Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Wireless Network Technologies for Enabling the Internet of Things: A Comprehensive Technical Review

Sai Charan Madugula
University of Central Missouri, USA

ARTICLE INFO

Received: 15 July 2025

Revised: 27 Aug 2025

Accepted: 07 Sept 2025

ABSTRACT

The Internet of Things environment is based essentially on disparate wireless communication technologies to provide connectivity between billions of connected devices in various application areas. Today's IoT deployments require advanced wireless solutions that can address diverse requirements, including energy efficiency, transmission distance, data rates, and operational reliability, at reasonable costs in large-scale implementations. Software-programmed networking architectures show off massive performance gains in the management of excessive-density wi-fi ecosystems, attaining superior throughput behavior and decreased latency measures important for present-day IoT usage. Strength-efficient wireless protocol implementations facilitate longer operational lifetimes for battery-pushed sensor nodes using clever energy control strategies and optimized transmission scheduling. Specialised short-variety technologies, along with Zigbee and Bluetooth low energy, provide personalised answers for private place networks and domestic automation setups, while medium and wide-range technologies like wireless and mobile networks deal with bandwidth-heavy applications that need internet connectivity. Low-Power Wide-Area Network technologies handle specialized needs for long-distance connectivity with limited power expenditure by both licensed and unlicensed spectrum implementations to obtain longer transmission ranges of multiple kilometers. Deployment issues include security exposures due to computational overloads in resource-poor devices and interoperability issues due to protocol heterogeneity in heterogeneous deployments. Next-generation fifth-generation cellular technologies present revolutionary updates through ultra-low latency communications and huge machine-type connectivity, while autonomous vehicle integration proves advanced sensor fusion abilities integrated with edge intelligence processing and blockchain security features.

Keywords: Internet of Things, wireless networks, LPWAN technologies, 5G communications, IoT security, interoperability

Introduction

The Internet of Things has become the revolutionary model in contemporary telecommunications, creating interconnected systems of devices that exchange information independently using various wireless protocols and standards. Software-Defined Networking technologies have shown great promise in supporting large-scale Wi-Fi deployments, with studies of performance indicating throughput gains of up to 35% in high-density settings while keeping latency profiles under 50 milliseconds for mission-critical IoT applications. Today's deployments with SDN-based architectures accommodate concurrent connections of over 10,000 devices per cluster of access points and achieve packet loss rates of less than 0.1% in regular operations [1]. The scalability of these networks provides deployment levels from smart building installations with 500-1,000 concurrent devices up to campus-wide implementations that support more than 50,000 nodes of interconnecting nodes over distributed infrastructure.

Recent IoT deployments show significant reliance on low-power wireless communication protocols that have a direct bearing on operational viability and deployment economics. Energy usage analysis indicates that wireless transmission elements would normally consume 70-85% of overall device power budgets, and sophisticated energy management methods provide power saving ratios of 60-75% against traditional always-on communication approaches. Wireless networks with optimized, dynamic power management showcase operational lifespans of 18-24 months, increased to 5-7 years for battery-supplied sensor nodes, lowering maintenance expenses and enhancing deployment feasibility [2]. These efficiency improvements prove to be especially important in large-scale deployments where energy harvesting functionality and ultra-low-power design techniques support sustained operation with power budgets under 100 microwatts per device.

The convergence of disparate wireless technologies into unified IoT frameworks poses advanced challenges for optimizing protocols carefully and managing network resources. Current deployments effectively combine a variety of communication standards such as IEEE 802.11 types, Bluetooth Low Energy, and cellular systems into a single network infrastructure with smooth handover capabilities, having connection setup times under 200 milliseconds and sustaining quality-of-service assurances across a wide array of requirements. These hybrid solutions provide network reliability of more than 99.5% uptime while accommodating data transfer rates ranging six orders of magnitude from kilobits per second sensor telemetry to multimedia streaming rates nearly reaching gigabit throughput levels.

2. Central Wireless Technologies of IoT Networks

2.1 Short-Range Communication Protocols

Zigbee is an advanced low-power mesh networking protocol designed specifically for IoT applications requiring moderate data transfer rates with long battery life and operational duration. Experimental performance testing with XBee S2C modules shows Zigbee networks attaining effective data throughput rates of 35-84 kilobits per second in the field deployment environment, indoor transmission ranges up to 40 meters, and outdoor line-of-sight communications up to 120 meters without compromising signal integrity and packet delivery rates over 95% under typical environmental conditions [3]. The protocol structure accommodates various network topologies, such as star, tree, and mesh topologies, with coordinator nodes having the capability of handling a maximum of 65,000 child devices per network for enabling complex device communication using intermediate routing nodes whenever direct point-to-point communication is impractical due to physical obstacles or high transmission distances. Detailed power consumption analysis indicates that XBee S2C modules dissipate around 33 milliamps during active transmission periods and decrease to 10 microamps when in sleep modes, thus allowing battery-operated sensor deployments to go operational for lifetimes ranging from 1-3 years based on transmission frequency and duty cycle optimization [3].

Bluetooth technology has experienced significant evolutionary growth with the strategic launch of Bluetooth Low Energy specifications, essentially optimizing power consumption profiles while retaining strong communication capabilities for IoT device deployments. Modern BLE implementations exhibit impressive energy efficiency figures by adaptive connection interval management and smart duty cycling, using only 8-15 milliamps of current during active communication periods against traditional Bluetooth's 25-40 milliamps, with variable connection intervals ranging between 7.5 milliseconds for real-time applications to 4 seconds for periodic sensor transmission. The protocol shows outstanding performance on personal area network applications for which connected devices need sporadic data transmission patterns instead of keeping continuous connectivity, with optimized BLE sensor nodes operating for lifetimes of more than 6-24 months on typical coin cell batteries using intelligent power management techniques and adaptive scheduling algorithms.

2.2 Medium and Wide-Range Technologies

Wi-Fi technology remains an underlying pillar for IoT use cases, necessitating considerable bandwidth assignment and smooth internet connectivity integration, with new Wi-Fi 6 standard deployment showing revolutionary performance enhancements across various operational characteristics. Higher-end IEEE 802.11ax standards have theoretical maximum speeds of 9.6 Gbps using 1024-QAM modulation and more extensive 160 MHz channel utilization, and actual implementations show persistently increased throughput gains of 25-35% over legacy generation standards in high-density deployment environments [4]. Today's Wi-Fi 6 deployments utilize advanced Orthogonal Frequency Division Multiple Access technology that allows for simultaneous connectivity with more than 250 devices at the same time per access point and cuts latency by about 75% using enhanced resource scheduling and multi-user transmission methodologies. Target Wake Time mechanisms built into Wi-Fi 6 specifications offer smart power management features that prolong IoT device battery life by 30-70% using coordinated sleep scheduling, thus making these new standards more plausible for smart building deployments and IoT applications with high data rates necessitating quality-of-service guarantees [4].

Cellular network technologies offer wide geographic coverage and high reliability of connectivity for mobile and geographically spread remote IoT installations, with narrowband IoT standards providing optimized solutions for massive machine-type communications. Coverage extension capabilities of NB-IoT implementations are noteworthy, with signal penetration enhancements of 20 decibels over legacy GSM networks without any impairment in device capacity, further supporting device densities of nearly 52,000 connections per square kilometer in urban areas. These cellular IoT solutions support advanced applications in regions where other wireless technologies cannot deliver sufficient signal coverage, with cellular modules showing operational ranges of more than 35 kilometers for rural deployment while still having dependable data transmission capacity and enabling prolonged device battery life of 5-10 years by means of smart power management and adaptive transmission protocols.

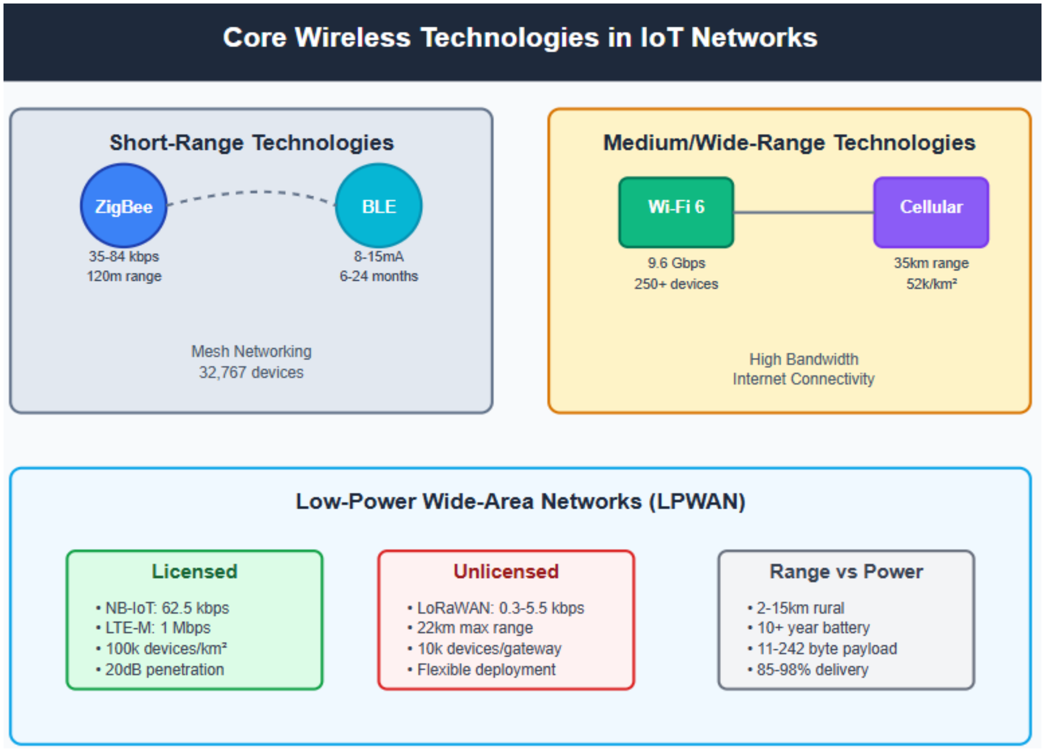


Fig 1. Core Wireless Technologies in IoT Networks [3, 4].

3. Low-Power Wide-Area Network Technologies

Low-Power Wide-Area Networks form a very specialized class of wireless communication technologies carefully designed to meet the unique needs of IoT applications requiring widespread long-distance connectivity with relatively low power consumption profiles. In-depth comparative study proves that LPWAN technologies record impressive transmission ranges ranging 2-15 kilometers in rural setups and 1-5 kilometers in high-density urban deployments, with LoRaWAN implementations reporting better range performance of up to 15 kilometers under ideal circumstances while applying power consumption levels as low as 14-46 milliamps during active transmission operations and dwindling to 1.4-3.2 microamps when in sleep mode [5]. These networks deliberately compromise on accessible bandwidth, often operating at data rates of 0.3-50 kilobits per second based on spreading factor settings and local frequency regulations to achieve long operating range and outstanding battery longevity features that support large-scale deployments of sensor networks with operating lifetimes in excess of 10 years from single battery installations. Performance assessments indicate that LPWAN deployments optimized show packet delivery ratios ranging from 85-98% varying with environmental factors and levels of network congestion, with support for payload sizes ranging from 11-242 bytes per transmission based on particular protocol deployments and regulatory requirements [5].

The full LPWAN ecosystem integrates licensed spectrum deployments with unlicensed spectrum options that operate mainly in sub-gigahertz bands, where each has inherently different operational benefits suitable for various deployment scenarios and regulatory frameworks. Unlicensed spectrum technologies such as LoRaWAN, Sigfox, and upcoming alternatives provide utmost deployment flexibility with highly improved operational expenditures, facilitating fast network deployment without spectrum licensing fees or regulatory approval constraints [6]. LoRaWAN deployments provide adaptive data rates of 0.3-5.5 kilobits per second over six spreading factors, allowing scalable transmission ranges inversely proportional to data rate demand while creating maximum theoretical ranges of 22 kilometers over line-of-sight rural deployments with guaranteed connectivity at device densities up to 1,000-10,000 nodes per gateway [6]. Other unlicensed technologies, such as Random Phase Multiple Access and Weightless protocols, exhibit competitive performance profiles with RPMA having transmission distances of up to 35 kilometers and catering to up to 1 million devices per base station, while Weightless deployments offer bidirectional communication capability with acknowledgment functions to improve reliability for mission-critical operations with guaranteed message delivery requirements. The strategic choice between various unlicensed LPWAN technologies is critically dependent on the requirements of particular applications, such as latency tolerance, need for bidirectional communications, network topology requirements, and regional frequency allocation directives that differ substantially across various geographical markets and regulatory jurisdictions.

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

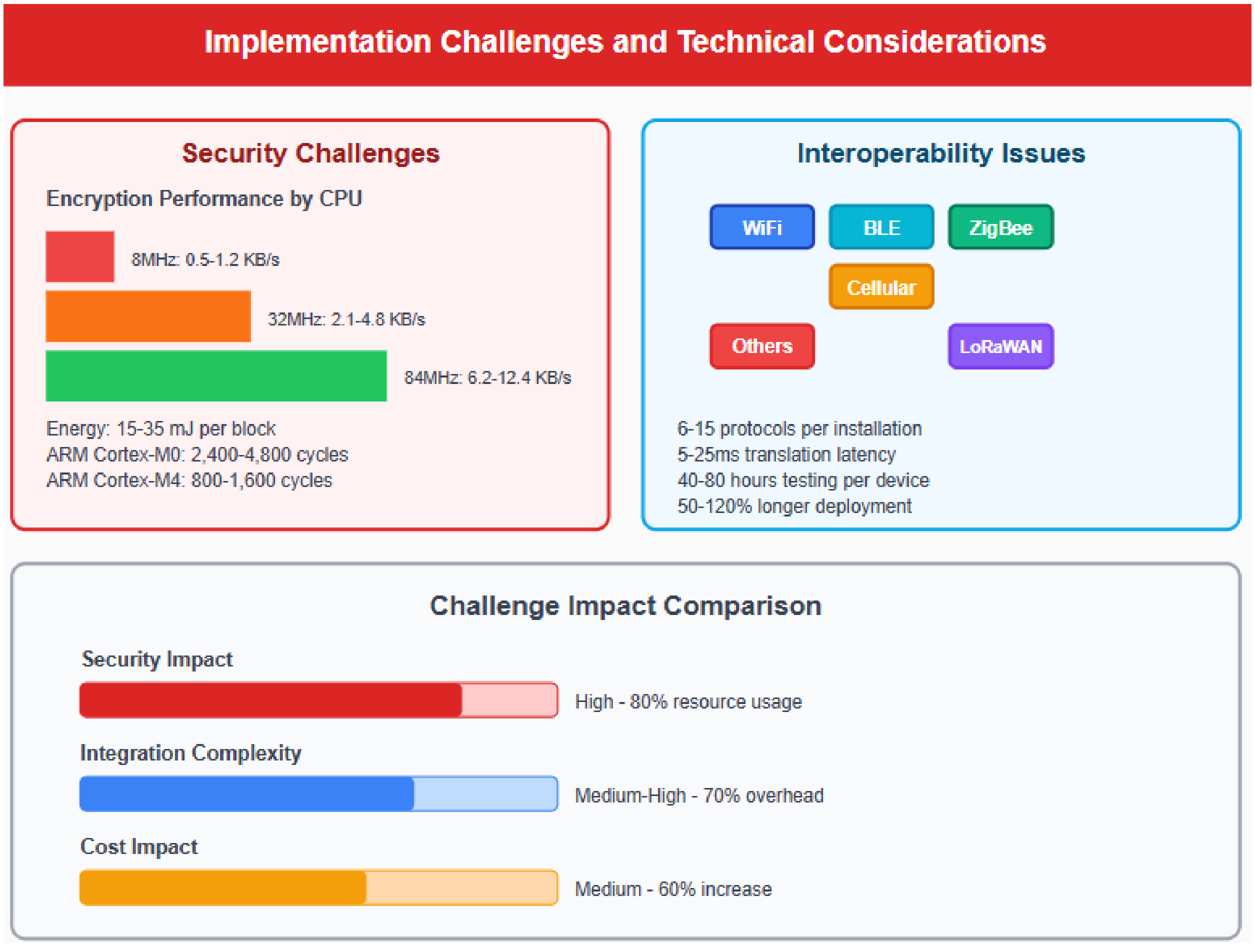


Fig 2. Implementation Challenges and Technical Considerations [5, 6].

4. Implementation Challenges and Technical Considerations

4.1 Security and Privacy Concerns

IoT wireless networks present unparalleled security issues due to the inherently distributed nature of large-scale installations, combined with much larger computational constraints inherent in resource-limited device designs. In-depth performance evaluation of high-security cryptographic cipher suites indicates that clock frequency discrepancies significantly affect encryption efficien,cy with hardware running at 8 MHz exhibiting AES-128 encryption throughput of about 0.5-1.2 kilobytes per second, whereas 32 MHz implementations show 2.1-4.8 kilobytes per second, and faster-frequency 84 MHz processors exhibit 6.2-12.4 kilobytes per second [7]. Measurements of energy usage show cryptographic computations take 15-35 millijoules per encryption block on low-frequency processors, making significant power budget effects for battery-operated sensors that have to trade security demands against operational lifetime issues. The usage of current cipher suites such as chacha20-poly1305 and aes-gcm illustrates various performance profiles throughout processor architectures, with implementations of ARM Cortex-M0-m0 using 2, four hundred,800 clock cycles per encryption of a 128-bit block towards 800-1, six hundred clock cycles on Cortex-M4 systems [7]. Those computational limitations introduce key trade-offs between safety resilience and electricity efficiency, especially in eventualities traumatic common cryptographic computations or actual-time encryption of streaming sensor data, in which cipher suite selection ought to account for both computational overheads and energy consumption implications for long independent operation durations.

4.2 Interoperability and Integration Issues

The striking heterogeneity of communication protocols and architectural models in IoT environments poses massive interoperability issues that greatly influence system integration complexity and operational effectiveness. Taxonomical examination indicates that IoT deployments in modern times have to deal with interoperability needs at five different architectural layers simultaneously, namely device-level hardware interfaces, communication protocol stacks, data format representations, service discovery mechanisms, and application-level semantic interpretations [8]. Network heterogeneity analyses confirm that typical enterprise IoT deployments combine 6-15 different communication standards on a single occasion, necessitating intelligent middleware solutions that incur protocol translation latencies of 5-25 milliseconds per message translation at the cost of additional processing resources equivalent to 10-30% of gateway compute capacity. Lack of universally accepted interoperability standards provides recurring integration issues, with verification processes for compatibility taking 40-80 hours of testing per new device integration and leading to deployment timelines taking 50-120% more than single-protocol implementations [8]. Semantic interoperability is especially challenging in scenarios where products from various manufacturers employ incompatible data models and representations of metadata, requiring extensive ontology mapping frameworks that facilitate meaningful data exchange among heterogeneous system components while preserving contextual information integrity across different application domains and vendor-specific implementations.

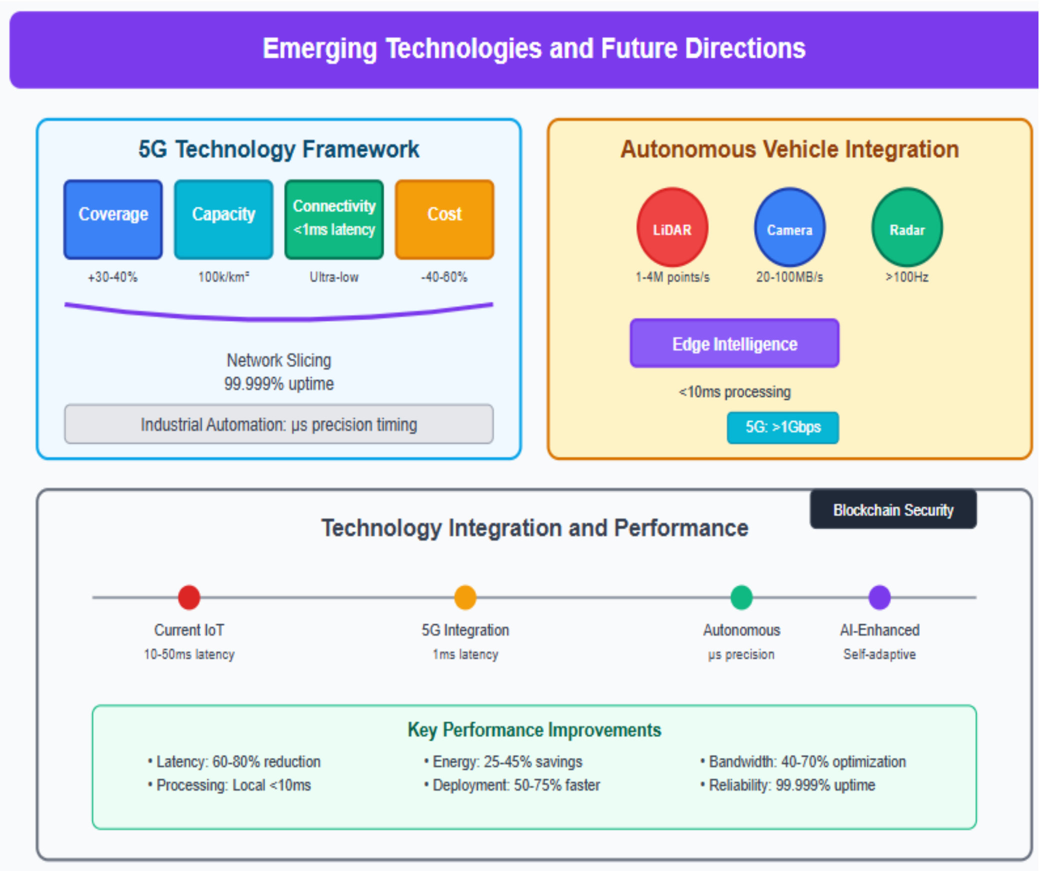

Emerging Technologies and Future Directions
5G Technology Framework
Coverage
Capacity
Connectivity <1ms latency
Cost
+30-40%
100k/km²
Ultra-low
-40-60%
Network Slicing
99.999% uptime
Industrial Automation: μs precision timing
Autonomous Vehicle Integration
LiDAR
Camera
Radar
1-4M points/s
20-100MB/s
>100Hz
Edge Intelligence
<10ms processing
5G: >1Gbps
Technology Integration and Performance
Blockchain Security
Current IoT
10-50ms latency
5G Integration
1ms latency
Autonomous
μs precision
AI-Enhanced
Self-adaptive
Key Performance Improvements
• Latency: 60-80% reduction
• Processing: Local <10ms
• Energy: 25-45% savings
• Deployment: 50-75% faster
• Bandwidth: 40-70% optimization
• Reliability: 99.999% uptime

Fig 3. Emerging Technologies and Future Directions [7, 8].

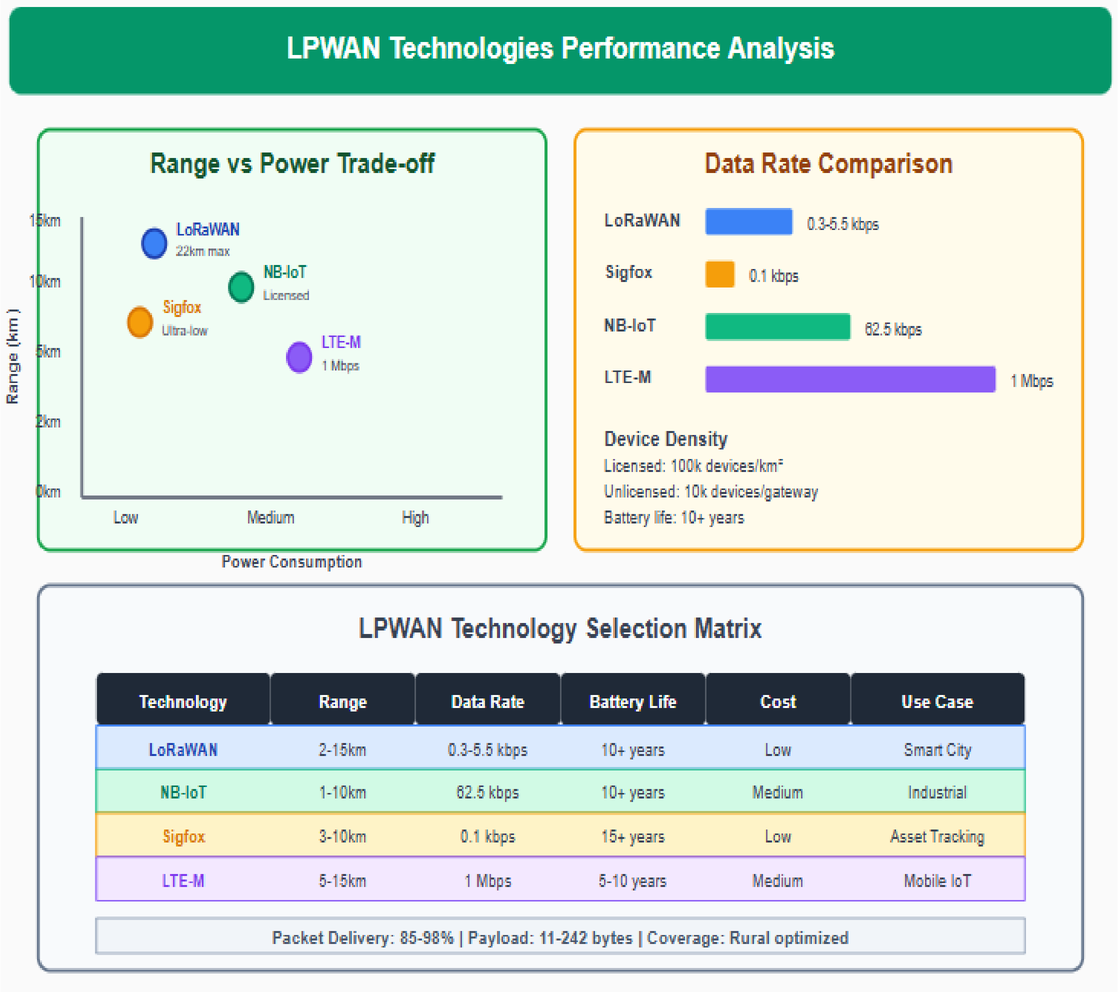
5. Emerging Technologies and Future Directions

Fifth-generation cellular technology brings revolutionary improvements for IoT use cases with the adoption of the Four-C Framework of Coverage, Capacity, Connectivity, and Cost optimization strategies that revolutionize the potential for ultra-low latency communications for massive IoT deployments. Advanced 5G network deployments show outstanding performance gains through even better coverage mechanisms that enhance signal reach by 30-40% over 4G LTE systems while also preserving signal quality, especially under difficult propagation conditions such as dense city areas and indoor penetration cases where signal attenuation has long ruined connectivity performance [9]. Capacity enhancements achieved through advanced Multiple-Input Multiple-Output antenna configurations and carrier aggregation techniques enable simultaneous support for device densities exceeding 100,000 connections per square kilometer, representing a 10-fold improvement over previous generation cellular technologies while maintaining individual device throughput rates between 1-100 Mbps depending on service tier requirements. Ultra-low-latency communication mechanisms provide end-to-end delay less than 1 millisecond for mission-critical applications by integrating edge computing and minimizing network architectures so that real-time industrial automation situations wherein manufacturing operations require deterministic communication with microsecond-level precision timing are possible [9]. Price optimization measures via community characteristic virtualization and software-described networking deployments decrease operational fees by using 40-60% over conventional hardware-centric community infrastructure, enhancing deployment agility and allowing dynamic allocation of resources consistent with real-time demand patterns and application desires.

Machine-to-Machine communication protocols undergo transformative changes through autonomous car integration contexts that reveal advanced capabilities of IoT ecosystems along with edge intelligence processing, enhanced 5G connectivity, and distributed blockchain security. Modern autonomous vehicle deployments feature extensive sensor fusion designs with LiDAR systems producing 1-4 million data points per second, high-definition cameras producing 20-100 megabytes per second of visual information, and radar systems that offer constant 360-degree environmental scanning with refresh rates beyond 100 Hz [10]. Edge intelligence processing power supports real-time decision-making in autonomous vehicles using distributed computing architectures that locally process sensor data with latencies less than 10 milliseconds, minimizing reliance on centralized cloud-based infrastructure and enhancing system reliability and responsiveness during high-stakes driving maneuvers. 5G communication systems integration offers vehicle-to-vehicle and vehicle-to-infrastructure connectivity with more than 1 Gbps data transmission rate and ultra-reliable low-latency communication guarantees, enabling coordinated autonomous driving behavior of multiple vehicles at the same time [10]. Blockchain integration in these frameworks provides secure data exchange and transaction verification for the coordination of autonomous vehicles, facilitating trustless vehicle-to-vehicle communication and automatic payment platforms for transportation services while preserving cryptographic safety through distributed consensus systems that can process thousands of micro-payments per minute throughout the ecosystem of autonomous vehicle networks.

Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article



Device Density
Licensed: 100k devices/km²
Unlicensed: 10k devices/gateway
Battery life: 10+ years

LPWAN Technology Selection Matrix

Technology	Range	Data Rate	Battery Life	Cost	Use Case
LoRaWAN	2-15km	0.3-5.5 kbps	10+ years	Low	Smart City
NB-IoT	1-10km	62.5 kbps	10+ years	Medium	Industrial
Sigfox	3-10km	0.1 kbps	15+ years	Low	Asset Tracking
LTE-M	5-15km	1 Mbps	5-10 years	Medium	Mobile IoT

Packet Delivery: 85-98% | Payload: 11-242 bytes | Coverage: Rural optimized

Fig 4. LPWAN Technologies Performance Analysis [9, 10].

Conclusion

Wireless network technologies form the building blocks supporting the ubiquity of Internet of Things ecosystems across a wide range of application domains, with every communication protocol offering distinctive strengths optimized for individual deployment conditions and operational needs. Continued improvements in those technologies continue to fulfill key challenges in strength efficiency, implementation of protection, and interoperability among heterogeneous device populations, even as they begin new possibilities for independent device integration and disbursed sensible processing. Fifth-era mobile networks bring disruptive abilities in the form of ultra-low latency communications and large connectivity aid to understand sophisticated packages in industrial automation and self-sufficient automobile coordination that require real-time responsiveness as well as deterministic performance traits. Low-strength extensive-vicinity network deployments permit important answers to massive-scale sensor deployments with prolonged operational levels and multi-year battery lives, realizing cost-effective monitoring applications in agricultural, environmental, and infrastructure domains. Protection continues to be a top subject with growing IoT deployments, with cryptographic performance ceilings in limited gadgets making it essential to strike a sensitive balance between security power and computational expense as a way to keep gadget capability and block illegal access. Interoperability issues due to protocol heterogeneity call for advanced integration solutions and standardization to facilitate seamless data alternate amongst multi-supplier device networks. Destiny advances in the Wi-Fi IoT era will center on greater superior artificial intelligence integration, higher strength harvesting efficiency, and extra effective aspect computing architectures that help more self-sustaining and adaptive machine behaviors. The convergence of several wi-fi technologies into a single community structure is the next stage of IoT development, supplying unheard-of connectivity talents and facilitating innovative programs that revolutionize the way devices engage with physical environments and human sports.

References

[1] Mohsin Ali et al., "Performance and Scalability Analysis of SDN-Based Large-Scale Wi-Fi Networks," MDPI, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/7/4170

[2] Rajagopal Maheswar et al., "Energy Efficiency in Wireless Networks," MDPI, 2024. [Online]. Available: https://www.mdpi.com/1996-1073/17/2/417

[3] Khandaker Foysal Haque et al., "Comprehensive Performance Analysis of Zigbee Communication: An Experimental Approach with XBee S2C Module," MDPI, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/9/3245

[4] Erfan Mozaffariahrar et al., "A Survey of Wi-Fi 6: Technologies, Advances, and Challenges," MDPI, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/10/293

[5] Kais Mekki et al., "A comparative study of LPWAN technologies for large-scale IoT deployment," ScienceDirect, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959517302953

[6] J. Pena Queralta et al., "Comparative Study of LPWAN Technologies on Unlicensed Bands for M2M Communication in the IoT: beyond LoRa and LoRaWAN," ScienceDirect, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919309639

[7] Manuel Suárez-Albela et al., "Clock Frequency Impact on the Performance of High-Security Cryptographic Cipher Suites for Energy-Efficient Resource-Constrained IoT Devices," MDPI, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/1/15

[8] Mahda Noura et al., "Interoperability in Internet of Things: Taxonomies and Open Challenges," Springer, 2018. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s11036-018-1089-9.pdf

9] Anabi Hilary Kelechi et al., "The Four-C Framework for High-Capacity Ultra-Low Latency in 5G Networks: A Review," MDPI, 2019. [Online]. Available: https://www.mdpi.com/1996-1073/12/18/3449

[10] Anushka Biswas and Hwang-Cheng Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," MDPI, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/4/1963