International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 6, Nov – Dec 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Wireless Communication Networks: Applications, Security Challenges, and Emerging Technologies

Chandrappa D N[1], Kavitha L[2]
[1]Department of Electronics and Communication Engineering, East Point College of Engineering & Technology, Bangalore, Karnataka, India
[2]Department of Mathematics, School of Applied Sciences, REVA University, Bangalore, Karnataka, India

----------**********----------

Abstract:
Wireless communication networks have become an essential part of modern communication infrastructure, providing flexible, mobile, and ubiquitous connectivity without physical cables. This paper presents a comprehensive overview of wireless communication networks, focusing on their evolution, major communication systems, applications, security challenges, and emerging technologies. The study reviews the historical development of wireless communication from early radio transmission and satellite communication to WLAN, Wi-Fi, Bluetooth, and successive generations of cellular networks from 1G to 5G, with 6G identified as an emerging direction. Different wireless communication systems, including radio, microwave, Wi-Fi, Bluetooth, cellular, satellite, RFID, NFC, infrared, and UAV-based communication, are examined with respect to their characteristics and applications. The paper also analyzes major security concerns arising from the open nature of wireless communication, including eavesdropping, unauthorized access, denial-of-service attacks, man-in-the-middle attacks, jamming, interference, data modification, and privacy violations. Security requirements and countermeasures such as confidentiality, integrity, authentication, encryption, access control, and intrusion detection are discussed. Finally, future developments involving 6G, artificial intelligence, machine learning, IoT, edge computing, UAVs, intelligent wireless technologies, and advanced security mechanisms are considered. The study emphasizes the need for wireless networks that are secure, reliable, scalable, energy-efficient, and capable of supporting the rapidly increasing number of connected devices and applications. Overall, the paper provides a consolidated understanding of the development, current challenges, and future directions of wireless communication networks.

Keywords: Wireless Communication Networks; Wireless Technologies; Network Security; 5G; Internet of Things (IoT); UAV Communication; Wi-Fi; Bluetooth; Cellular Networks; Emerging Technologies.

----------**********----------

Introduction:

Wireless communication networks have become a fundamental component of modern information and communication technology, providing ubiquitous connectivity for users, machines, sensors, vehicles, and intelligent devices. The rapid evolution from conventional cellular networks to 5G has significantly improved data rates, network capacity, reliability, and latency while enabling large-scale connectivity for emerging applications. The continuous growth of connected devices and data-intensive applications has, however, created new requirements that extend beyond the capabilities of existing 5G networks, motivating extensive research toward sixth-generation (6G) wireless communication systems [1]–[3]. Recent studies describe 6G as a technology platform intended to support highly intelligent, heterogeneous, and globally connected environments through advanced radio access technologies, artificial intelligence (AI), terahertz communication, and integrated terrestrial and non-terrestrial networks [1]–[4].

 ©IJSRED: All Rights are Reserved

The development of next-generation wireless networks is being driven by the increasing demand for high-speed communication, ultra-low latency, massive connectivity, improved reliability, and intelligent network management. Recent research indicates that 6G networks are expected to integrate technologies such as massive multiple-input multiple-output (MIMO), millimetre-wave and terahertz communication, intelligent network automation, machine learning, edge computing, and Internet of Things (IoT) connectivity [1], [2], [5]. In addition, emerging 6G architectures are expected to support diverse applications including smart healthcare, intelligent transportation, Industry 5.0, virtual and augmented reality, autonomous systems, and large-scale IoT services [3], [4].

The Internet of Things is one of the major application domains influencing the evolution of wireless communication networks. IoT systems connect large numbers of heterogeneous and resource-constrained devices that continuously exchange sensing and control information. The increasing scale of IoT deployments introduces challenges related to communication efficiency, scalability, privacy, security, and resource management [12]–[16]. Recent studies have investigated intelligent IoT architectures that combine wireless communication with edge computing, machine learning, blockchain, and distributed intelligence to provide more efficient and secure services [13], [16]. Such developments are particularly important for smart cities, industrial automation, healthcare, transportation, energy systems, and other cyber-physical applications.

Security has become one of the most critical challenges in modern wireless communication networks. The open nature of wireless channels makes networks vulnerable to eavesdropping, jamming, spoofing, denial-of-service attacks, unauthorized access, privacy violations, and other cyber threats. The increased use of virtualization, network slicing, IoT devices, edge computing, and AI-based network management further expands the attack surface [8]–[11]. A recent systematic survey of 5G and 6G security identified confidentiality, integrity, availability, privacy, authentication, and access control as important requirements for next-generation networks [8]. Similarly, research on 5G network slicing has identified numerous security threats associated with slice deployment, activation, operation, resource sharing, and isolation, demonstrating the need for comprehensive security frameworks [9].

Physical-layer security is also receiving increasing attention because wireless communication is inherently exposed to the propagation environment. Recent research has examined physical-layer security mechanisms for 5G and 6G systems to protect communication against eavesdropping, jamming, and other attacks [10], [11]. Artificial intelligence and machine learning are increasingly being investigated as tools for improving security by enabling intelligent detection of anomalous behaviour, adaptive resource allocation, attack identification, and dynamic security management [2], [10]. Furthermore, blockchain-based mechanisms have been explored for 6G networks because their decentralized and tamper-resistant characteristics can support authentication, trust management, access control, and secure resource sharing [11].

Another important development is the integration of wireless networks with unmanned aerial vehicles (UAVs). UAVs can act as mobile communication platforms, aerial base stations, sensing devices, and computing nodes. Their mobility and flexible deployment make them useful for surveillance, disaster management, logistics, agriculture, infrastructure monitoring, and emergency communication. However, UAV networks introduce additional challenges related to mobility, energy limitations, communication reliability, privacy, authentication, and cyber security [5], [6], [21]. Recent studies have investigated secure communication mechanisms for IoT-based UAV networks and have identified threats such as jamming, eavesdropping, spoofing, and attacks on UAV-to-ground communication [21]. AI-based approaches are also being explored to improve UAV security through intelligent attack detection and prevention [22].

Edge computing and mobile edge computing (MEC) have emerged as important technologies for reducing communication latency and supporting computation-intensive applications in 5G and beyond-5G networks. By moving computational resources closer to end users, MEC can reduce

 ©IJSRED: All Rights are Reserved

transmission delays, energy consumption, and dependence on centralized cloud infrastructure [17], [18]. Recent research has investigated task offloading, resource allocation, and intelligent computation strategies for MEC systems, particularly for IoT and latency-sensitive applications [17]. UAV-enabled MEC further combines aerial communication, edge computing, and wireless connectivity to provide flexible computational services in dynamic environments [18].

Ultra-reliable low-latency communication (URLLC) is another important research direction for 5G and 6G networks. URLLC is designed to support applications requiring extremely high reliability and very low communication latency, including industrial automation, intelligent transportation, smart grids, and mission-critical systems. Recent studies have investigated AI/ML-based resource allocation, multi-access techniques, beamforming, and massive MIMO as mechanisms for improving the capacity and reliability of URLLC services [19].

Sustainability and energy efficiency are also becoming increasingly important as wireless networks continue to expand. The growth of IoT devices, edge computing infrastructure, and intelligent communication systems can significantly increase energy consumption and carbon emissions. Recent research has therefore focused on green communication, energy-efficient architectures, renewable energy integration, and sustainable Internet-of-Everything (IoE) systems for future 6G networks [20]. At the same time, emerging research on quantum computing, federated learning, and 6G networks has explored new approaches for improving IoT security and privacy while maintaining distributed learning and data protection [12].

Therefore, wireless communication networks are undergoing a major transformation from conventional connectivity-oriented systems toward intelligent, secure, distributed, and application-driven communication infrastructures. The convergence of 5G, 6G, IoT, AI, edge computing, UAVs, blockchain, and advanced security technologies provides significant opportunities for future applications but also introduces new technical and research challenges [1]–[22].

This paper presents a comprehensive review of wireless communication networks, their applications, security challenges, and emerging technologies. The study examines the evolution and characteristics of modern wireless networks, major application areas, security and privacy challenges, and emerging technologies associated with 5G and 6G systems. Particular attention is given to IoT, UAV communication, AI-enabled wireless networks, edge computing, network slicing, physical-layer security, and sustainable communication. Finally, the paper identifies important research challenges and future directions for developing secure, reliable, scalable, intelligent, and energy-efficient wireless communication networks.

History of Wireless Communication Networks

The history of wireless communication networks represents a continuous development from basic radio transmission to highly advanced cellular and intelligent wireless networks. Wireless communication refers to the transmission of information between two or more devices without the use of physical wires or cables. Instead, electromagnetic waves, including radio, microwave, infrared, and other frequency bands, are used to carry information through space [1]. The development of wireless communication has played an important role in transforming telecommunications, computer networking, mobile computing, and Internet connectivity.

Early Development of Wireless Communication

The foundations of wireless communication were established through the development of electrical and electromagnetic theories during the seventeenth to nineteenth centuries. Theoretical developments in electromagnetism provided the basis for understanding the generation and propagation of electromagnetic waves. During the late nineteenth century, experiments by researchers and inventors such as Nikola Tesla and Guglielmo Marconi contributed significantly to the development of practical radio communication [1]. Marconi's successful transmission of wireless signals over long distances, including across the Atlantic Ocean,

 ©IJSRED: All Rights are Reserved

demonstrated that information could be transmitted without physical communication cables [1].

During the early twentieth century, radio communication became increasingly important for broadcasting, maritime communication, military communication, and other long-distance applications. The development of radio technology established the fundamental concept of transmitting information through electromagnetic waves and provided the technological foundation for subsequent wireless communication networks.

Development of Radio, Microwave, and Satellite Communication

During the 1920s, commercial radio broadcasting expanded and enabled information, news, and entertainment to be distributed to large populations. During the 1940s, microwave communication technology enabled the use of higher-frequency radio transmission and contributed to the development of long-distance communication systems. Satellite communication subsequently became an important technology for providing communication over large geographical areas [1].

The launch of Sputnik 1 in 1957 represented an important milestone in satellite communication. Since then, satellites have become an important component of global communication systems, supporting communication over areas where terrestrial infrastructure may be difficult to deploy [1]. Satellite-based wireless communication continues to be useful for navigation, broadcasting, remote communication, and connectivity in geographically isolated regions.

Development of Wireless Local Area Networks

Another important stage in the history of wireless networking was the development of wireless local area networks (WLANs). In 1971, researchers at the University of Hawaii developed ALOHNET, an early packet-based radio communication network consisting of seven computers communicating through a bidirectional star topology [2]. This development demonstrated the feasibility of using radio communication for computer networking.

During the 1990s, the Institute of Electrical and Electronics Engineers (IEEE) established the IEEE 802.11 Working Group to develop standards for wireless local area networks. In 1997, IEEE 802.11 was approved as an early WLAN standard, supporting wireless data communication in the 2.4 GHz industrial, scientific, and medical (ISM) band [2].

The development of WLAN technologies led to the widespread adoption of Wi-Fi. Wi-Fi enabled computers, smartphones, and other devices to connect to local networks and the Internet without physical cables. This significantly improved mobility and simplified network installation in homes, offices, universities, airports, hotels, and other public environments [1], [2].

Evolution of Cellular Wireless Networks

The development of cellular networks represented one of the most significant advances in wireless communication. A cellular network divides a geographical area into multiple cells, with each cell served by a base station. Frequency reuse between cells allows a large number of users to communicate while making efficient use of the available radio spectrum [2].

The evolution of cellular communication is commonly described through several generations:

1G – First Generation

The first generation (1G) of cellular networks introduced analog mobile communication primarily for voice services. These systems provided users with mobility but had limitations in terms of capacity, security, spectrum efficiency, and communication quality. Nevertheless, 1G established the foundation for modern mobile communication networks.

2G – Second Generation

The second generation (2G) introduced digital cellular communication. Compared with 1G, 2G provided improved voice quality, greater capacity, better spectrum utilization, and additional services such as text messaging. Digital communication also provided improved opportunities for implementing security mechanisms.

3G – Third Generation

The third generation (3G) introduced significantly improved mobile data capabilities. Wireless networks were no longer limited primarily to voice communication and began supporting Internet access, multimedia applications, video communication, and other data-intensive services. This period contributed significantly to the transformation of mobile phones into

 ©IJSRED: All Rights are Reserved

multifunctional communication and computing devices.

4G – Fourth Generation

The fourth generation (4G) represented a major transition toward high-speed mobile broadband and Internet Protocol (IP)-based communication. Technologies such as Long-Term Evolution (LTE) provided higher data rates and improved network performance. 4G enabled applications such as high-quality video streaming, mobile cloud services, online gaming, video conferencing, and large-scale mobile Internet access.

5G – Fifth Generation

The fifth generation (5G) introduced significant improvements in data rate, latency, reliability, network capacity, and device connectivity. The technology was designed not only for enhanced mobile broadband but also for mission-critical communication and massive Internet of Things (IoT) connectivity [1]. The uploaded literature identifies 5G as an important development capable of supporting high data speeds, reduced latency, improved reliability, and a large number of interconnected devices.

5G has consequently expanded wireless communication beyond conventional smartphone connectivity toward applications such as industrial automation, smart cities, autonomous transportation, healthcare, augmented reality, virtual reality, and IoT systems.

Emergence of IoT and Advanced Wireless Networks

The increasing number of connected devices has led to the emergence of the Internet of Things. IoT connects physical objects, sensors, machines, vehicles, and other smart devices so that they can exchange information through communication networks. Wireless technologies are particularly important for IoT because many IoT devices require flexible and low-power connectivity.

Wireless communication has also become an important foundation for smart-city applications. Wireless networks can support services involving transportation, environmental monitoring, public safety, automation, surveillance, and efficient management of urban infrastructure [2].

UAV-Based Wireless Communication

More recently, wireless communication has been extended to unmanned aerial vehicle (UAV) networks. UAVs can be used as communication platforms, mobile sensing devices, or aerial base stations. Their high mobility and flexible deployment make them suitable for applications such as surveillance, disaster management, navigation, environmental monitoring, and communication coverage [3].

UAV communication networks introduce new requirements for reliable connectivity, efficient path planning, energy management, security, and privacy. Research has identified the integration of UAVs with IoT, as well as communication among UAVs, satellites, and ground stations, as promising directions for future wireless networks [3].

Future Evolution Toward 6G

The current development of wireless communication is moving beyond 5G toward sixth-generation (6G) networks. Future wireless systems are expected to provide higher capacity, lower latency, improved energy efficiency, intelligent network management, and support for extremely large numbers of connected devices. Artificial intelligence, machine learning, advanced IoT, edge computing, satellite communication, and intelligent wireless technologies are expected to play important roles in future networks.

The evolution of wireless communication can therefore be summarized as a transition from basic radio communication to digital wireless networks, mobile cellular systems, broadband 4G/5G networks, and intelligent future 6G networks. Each generation has introduced new capabilities to overcome the limitations of previous systems and to meet the growing requirements of users and connected devices.

Overall, the history of wireless communication networks demonstrates a continuous progression toward higher data rates, greater mobility, improved reliability, lower latency, increased connectivity, and intelligent network operation. The development from early radio systems to 5G and emerging 6G technologies has established wireless communication as a fundamental infrastructure for modern digital society.

 ©IJSRED: All Rights are Reserved

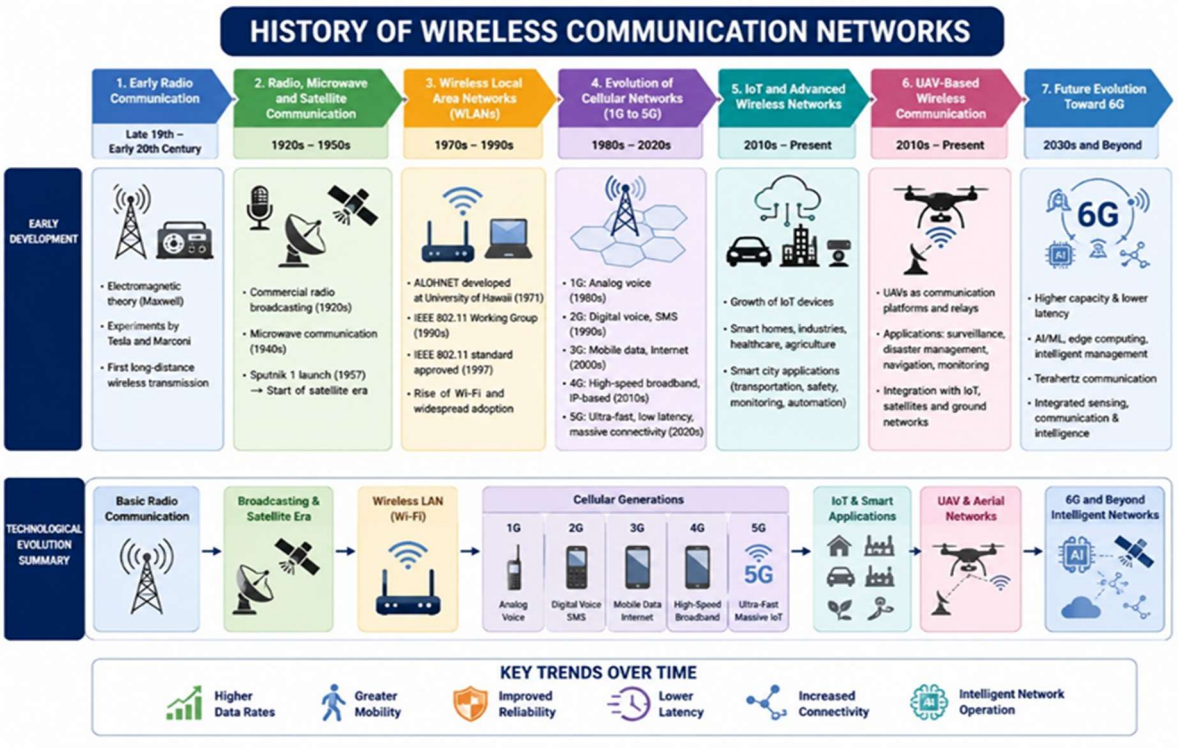


Figure 1: History of wireless communication network

Types of Wireless Communication Systems and Their Frequency Ranges

Wireless communication systems use electromagnetic waves to transmit information without physical cables. Different wireless technologies operate over different frequency ranges depending on their applications, coverage, bandwidth, and propagation characteristics. The major types of wireless communication systems are summarized below.

Radio Communication

Radio communication is one of the oldest forms of wireless communication. It uses electromagnetic waves to transmit information through free space. Radio-frequency communication is used in broadcasting, navigation, military systems, mobile communication, and many other applications.

Microwave Communication

Microwave communication uses relatively high-frequency electromagnetic waves and is commonly used for point-to-point communication. In the literature you provided, terrestrial microwave systems are described as typically operating around 4–6 GHz, while satellite systems are described around 11–14 GHz in the specific example given. Microwave links generally require a relatively clear line of sight between transmitting and receiving antennas.

Wi-Fi

Wi-Fi is a low-power wireless networking technology used to connect computers, smartphones, laptops, and other devices. Your source describes Wi-Fi as a common wireless technology in which a router acts as a communication hub.

Common Wi-Fi frequency bands are:

- 2.4 GHz
- 5 GHz
- 6 GHz

The 2.4 GHz band is particularly important because it is also used by Bluetooth, which can result in interference when both systems operate simultaneously.

Bluetooth

Bluetooth is designed primarily for short-range wireless communication between electronic devices such as smartphones, headphones, keyboards, mice, and other peripherals. Your source specifically describes Bluetooth as operating in the 2.4 GHz band.

 ©IJSRED: All Rights are Reserved

Cellular Communication

Cellular communication provides wide-area wireless connectivity through geographically divided cells. Mobile networks have evolved through several generations:

1G → 2G → 3G → 4G → 5G → 6G (emerging)

The exact frequency depends on the country, operator, and cellular generation. Modern 5G networks can operate in low-band, mid-band, and high-band/mmWave spectrum.

Satellite Communication

Satellite communication uses satellites as relay stations between ground-based transmitters and receivers. It is particularly useful for long-distance and global communication. The source you provided gives an example of satellite communication using 11–14 GHz, with terrestrial microwave communication typically using 4–6 GHz.

RFID

Radio Frequency Identification (RFID) uses radio waves to identify and track objects using tags and readers. It is widely used in inventory management, logistics, access control, libraries, and supply chains.

NFC

Near Field Communication (NFC) is a very short-range wireless technology operating at 13.56 MHz It is commonly used for contactless payments, access cards, identification, and short-range data exchange.

Infrared Communication

Infrared communication uses electromagnetic radiation above the microwave range and below visible light. It is commonly used for short-distance applications such as television remote controls and some sensor and communication systems.

UAV Wireless Communication

UAVs can communicate with ground stations, other UAVs, satellites, and IoT devices using different wireless technologies. UAV communication requires reliable connectivity because UAVs have high mobility and may operate in dynamic environments. Research identifies communication, energy efficiency, security, privacy, and integration with IoT as important UAV-network challenges.

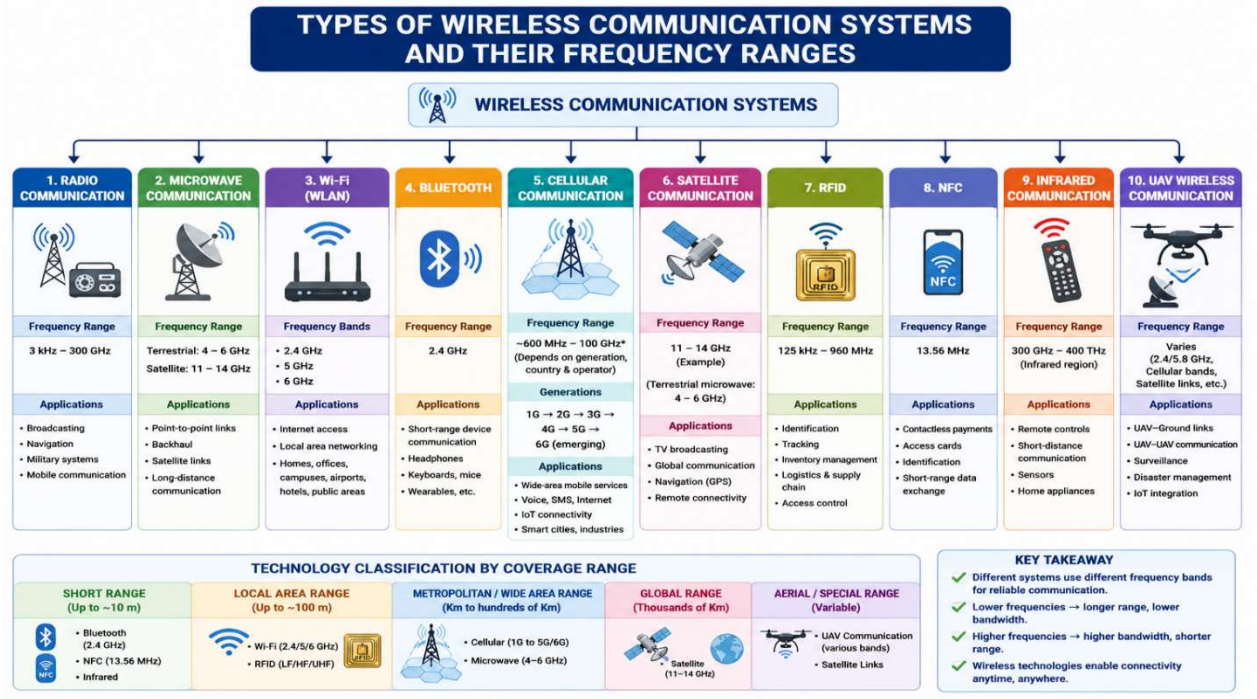


Figure 2: Types of Wireless communication system

 ©IJSRED: All Rights are Reserved

Wireless Communication Security

Wireless communication security is an important aspect of modern wireless networks because information is transmitted through an open and shared medium rather than through protected physical cables. Wireless networks provide mobility, flexibility, and easy deployment, but the open nature of radio transmission also makes them vulnerable to unauthorized access, eavesdropping, interference, data interception, and other security threats.

Security Requirements in Wireless Networks

The primary objective of wireless communication security is to protect information and network resources from unauthorized users and malicious activities. The major security requirements include:

Confidentiality

Confidentiality ensures that transmitted information can only be accessed by authorized users. Since wireless signals can potentially be intercepted while propagating through the air, encryption is required to prevent attackers from understanding captured data.

Integrity

Integrity ensures that transmitted information is not modified, manipulated, or corrupted by unauthorized users during communication. Authentication mechanisms and cryptographic techniques can be used to verify the validity of transmitted information.

Authentication

Authentication verifies the identity of users and devices before allowing them to access a wireless network. Strong authentication helps prevent unauthorized devices from joining the network.

Availability

Availability ensures that wireless network services remain accessible to legitimate users. Wireless systems can be affected by interference and deliberate attacks such as denial-of-service (DoS) and jamming. UAV communication networks, for example, are identified as being vulnerable to DoS, eavesdropping, and other malicious attacks.

Privacy

Privacy protects sensitive information about users, devices, locations, and communication activities. This is particularly important in IoT, mobile, UAV, and smart-city environments where large amounts of personal and operational data may be transmitted wirelessly.

Major Security Threats

Eavesdropping

Eavesdropping occurs when an unauthorized person intercepts wireless signals to obtain transmitted information. Because wireless communication uses the open air as the transmission medium, an attacker may attempt to capture communication without having physical access to network cables.

Denial-of-Service Attack

A Denial-of-Service (DoS) attack attempts to make network resources unavailable to legitimate users. In wireless networks, attackers can generate excessive traffic or interfere with communication channels, preventing normal communication. DoS attacks are specifically identified as a threat in UAV communication networks.

Man-in-the-Middle Attack

In a man-in-the-middle attack, an attacker attempts to position themselves between two communicating devices and intercept or manipulate their communication. Secure authentication and encryption are important mechanisms for reducing this risk.

Unauthorized Access

Unauthorized access occurs when an attacker obtains access to a wireless network without permission. Weak passwords, poor authentication mechanisms, and improperly configured wireless devices can increase this risk.

Signal Interference

Interference occurs when unwanted radio signals affect legitimate wireless communication. For example, Wi-Fi and Bluetooth can operate in the 2.4 GHz band, creating the possibility of interference when both technologies are operating simultaneously.

Jamming

Jamming deliberately introduces radio-frequency interference into a communication channel. This can reduce communication quality or completely prevent legitimate devices from communicating.

 ©IJSRED: All Rights are Reserved

Wireless Network Security Mechanisms

Several mechanisms can be used to improve the security of wireless communication networks.

Encryption: Converts transmitted information into a protected form so that intercepted data cannot easily be understood by unauthorized users.

Authentication: Verifies the identity of users and devices before granting network access.

Access Control: Restricts network resources to authorized users and devices.

Intrusion Detection and Prevention: Wireless intrusion detection and prevention systems can identify suspicious activities and alert network administrators when security breaches occur.

Secure Wireless Protocols: Security standards and protocols can provide protection for wireless communication. The uploaded literature identifies WEP and WPA among wireless security standards.

Security in Emerging Wireless Networks

Security becomes increasingly complex as wireless networks integrate 5G, IoT, UAVs, edge computing, and future 6G technologies. IoT environments may contain a very large number of resource-constrained devices, increasing the potential attack surface. UAV networks introduce additional security and privacy requirements because UAVs operate over open wireless links and communicate with other UAVs, ground stations, satellites, and IoT devices.

Future wireless networks therefore require security mechanisms that are scalable, adaptive, intelligent, energy-efficient, and capable of protecting both communication data and network infrastructure.

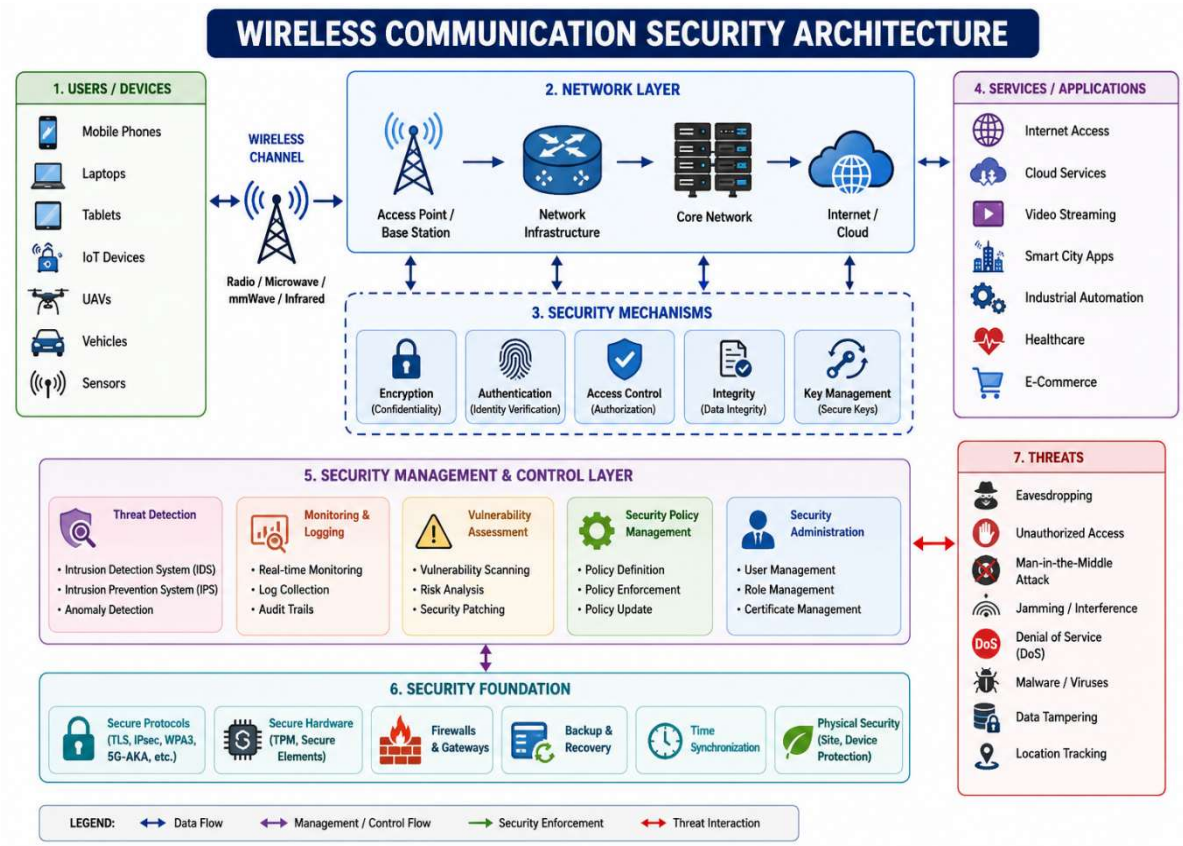


Figure 3: Wireless Communication Security Architecture

 ©IJSRED: All Rights are Reserved

Table 1: Major Wireless Security Threats and Countermeasures

Security Threat	Main Problem	Possible Countermeasure
Eavesdropping	Unauthorized interception	Encryption
DoS attack	Network service disruption	Intrusion detection, traffic filtering
Man-in-the-middle	Communication interception/manipulation	Strong authentication, encryption
Unauthorized access	Access by illegitimate users	Authentication and access control
Jamming	Radio-frequency interference	Anti-jamming techniques
Data modification	Loss of data integrity	Integrity verification, cryptography
Privacy violation	Exposure of sensitive information	Encryption and privacy mechanisms
Signal interference	Communication degradation	Frequency/channel management
Malicious UAV attacks	Threats to UAV communication	Secure authentication and encryption

Future of Wireless Communication Networks

The future of wireless communication networks is expected to move beyond conventional connectivity toward intelligent, secure, reliable, and highly efficient communication systems. The development of sixth-generation (6G) networks is expected to provide higher data rates, ultra-low latency, massive connectivity, improved reliability, and intelligent network management. Emerging technologies such as artificial intelligence (AI), machine learning (ML), terahertz (THz) communication, edge computing, intelligent reflecting surfaces, and integrated sensing and communication are expected to play important roles in future wireless networks. AI and ML can enable autonomous network optimization, intelligent resource allocation, traffic prediction, anomaly detection, and improved security. THz communication is being investigated to provide extremely high bandwidth and support data-intensive applications, while edge computing can reduce latency by processing information closer to end users. The future wireless ecosystem is also expected to integrate terrestrial networks with UAVs, satellites, and other non-terrestrial networks to provide ubiquitous connectivity, particularly in remote and disaster-affected areas. At the same time, the rapid growth of IoT devices will require wireless networks to support massive connectivity while maintaining energy efficiency, privacy, and security. Future networks will therefore need advanced encryption, authentication, intrusion detection, privacy protection, and intelligent security mechanisms to address increasingly sophisticated cyber threats. Overall, wireless communication is expected to evolve toward an intelligent and integrated infrastructure that combines communication, sensing, computing, and AI, supporting applications such as smart cities, autonomous transportation, healthcare, industrial automation, UAV systems, and the Internet of Things. Recent research identifies these technologies as important directions for the evolution of 6G and beyond-6G wireless networks.

 ©IJSRED: All Rights are Reserved

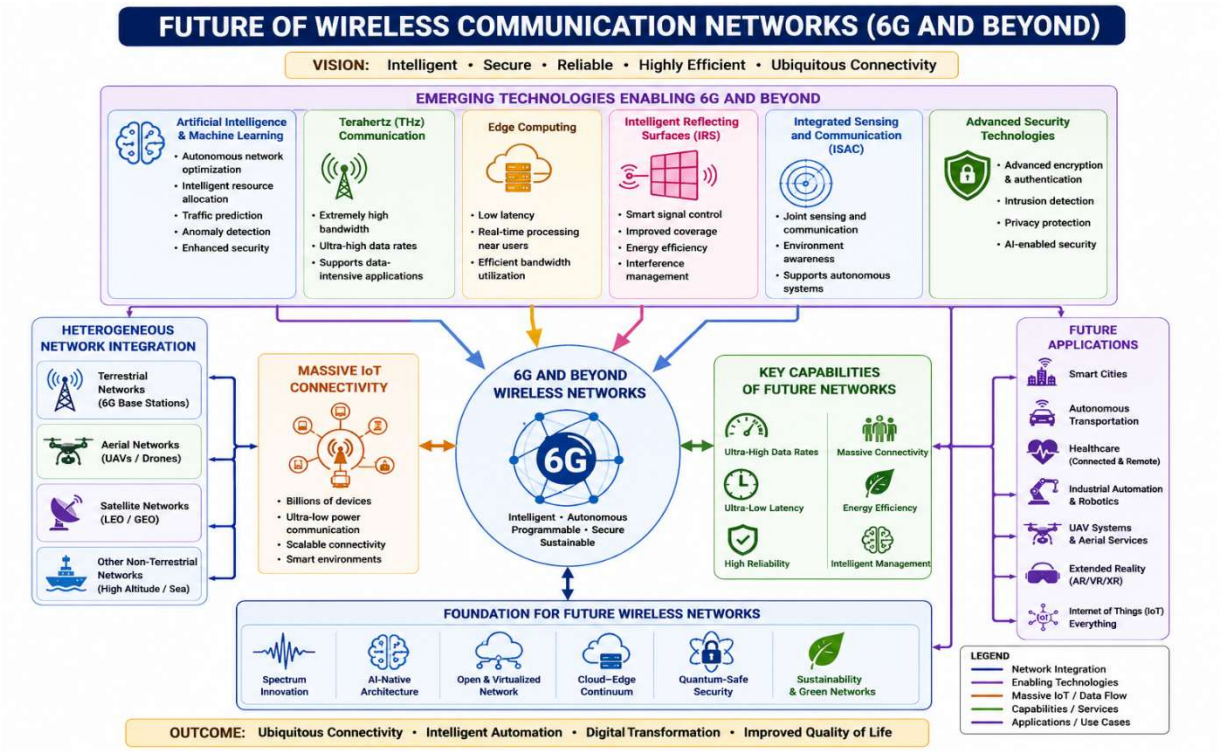


Figure 4: Future of wireless communication network

Conclusion:

Wireless communication networks have evolved from basic radio transmission into advanced, high-speed, and intelligent communication infrastructures that support a wide range of applications. This paper reviewed the history and development of wireless communication networks, including radio, microwave, satellite communication, WLAN, Wi-Fi, Bluetooth, cellular networks, IoT, and UAV-based communication. The evolution from 1G to 5G has resulted in significant improvements in data rates, mobility, network capacity, reliability, and latency, while emerging 6G technologies are expected to further enhance intelligent and ubiquitous connectivity.

The study also highlighted that the increasing dependence on wireless networks introduces significant security challenges, including eavesdropping, unauthorized access, man-in-the-middle attacks, jamming, denial-of-service attacks, interference, data modification, and privacy violations. Therefore, confidentiality, integrity, authentication, availability, and

privacy must remain fundamental requirements of wireless network design. Encryption, authentication, access control, intrusion detection and prevention, and secure communication protocols can provide important layers of protection.

Furthermore, emerging technologies such as 5G, 6G, artificial intelligence, machine learning, IoT, edge computing, UAV communication, blockchain, physical-layer security, and sustainable communication are creating new opportunities as well as new research challenges. Future wireless networks will need to be scalable, energy-efficient, secure, reliable, and capable of supporting massive numbers of connected devices and latency-sensitive applications.

In conclusion, wireless communication networks are moving toward an intelligent, secure, autonomous, and integrated communication ecosystem**.** The successful development of future 6G and beyond-6G networks will depend not only on achieving higher data rates and lower latency but also on addressing security, privacy, energy efficiency, interoperability, and reliability. Continued research in AI-enabled networking, intelligent wireless technologies, UAV and satellite communication, edge computing, and advanced security mechanisms will be essential for realizing

 ©IJSRED: All Rights are Reserved

the full potential of future wireless communication systems.

References

[1] W. Tashan, A. I. Pekdemir, I. Shayea, M. Alnakhli, M. Ergen, and S. A. Saad, "An overview of 6G wireless networks," Physical Communication, vol. 72, 102790, 2025, doi: 10.1016/j.phycom.2025.102790.

[2] H. U. Rashid and S. H. Jeong, "AI empowered 6G technologies and network layers: Recent trends, opportunities, and challenges," Expert Systems with Applications, vol. 267, 125985, 2025, doi: 10.1016/j.eswa.2024.125985.

[3] "On challenges of sixth-generation (6G) wireless networks: A comprehensive survey of requirements, applications, and security issues," Journal of Network and Computer Applications, vol. 233, 104040, 2025, doi: 10.1016/j.jnca.2024.104040.

[4] M. M. Saeed, R. A. Saeed, M. K. Hasan et al., "A comprehensive survey on 6G-security: physical connection and service layers," Discover Internet of Things, vol. 5, article 28, 2025, doi: 10.1007/s43926-025-00123-7.

[5] M. A. Khan, N. Kumar, S. H. Alsamhi, I. Ullah et al., "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review," IEEE Transactions on Network and Service Management, vol. 22, no. 1, pp. 892–912, 2025, doi: 10.1109/TNSM.2024.3487265.

[6] "Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications," 2025.

[7] M. A. Haque, S. Ahmad, A. J. Abboud, M. A. Hossain, K. Kumar, S. Haque, D. Sonal, M. Rahman, and S. Marisennayya, "6G Wireless Communication Networks: Challenges and Potential Solution," International Journal of Business Data Communications and Networking, vol. 19, no. 1, pp. 1–27, 2024, doi: 10.4018/IJBDCN.339889.

[8] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, "A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas," Future Internet, vol. 16, no. 3, 67, 2024, doi: 10.3390/fi16030067.

[9] S. Gao, R. Lin, Y. Fu, H. Li, and J. Cao, "Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey," Electronics, vol. 13, no. 10, 1860, 2024, doi: 10.3390/electronics13101860.

[10] S. Zhang, D. Zhu, and Y. Liu, "Artificial intelligence empowered physical layer security for 6G: State-of-the-art, challenges, and opportunities," Computer Networks, vol. 242, 110255, 2024, doi: 10.1016/j.comnet.2024.110255.

[11] "Blockchain technology meets 6G wireless networks: A systematic survey," Alexandria Engineering Journal, vol. 92, pp. 199–220, 2024, doi: 10.1016/j.aej.2024.02.031.

[12] "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," Future Generation Computer Systems, vol. 160, pp. 577–597, 2024, doi: 10.1016/j.future.2024.06.023.

[13] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim et al., "Internet of Things (IoT) applications security trends and challenges," Discover Internet of Things, vol. 4, article 36, 2024.

[14] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard et al., "Securing internet of things using machine and deep learning methods: a survey," Cluster Computing, vol. 27, pp. 9065–9089, 2024.

[15] "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)," High-Confidence Computing, vol. 4, no. 2, 100220, 2024, doi: 10.1016/j.hcc.2024.100220.

[16] "Internet of Intelligent Things: A convergence of embedded systems, edge computing and machine learning," Internet of Things, vol. 26, 101153, 2024, doi: 10.1016/j.iot.2024.101153.

[17] S. Dong, J. Tang, K. Abbas, R. Hou, J. Kamruzzaman, L. Rutkowski, and R. Buyya, "Task offloading strategies for mobile edge computing: A survey," Computer Networks, vol. 254, 110791, 2024, doi: 10.1016/j.comnet.2024.110791.

[18] M. H. Adnan, Z. A. Zukarnain, and O. A. Amodu, "Fundamental design aspects of UAV-enabled MEC systems: A review on models, challenges, and future opportunities," Computer Science Review, vol. 51, 100615, 2024, doi: 10.1016/j.cosrev.2023.100615.

[19] R. B. Shaik, P. Nagaradjane, I. Ioannou, V. Sittakul, V. Vasiliou, and A. Pitsillides, "AI/ML-aided capacity maximization strategies for URLLC in 5G/6G wireless systems: A survey," Computer Networks, vol. 249, 110506, 2024, doi: 10.1016/j.comnet.2024.110506.

[20] S. H. Alsamhi, A. Hawbani, R. Sahal, S. Srivastava, S. Kumar et al., "Towards sustainable industry 4.0: A survey on greening IoE in 6G networks," Ad Hoc Networks, vol. 165, 103610, 2024, doi: 10.1016/j.adhoc.2024.103610.

[21] "Secure communication in IoT-based UAV networks: A systematic survey," Internet of Things, vol. 23, 100883, 2023, doi: 10.1016/j.iot.2023.100883.

[22] "Review of Physical Layer Security in 5G Wireless Networks," Applied Sciences, vol. 13, no. 12, 7277, 2023, doi: 10.3390/app13127277.

 ©IJSRED: All Rights are Reserved