, increasing the likelihood of interference. The IEEE 802.15.4 standard recommends low transmit power for WLANs to reduce multi-channel interference. Wi-Fi, based on IEEE 802.11 standards, enables wireless communication via radio waves, facilitating cheaper local network deployment. The latest standard, Wi-Fi 7, is set for implementation in 2024. Wi-Fi interference can weaken signals, leading to slower internet speeds or disconnection, especially in densely populated areas. Types of interference include co-channel interference, neighborhood interference, electromagnetic interference, channel crowding, and physical interference [20].

A Wireless Sensor Network (WSN) consists of sensor nodes monitoring conditions and connecting to a base station for data processing. Applications include IoT, security, and environmental monitoring. WSNs face interference challenges, causing packet loss and instability, mitigated by using shared or unlicensed frequency bands and addressing overlapping channels and environmental barriers.

The general characteristics of the standards under review are shown in Table 1.

Table 1

Features of the IEEE 802 family of standards with a small coverage area

Metrics	Wi-Fi	WSN	BT	Zigbee	WBAN
Physical layer (band)	Narrow	Narrow	Narrow	Narrow	Narrow, broad, on the human body
Freq range (MHz)	869 – 921; 2400; 5000	2400; 5000; 6000	2400	868; 915,5; 2400	402 – 405; 420 – 450; 863 – 870; 902 – 928; 950 – 956; 2360 – 2400; 2400 – 2438,5
Range of action (m)	30	250	10 - 100	75	10
Speed (per sec)	30 Gb (Wi-Fi 7)	250 Kb – 600 Mb	1 Mb	250 Kb	10 Kb – 10 Mb

A Wireless Campus Area Network (WCAN) interconnects WLANs within a campus using switches and routers, offering fast data transfer, security, and cost-effectiveness but facing reliability issues and traffic overlap. WCANs encounter similar interference problems as local networks, including inter-channel interference, environmental barriers, and adjacent frequency use. No separate IEEE standard exists for WCANs, as they combine multiple local networks, mostly Wi-Fi. Examples include Stanford University Network (SUNet) and Google's Googleplex network.

A Wireless Metropolitan Area Network (WMAN) provides city-wide wireless connectivity using technologies like Gigabit Ethernet and Resilient Packet Ring. It includes Backhaul and Last Mile networks, with point-to-point or point-to-multipoint connections. The IEEE 802.16 standard (WirelessMAN) offers broadband access as an alternative to cable and DSL, focusing on the "last mile." WiMAX, a popular protocol under this standard, provides data rates up to 1 Gbps [21].

A Wireless Regional Area Network (WRAN) is designed for rural areas, using unused TV spectrum channels for signal propagation. WRAN needs high performance, efficiency, flexibility, and transmit power control. The IEEE 802.22 standard uses TV broadcast frequencies (54 to 862 MHz) for broadband access in rural areas. It allows license-free use of television frequencies, operating in a Point-to-Multipoint configuration with a coverage radius of 10-100 km. This is beneficial in villages and suburbs due to better transmission at low frequencies. In the U.S., unoccupied TV channels are used, offering economic and technical advantages.

A Wireless Wide Area Network (WWAN) provides coverage over large areas using cellular technologies like 2G, 3G, 4G LTE, and 5G. Advantages include global coverage, cloud management flexibility, security, cost-effective backups, and rapid deployment. WWANs support portable communication, fleet management, public safety, and environmental monitoring. The main disadvantage is environmental influence on RF signals over long distances. WWAN services are typically offered by operators on a paid basis, allowing users with a WWAN adapter to access the Internet, use email, and connect to VPNs within the operator's coverage area. WWAN networks can use packet switching (GPRS) or circuit switching (CSD, HSCSD) and are part of the IEEE 802.16 standard, utilizing GSM and LTE technologies for wide-area coverage [22].

The characteristics of WAN standards are shown in Table 2.

Table 2

Features of the IEEE 802 family of standards with a large coverage area

Parameters	WCAN	WMAN	WRAN	WWAN
Physical layer (band)	Narrow	Broad	Broad	Broad
Freq range (MHz)	2400; 5000	2000 – 11000	54-862	850; 868; 900; 1800; 1900; 2100; 2400
Range of action (km)	1 – 5	5	10 – 100	> 35
Speed (per sec)	3.5 Gb	44 – 155 Mb	114 Kb – 100 Mb	384 Kb – 2 Mb

The first group includes nanonetworks, which involve the implementation of nodes and operation in very small sizes (nanometers) and in specific environments. They are intended for use in bioengineering and help to solve problems at the molecular level.

The next level of classification is conditionally local networks, which are intended for use in relatively small radio. These include standards for human body monitoring (WBAN), personal networks (WPAN), and wide area networks (WLAN). They have different topologies, perform both data selection (structuring) and routing (transmission), but operate within a certain range (from 10 to 250 m).

The last link involves combining types of networks that operate over relatively large areas. These include campus networks (WCANs), city networks (WMANs), regional networks (WRANs), and wide area networks (WWANs). All of them are an amalgamation of groups of local area networks with different standards (or lack thereof). Their radius of operation correlates from 1 to

35 km, but it is not possible to explicitly classify the boundary, as WANs can agglomerate into a large ICT cluster, which helps to cover a very large area.

The general classification based on the analysis of wireless network types and standards is shown in Fig. 3. This classification suggests that existing types of wireless networks can be divided into three general groups.

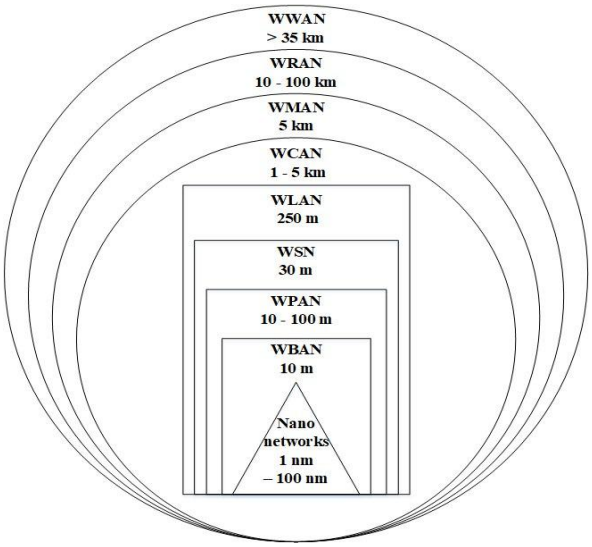

Fig. 3. Classification of wireless network types

V. TYPES OF INTERFERENCE AND MEANS OF IMMUNITY

Interference in wireless computer networks can include physical obstacles like buildings or mountains and electromagnetic interference from radio or television signals. It can also result from competition for resources, such as other wireless networks using the same radio wave band.

Analyzing wireless networks, the common types of interference include co-channel interference, where networks share the same channel; neighborhood interference, from networks using nearby channels; electromagnetic interference from devices like microwaves and Bluetooth; channel congestion in public places; physical obstacles like concrete and metal reducing signal range; and outdated network security tools and firmware causing interference.

Signal propagation is affected by barriers, range, and synchronization. A signal may reach its destination, but if the receiver is not ready, it leads to transmission failures. Lack of synchronization mechanisms can cause data transmission failures and reduce network performance.

Proper synchronization is critical for efficient data transmission and network reliability. Faulty synchronization can cause timing errors, instability, and resource conflicts. Solutions involve developing effective synchronization mechanisms and using precise protocols.

Compatibility is another consideration. Networks must support various devices and standards, including older ones. Wi-Fi, for example, has multiple standards from 802.11 to 802.11be (Wi-Fi 7). Ensuring compatibility across different standards is crucial.

Artificial intelligence (AI) can enhance interference resistance by automating and optimizing network infrastructure. AI can monitor network health, detect malfunctions, predict network load, optimize traffic distribution, resolve network conflicts, manage redundancy, and correct errors. AI can adapt protocols, amplify signals, and reconfigure networks, making this area of research highly relevant as technology evolves.

VI. CONCLUSIONS

Various types of wireless computer networks, comparing technologies and standards were analyzed in the paper. Wireless networks by coverage radius and examines their advantages, disadvantages, and interference issues were classified. Common interference types included inter-channel, inter-band, standards conflicts, and environmental factors. To improve interference immunity, it recommended increasing the distance between networks, using different frequencies and channels, increasing the number of nodes, and considering the deployment environment. These methods were mostly applicable to simple network deployments.

Additional methods for improving interference resistance included synchronizing nodes and users, multiplexing different wireless network standards for better interoperability, and using AI to enhance interference resistance. Future research would focus on synchronization in wireless networks, analyzing interoperability mechanisms, and applying AI to minimize interference and increase noise immunity.

References

[1] L. Stosic, S. Dermendzhieva, L. Tomczyk (2020). "Information and communication technologies as a source of education," *World Journal on Educational Technology: Current Issues, 12*(2), 128-135. DOI: https://doi.org/10.18844/wjet.v12i2.4815.

[2]Pundalik Chavan, Anooja Ali, Ramaprasad H C, Ramachandra H V, Hari Krishna H, & E G Satish. (2023). Analysis of Wireless Networks: Successful and Failure Existing Technique. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (Eds.), *Data Science and Intelligent Computing Techniques* (pp. 877-891). SCRS, India. DOI: https://doi.org/10.56155/978-81-955020-2-8-75.

[3] L. Wu et al. (2020). Artificial Neural Network Based Path Loss Prediction for Wireless Communication Network. *IEEE Access, 8*, 199523-199538. DOI: https://doi.org/10.1109/ACCESS.2020.3035209.

[4] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, & X. Li. (2023). A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications. *IEEE Communications Surveys & Tutorials, 25*(4), 2494-2528. DOI: https://doi.org/10.1109/COMST.2023.3315374.

[5]Tarnavskyi Y. A., Kuzmenko I. M. Organisation of computer networks. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2018, p. 259. Available at: https://ela.kpi.ua/server/api/core/bitstreams/e0a0c843-a57d-4d82-8f42-0eba294bef1f/content (Accessed: 10/14/2024).

[6] Shukla, S., Meghana, K.M., Manjunath, C.R., & Shantosh, N. (2017). Comparison of Wireless Network over Wired Network and Its Type. *Int. J. Res. Granthaalayah, 5*, 14-20. DOI: https://doi.org/10.5281/zenodo.572289.

[7] Jordi Salazar. Wireless networks. Czech Technical University of Prague. Faculty of electrical engineering. ISBN: 978-80-01-06197-8 (Online), 2017. [Electronic resource]. – Available at: https://upcommons.upc.edu/bitstream/handle/2117/110811/LM01_F_EN.pdf (Accessed: 10/14/2024).

[8] Wireless Network Interference and Optimization. [Electronic resource]. – Available at: https://interferencetechnology.com/wireless-network-interference-and-optimization/ (Accessed: 10/14/2024).

[9] User's and developer's manual of BitSimulator. [Electronic resource]. – Available at: http://eugen.dedu.free.fr/bitsimulator/manual.pdf (Accessed: 10/14/2024).

[10] H. Mabed. (2017). Enhanced spread in time on-off keying technique for dense Terahertz nanonetworks. In *2017 IEEE Symposium on Computers and Communications (ISCC),* Heraklion, Greece, 710-716. DOI: https://doi.org/10.1109/ISCC.2017.8024611.

[11] Yeh, T.-CJ., Dong, Y., & Ye, S. (2023). Molecular Diffusion. In *An Introduction to Solute Transport in Heterogeneous Geologic Media* (pp. 93-122). Cambridge University Press. DOI: https://doi.org/10.1017/9781009049511.005.

[12] J. Wang, X. Liu, M. Peng, & M. Daneshmand. (2020). Performance Analysis of D-MoSK Modulation in Mobile Diffusive-Drift Molecular Communications. *IEEE Internet of Things Journal, 7*(11), 11318-11326. DOI: https://doi.org/10.1109/JIOT.2020.2997372.

[13] B. C. Akdeniz, A. E. Pusane, & T. Tugcu. (2018). Position-based modulation in molecular communications. *Nano Communication Networks, 16*, 60-68. DOI: https://doi.org/10.1016/j.nancom.2018.01.004.

[14] M. Hernandez, R. Kohno, T. Kobayashi, & M. Kim. (2022). New Revision of IEEE 802.15.6 Wireless Body Area Networks. *2022 IEEE 16th International Symposium on Medical Information and Communication Technology (ISMICT)*, Lincoln, NE, USA, 1-5. DOI: https://doi.org/10.1109/ISMICT56646.2022.9828139.

[15] Park, K., Baek, J., Kim, S., Jeong, M., & Kim, Y. (2019). Touch-Based Dual-Band System Combined Human Body Communication and Wireless LAN for Wearable Devices. *Electronics, 8*, 335. DOI: https://doi.org/10.3390/electronics8030335.

[16] N. Choudhury, R. Matam, M. Mukherjee, & J. Lloret. (2020). A Performance-to-Cost Analysis of IEEE 802.15.4 MAC With 802.15.4e MAC Modes. *IEEE Access, 8*, 41936-41950. DOI: https://doi.org/10.1109/ACCESS.2020.2976654.

[17] Telecommunications Signals & Systems Lab Equipment. [Electronic resource]. – Available at: https://tecnoedu.com/Download/Emona-TIMS-curriculum background-r1.pdf (Accessed: 10/14/2024).

[18] D. Verma et al. (2020). A Design of 8 fJ/Conversion-Step 10-bit 8MS/s Low Power Asynchronous SAR ADC for IEEE 802.15.1 IoT Sensor Based Applications. *IEEE Access, 8*, 85869-85879. DOI: https://doi.org/10.1109/ACCESS.2020.2992750.

[19] DongFeng Fang, Yi Qian, & Rose Qingyang Hu. (2024). Introduction to 5G Wireless Systems. In *5G Wireless Network Security and Privacy* (pp. 1-6). IEEE. DOI: https://doi.org/10.1002/9781119784340.ch1.

[20] C. Deng et al. (2020). IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities. *IEEE Communications Surveys & Tutorials, 22*(4), 2136-2166. DOI: https://doi.org/10.1109/COMST.2020.3012715.

[21] Behnam Kamali. (2018). The IEEE 802.16 Standards and the WiMAX Technology. In *AeroMACS: An IEEE 802.16 Standard-Based Technology for the Next Generation of Air Transportation Systems* (pp. 189-258). IEEE. DOI: https://doi.org/10.1002/9781119281139.ch5.

[22] D. M. Molla, H. Badis, L. George, & M. Berbineau. (2022). Software Defined Radio Platforms for Wireless Technologies. *IEEE Access, 10*, 26203-26229. DOI: https://doi.org/10.1109/ACCESS.2022.3154364.

Mykola Voloshyn is a master's degree graduate of the Department of Electronic Computers at Lviv Polytechnic National University. In 2022, he received a Master's degree in Computer Systems and Networks, Department of Electronic Computers. In 2020, he received a bachelor's degree in Computer Engineering, Department of Specialized Computer Systems. He is currently working on his PhD in Computer Engineering.

Maksym V. Oleksiv is a PhD candidate at the Department of Electronic Computers, Institute of Computer Technology, Automation and Metrology, Lviv Polytechnic National University. He received his PhD in Computer Systems and Components at Lviv Polytechnic National University in 2012.

Research interests: research of heterogeneous computing systems, artificial intelligence, digital signal and image processing, development and testing of hardware and software systems.