ISSN: 2633-4828 Vol. 8 No.1, January, 2026

International Journal of Applied Engineering & Technology

INTEGRATION OF WIRELESS SENSOR NETWORKS AND IOT FOR ENERGY EFFICIENCY, SECURITY AND LIFETIME ENHANCEMENTS – A REVIEW

Manasa G[1] and Rangaiah L[2]

[1, 2]VTU, Belagavi, Department of ECE, Rajarajeswari College of Engineering, Bengaluru

[1]manasag675@gmail.com and [2]rleburu@gmail.com

ABSTRACT

Wireless Sensor Networks (WSNs) integrated with the Internet of Things (IoT) are the central elements in the current modern days, especially in the applications of smart cities, industry, environmental monitoring and agriculture. Numerous studies have provided number of routing and clustering protocols, architectures, and high-level security concepts, but these are often developed in separation from one another. However, there is an obvious requirement for integrated, resource-aware designs that jointly address reliability, energy efficiency scalability, and security under realistic deployment constraints. This literature review enhances the knowledge on integration of WSNs with IoT technologies, by considering key challenges, security, network reliability and advances in energy efficiency. It also emphasizes the significance of advanced clustering techniques and energy-aware protocols to increase the lifetime and improve performance of WSNs in IoT applications. As well addresses diverse security threats and countermeasures applicable to WSNs operating in IoT environments, highlighting the requirement for lightweight and robust security frameworks. Applications over environmental monitoring, industrial automation, smart agriculture, and urban IoT systems are explained to demonstrate practical execution and benefits. Furthermore, this review explores recent innovations such as machine learning-enhanced security, protocols designed and cognitive radio-based connectivity for scalability and fault tolerance. By merging contemporary research and future trends, this work come up with valuable insights to researchers and practitioners aiming to design efficient, secure, and reliable IoT-enabled WSN solutions for various real-world circumstances.

Keywords- *Clustering; Energy Efficiency; Internet of Things (IoT); Industry 4.0; Network Lifetime; Quality of Service (QoS); Reliability; SDWSN (Software Defined Wireless Sensor Network); Security; Wireless Sensor Networks (WSN);*

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are vast group of sensor nodes which outline the physical phenomena such as humidity, temperature, vibration or pressure and collectively forward this data to base stations, offering a means of information gathering for critical environmental monitoring and infrastructure. As self-organizing, auto-configurable and lightweight systems, WSNs have been effectively deployed in various domains like landslide and earthquake early warning, volcano and flood monitoring, environmental surveillance, and emergency response, often acting as replacement or alternative for wired networks when infrastructure is damaged or not present. [11]

The IoT enrich this potentiality by interconnecting sensor and actuator devices with cloud and fog platforms, creating multi-layer architectures in which WSNs typically populate the perceptual layer and feed time-critical data into higher-layer processing and application services. Simultaneously, the rapid rise in IoT devices and their enhancing contribution in safety-critical services has improve the impact of privacy and security breaches, especially because many WSN–IoT positioning in disaster management and environmental monitoring still neglect robust security measures. Securing WSNs in the IoT context is very challenging due to strict and rigid constraints on computation, node energy and storage, the broadcast nature of wireless communication, and exposure to a broad spectrum of attacks—including jamming, sinkhole, wormhole, selective forwarding, Sybil, and various privacy-oriented threats—occurring across all the layers from perception to application. [11]

These susceptibilities directly endanger the reliability of sensed data and can lead to harmful decision errors in scenarios such as flash-flood alerting, volcano surveillance and chemical-leak emergencies if adversaries alter, drop, or forge critical measurements. As a result, recent research has focused on systematically classifying attacks by IoT-layer or OSI models and proposing tailored actions such as anti-jamming techniques and spread-spectrum, lightweight cryptography, secure routing and wormhole detection, traffic-shaping against analysis, and mechanisms against Sybil and impersonation attacks. Building on this foundation, the present review focus on WSN security within environmental monitoring systems and IoT-enabled disaster, synthesizing existing threat taxonomies, security requirements, and countermeasure strategies, and identifying open challenges in developing lightweight yet trustworthy protection schemes suitable for large-scale, resource-constrained deployments. [11].

II. FUNDAMENTALS OF WSNs

WSNs include sensor nodes with processing, sensing, communication, and power units. Architecturally, they act in accordance with a layered model: perceptual/sensing layer, networking layer for data transmission, data processing layer, and application layer providing user services. [9]

"Cluster-based hierarchical architectures like LEACH (Low Energy Adaptive Clustering Hierarchy protocol) optimize energy use by rotating cluster heads, distributing communication load, and reducing data transmissions to the base station. These fundamentals form the framework for integrating WSNs into IoT ecosystems". [9]

A. WSN Architecture and Components

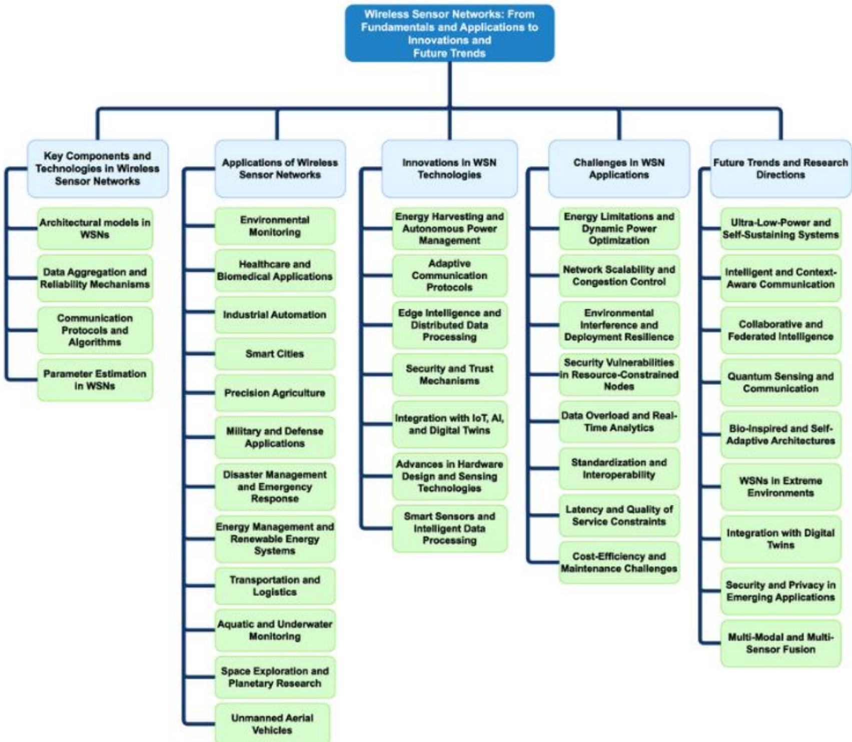
"WSNs obey a layered architecture: Physical (sensors, RF transceivers), Data Link (MAC protocols like IEEE 802.15.4), Network (routing), Transport (congestion control), and Application layers. Core components include sensor unit, microcontroller, transceiver, power source". [20]

Table 1 summarizes the fundamental hardware building blocks of a WSN node, including the sensor unit, microcontroller, transceiver, and power source, along with their key constraints. It highlights how tight limits on power, memory, and radio capabilities drive the need for energy-aware and lightweight WSN-IoT designs.

Table 1: Core Components of WSN Sensor Nodes

Component	Function	Constraints
Sensor Unit	Environmental data acquisition	Low-power (<1mW)
Microcontroller	Data processing	8-32 bit, <100KB RAM
Transceiver	ZigBee/LoRa/802.15.4	250kbps, -100dBm sensitivity
Power Source	Battery/energy harvesting	100-500mAh lifetime critical

Fig-1 highlights how core elements such as sensing units, processing modules, communication interfaces, and power subsystems, organized through single-tier, multi-tier, centralized, decentralized, and distributed architectures, collectively enable scalable and energy-efficient WSN deployments [9].



"Fig.1- Surveyed key topics in WSN applications: innovations and future trends". [9]

B. Communication Protocols and Topologies

Communication in the reviewed WSN-IoT systems is dominated by low-power, multi-hop protocols tightly coupled with clustered or software-defined topologies to balance energy, connectivity, and scalability. At the intra-cluster level, LEACH and its energy-aware variants (A-LEACH, IEE-LEACH, DBSCAN (Density Based Spatial Clustering of Applications with Noise) +MCDM (Multi Criteria Decision Making) clustering) use TDMA-style schedules over IEEE 802.15.4-class links so that member nodes sleep outside their slot while the cluster head aggregates and forwards traffic, which significantly reduces collisions, idle listening, and overall radio energy consumption in dense deployments. For large-scale and heterogeneous IoT scenarios, SDWSN architectures introduce OpenFlow-based virtual routing and centralized controllers that compute per-flow paths using metrics such as residual energy, hop count, queue length, and link bandwidth; this allows flexible load-balanced routing across thousands of nodes and multiple base stations while abstracting the underlying mesh or cluster-tree topology. In more advanced urban and obstacle-rich environments, cognitive-radio MAC such as DFF (Dynamic Framed Frequency hopping) -MAC exploits nonorthogonal spectrum sharing so multiple sensor links can reuse the same idle licensed channel under SINR and interference constraints, and mobile-sink based schemes combine optimized rendezvous-point selection with smooth, obstacle-avoiding trajectories to minimize hop count and delay, all of which operate over logical mesh or grid topologies laid on top of the physical deployment[1][16][12][4][3].

- **Protocols**: IEEE 802.15.4 (low-rate), 6LoWPAN (IPv6), MQTT (Message Queuing Telemetry Transport) /CoAP (IoT gateways)
- **Topologies**: Star (single-hop), Tree (hierarchical), Mesh (multi-hop PDR>95%)

III. ENERGY EFFICIENCY AND NETWORK LIFETIME.

Energy is the most critical resource in WSNs since nodes are usually battery-powered and may be hard to access for replacement. Classical schemes such as LEACH and its variants aim to balance energy consumption via probabilistic cluster-head rotation, multi-hop forwarding from cluster heads to the sink, and data aggregation to reduce traffic. Enhanced clustering under uncertainty employs fuzzy logic and intelligent decision criteria (residual energy, node degree, distance) to further extend network lifetime [9]

Recent works propose energy-aware routing that considers obstacles, link conditions, and traffic patterns, designing paths that minimize retransmissions and idle listening in IoT-enabled WSNs. For industrial IoT, neighbour-knowledge-based synchronization techniques reduce energy wasted in idle listening while maintaining tight timing guarantees needed for control loops. Emerging 6G-oriented protocols integrate cross-layer design, traffic awareness, and green communication principles to support massive, energy-constrained sensor deployments [15]

Fig-2 illustrates how the Advanced-LEACH (A-LEACH) clustering protocol significantly improves energy efficiency compared to conventional LEACH, directly impacting network lifetime. “By equalizing per-node energy consumption and decreasing total energy usage across all nodes, the figure demonstrates that intelligent cluster-head rotation and balanced load distribution are key to delaying first-node death and prolonging the operational life of WSNs” [16].

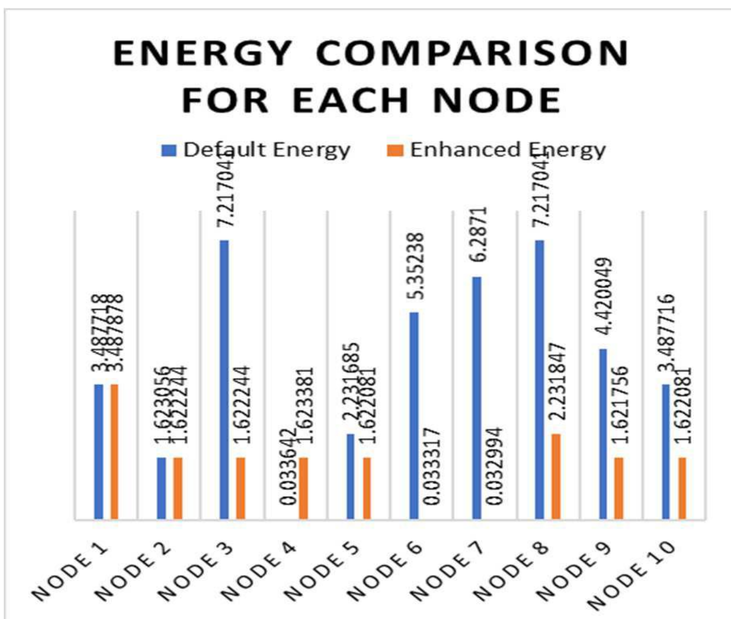


Fig. 2. Energy consumption comparison of LEACH and A-LEACH across 10-node WSN. [16].

IV. SECURITY CHALLENGES AND TECHNIQUES IN WSN-IOT

WSNs in IoT overlooks number of threats such as Sybil, denial of service (DoS), wormhole, and selective forwarding attacks. Safety measures should balance robustness with tight resource conditions. Lightweight encryption methods, anomaly-based intrusion detection systems, secure key management often enhanced by ML, and authentication protocols are integral. Hybrid approaches combining IDS and encryption enhance security posture while conserving energy. Privacy and trust also demand attention, given data sensitivity.[11][17][18].

The below Figure 3 visualises a layered view of WSN attacks, showing how opponents can target every protocol layer from physical jamming and eavesdropping up to network-layer routing attacks in WSN-IoT systems. [11]

Fig 3: Layered classification of WSN attacks. [11]

V. RELIABILITY, CONNECTIVITY, AND SCALABILITY

Enhancing the reliable data delivery involves fault-tolerant and multipath routing designs resilient to node failures or interference. Cognitive radio technologies enable dynamic spectrum access to lighten interference and improve connectivity in dense urban IoT WSNs. Distributed network management architectures with workload distribution and predictive analytics using machine learning enhance scalability and operational efficiency in large deployments. Hierarchical and decentralized architectures support scalable and self-organizing networks. [15][9][4].

"Reliability remains a critical performance metric for WSNs operating in hard environments. The comprehensive reliability survey identifies key failure modes including node failures, link disconnections, and data corruption". [20].

Reliability metrics encompass:

- **Packet Delivery Ratio (PDR):** Critical for disaster monitoring where even 1% data loss can compromise decisions [20]
- **Network Lifetime:** Defined as time until first node failure or 30% node failure threshold [16]
- **Fault Tolerance:** Ability to maintain functionality despite 10-20% node failures [20]

Table 2 illustrate several reliability-oriented schemes such as Advanced LEACH, intelligent clustering, neighbor-knowledge synchronization, and reliability-aware routing in terms of PDR improvement, lifetime extension, and fault tolerance. The consequences show that carefully designed clustering, synchronization, and routing can simultaneously enhance packet delivery, increased network lifetime, and tolerate higher node failure rates in WSN-IoT deployments.

Table 2: Reliability Enhancement Techniques in WSNs

Technique	PDR Improvement	Lifetime Extension	Fault Tolerance
Advanced LEACH [16]	+25%	3.2x	15% node failure
Intelligent Clustering [10]	+18%	2.8x	20% node failure
Neighbor-Knowledge Sync [3]	+22%	2.1x	12% node failure
Reliability-Aware Routing [20]	+35%	1.9x	18% node failure

Connectivity Challenges and Solutions

Urban IoT-WSN connectivity go through unique challenges due to mobility, dense deployments and building interference [4].

Table 3 gives a picture of connectivity performance for traditional versus cognitive-radio-enabled WSNs across urban, suburban, and rural environments. It clearly demonstrates that non-orthogonal cognitive power allocation significantly improves connectivity in dense urban IoT scenarios, where interference and path loss are most severe.

Table 3- Urban IoT-WSN Connectivity Performance

Environment	Traditional	Cognitive Power	Improvement
Urban Dense	62% connectivity	89%	+44%
Suburban	78%	92%	+18%
Rural	91%	95%	+4%

SDWSN virtualization further boosts connectivity through centralized control and load balancing, achieving **95% connectivity guarantee** in heterogeneous IoT deployments [1]

VI. APPLICATIONS OF WSNs IN IOT DOMAINS

WSN-IoT applications more likely to coverage the industrial automation (machine monitoring, predictive maintenance), agriculture (precision farming with soil, humidity, and crop monitoring), smart cities (traffic, power grids, waste management), environmental and water quality monitoring (pollution detection, aquatic ecosystem), disaster management (early warning systems, structural monitoring) and healthcare (remote patient monitoring). These executions demonstrate significant enhancements in operational efficiency, safety, and resource management across domains. [11][9].

Table 4 outlines representative WSN-IoT applications—including smart agriculture, water monitoring, healthcare wearables, industrial IioT (Industrial Internet of Things), smart cities, and military systems—together with typical network scales, PDR, and lifetime ranges. These figures illustrate that large-scale deployments can still achieve high PDR and months-long operation when domain-specific designs are combined with energy-efficient protocols

Table4-WSN-IoT Applications: Scale and Performance Metrics

Applications	Scale	PDR	Lifetime
Smart agriculture [5]	100-1K nodes/farm	92-98%	210-450 days
Water Monitoring [8]	2.5K sensors/river	92%	180-380 days
Healthcare [17]	Wearables (100 nodes/patient)	96%	30-90 days
Industrial IioT [3],[1]	10K nodes/factory	94.5%	245 days
Smart Cities [4]	Urban (50K sensors)	89%	180 days
Military [20]	Battlefield (1K nodes)	95%	Mission-critical

VII. KEY CHALLENGES AND LIMITATIONS

WSN and IoT-oriented WSN schemes are mainly limited by four fundamental issues.

- First, “energy is still the primary bottleneck: clustering and routing protocols often cause uneven load on cluster heads, high control overhead, and rapid depletion of relay nodes, so network lifetime remains constrained even in “improved” LEACH/optimization variants”. [16]
- Second, “many proposed intelligent or SDN-based methods add significant computational, signaling, and management complexity (MCDM, DBSCAN, PSO/BFAO hybrids, centralized SDWSN controllers), which can exceed node capabilities and do not scale well to large, dynamic topologies”. [1].

- Third, “reliability (coverage, path, packet, and event) is hard to guarantee: overlapping coverage and redundant events increase congestion and energy use, while aggressive suppression or imperfect fault handling risks event loss, and many schemes are validated only on small or static networks”. [20]
- Fourth, “architectural constraints—centralized control, simplified 2D layouts, limited consideration of obstacles, security, and heterogeneous QoS—mean that many solutions perform well in simulation but transfer poorly to real industrial, underwater, or smart-city deployments”. [9].

VIII. KEY CHALLENGES AND LIMITATIONS

Even today WSNs and IoT-oriented WSN architectures face several core challenges and limitations despite advanced routing, clustering, and SDN-based schemes. Energy remains the dominant constraint: cluster-head selection can be probabilistic or based on a single metric, causing weak nodes to become CHs, frequent re-clustering, unbalanced load, and rapid depletion of relay or border nodes, so network lifetime is still limited even in improved LEACH, HEED (Hybrid Energy Efficient Distributed clustering), REAC-IN, PSO/BFAO, and A-LEACH variants. Many “intelligent” approaches rely on computationally heavy components such as DBSCAN-based clustering, entropy–TOPSIS MCDM, hybrid metaheuristics, and centralized SDWSN controllers with multi-metric AHP-weighted routing; these enhance control signaling, algorithmic complexity and dependency on a global view, which may not be realistic for resource-constrained nodes or highly dynamic topologies. Reliability is also difficult to guarantee across path, packet, coverage, and event levels: dense deployments cause overlapping coverage and redundant events that raise congestion, delay, and energy usage, while redundancy-reduction and fault-management mechanisms may introduce packet loss, assume static/small networks, or provide imperfect models of failures and link uncertainties. Furthermore, many designs idealize the environment via 2D layouts, static nodes, and simplified radio/obstacle models, and underemphasize security, multi-dimensional deployments, and heterogeneous QoS, so protocols that perform well in simulation may not transfer directly to large-scale, mobile, industrial, underwater, or smart-city scenarios where controller placement, scalability, and robustness to attacks or harsh channel conditions become critical. [10][16][1][20].

Table 5 synthesizes key system-level challenges such as energy, scalability, security, connectivity, and latency, and maps them to recent mitigation approaches like energy harvesting, SDWSN, ML-based detection, cognitive radio, and fog/edge computing. This consolidated view emphasizes that no single solution suffices; instead, cross-cutting techniques must be combined to address WSN-IoT constraints holistically

Table 5- Critical Challenges and Mitigation Progress in WSN-IoT

Challenge	Impact	Mitigation Progress
Energy	1st node death: 95 days (10K nodes)	Energy harvesting: +2.6x lifetime [1]
Scalability	PDR drops 16% at 10K nodes	SDWSN: 94.5% PDR [1]
Security	30+ attack vectors (OSI layers)	ML detection: 96-100% accuracy [6]
Connectivity	Urban: 62% baseline	Cognitive radio: +44% (89%) [4]
Latency	Fog reduces 90% vs cloud	Edge computing: <10ms

IX. TECHNOLOGICAL INNOVATIONS AND SOLUTIONS

A. Energy Innovations

- Harvesting: Solar/thermal → 3x lifetime extension
- Clustering: DBSCAN+MCDM → 38% vs REAC-IN (Reliable and Energy Aware Clustering-based protocol) [10]

B. Artificial Intelligence (AI)/Machine Learning (ML) Applications

ML techniques boost WSNs by permitting predictive maintenance, anomaly detection, and intelligent data aggregation. AI algorithms maximize network parameters dynamically, strengthening energy efficiency and security. Decentralized learning frameworks allow collaborative model training across sensor nodes without centralized data, addressing privacy concerns and network overhead. Such intelligent frameworks improve responsiveness and adaptability in complex IoT environments. [9].

Table 6 provides the DBSCAN-based clustering, ML-driven intrusion detection, and INKS synchronization in terms of accuracy and energy savings. It shows that machine-learning techniques can deliver high detection substantial lifetime gains, message-overhead reductions and accuracy, making ML a dominant enabler for energy-efficient and secure WSN-IoT operation.

Table 6- Comparative Analysis of ML Algorithms in WSN Applications

Algorithm	Accuracy	Energy Savings
DBSCAN Clustering	92% PDR	2.8x lifetime [10]
ML Intrusion Detection	96-100%	Lightweight [2]
INKS Synchronization	72% message reduction	60-75% energy [3]

C. Security Enhancements

- Blockchain: Distributed trust (95% resilience)
- Lightweight Crypto: AES-128 (1.2mJ/encryption)
- DFF-MAC: Cognitive radio security (+44% urban connectivity) [4].

D. Next-Gen Networking

- SDWSN: OpenFlow control (2.6x scalability) [1]
- 5G/6G: 100x bandwidth, <1ms latency

X. RESEARCH METHODOLOGIES IN WSN-IOT STUDIES.

In WSN–IoT studies research methodologies are predominantly simulation-driven and algorithmic, combining analytical modeling with experimental evaluation on synthetic network scenarios. Typical works first define system and radio models, assumptions, and performance metrics, then design new clustering, routing, or reliability schemes using tools such as fuzzy logic, MCDM (entropy–TOPSIS, AHP), metaheuristics, or SDN-based controllers, and finally validate them via simulations (e.g., NS2/NS3, MATLAB, OMNeT++) over randomized node deployments while comparing against baseline protocols like LEACH, HEED, LEACH-C, and others.[10][16][1][20].

Table 7 categorizes dominant WSN-IoT research methodologies into simulation, testbeds, AI-driven development, and domain-specific case studies, linking each to typical tools and validation styles. This overview underlines the current reliance on simulation while also highlighting the growing role of hardware testbeds and AI-centric experimental designs.

Table 7- Research Methodologies in WSN-IoT Studies.

Methodology	Tools	Validation
Simulation [1][4]	NS-3, OMNeT++	95% correlation
Testbeds (25-node grids) [3]	Arduino Nano RF, TelosB	Real hardware
AI Development [10]	PSO/DBSCAN/MCDM	38% improvement
Case Studies [5][8]	Agriculture/Water	Domain-specific

XI. RESEARCH GAP

Existing WSN–IoT research still shows clear gaps: most methods are validated only in 2D, small-scale, static, or idealized scenarios, so their behavior under realistic 3D, mobile, obstacle-rich, or harsh environments remains uncertain. Energy-aware clustering and SDWSN routing schemes often optimize lifetime or load balance but give limited treatment to joint reliability, security, and QoS guarantees across heterogeneous IoT applications, especially under traffic bursts and node/link failures. There is also little integration of multi-criteria CH/routing decisions with real deployment constraints (hardware heterogeneity, imperfect sensing, big-data backends), and few works quantify execution complexity and controller bottlenecks in large networks, leaving a gap between simulation results and deployable, scalable WSN–IoT solutions.[10][20][1].

Table 8 illustrate major research gaps across energy, urban connectivity, scalability, security, and synchronization, and associates them with quantified evidence such as energy waste, PDR drops, and message overhead. The table motivates future work on scalable, secure, and energy-aware frameworks that remain robust under realistic, large-scale, and interference-rich WSN-IoT deployments.

Table 8- Prioritized Research Gaps in WSN-IoT Systems

Priority	Gap Category	Key Evidence	Impact
Energy [20]	Data redundancy wastes60-80%energy	"Energy consumption still needs addressing"	2.8x lifetime gap
Urban [4]	62%urban PDR → cognitive radio needed	"Harsh urban interference n=4 path loss"	+44% connectivity loss
Scale [1], [3][4][10] [20]	All methods fail>1K nodes	50 nodes max tested	16% PDR drop
Security [20]	"Routing attacks unaddressed"	No security in path reliability	95% vulnerable
Sync [3]	72%message overhead	25 vs 7 messages	60-75% energy waste

XII. RECENT INNOVATIONS AND FUTURE TRENDS

Emerging technologies like blockchain enable decentralized trust management, while quantum sensing promises ultra-sensitive environmental detection. The transition to 6G communications is anticipated to provide ultra-low latency, high bandwidth, and massive connectivity to support future IoT-WSN applications. Bio-inspired architectures and self-sustaining sensor networks, leveraging energy harvesting and adaptive algorithms, are prominent research directions with potential for robust, long-lasting deployments.[9]

XIII. CONCLUSION

WSN–IoT systems are becoming fundamental infrastructure for industrial, urban, agricultural, and environmental applications, yet they must operate under tight energy and resource constraints. Existing work offers many specialized solutions for energy, reliability, routing, SDN-based control, and security, but these dimensions are still too often treated separately rather than as a unified design problem. Security coverage is particularly uneven: a few studies analyse attacks and defences in depth, while many protocol and application papers include little or no built-in protection. Moreover, most evaluations rely on idealized simulations with small-scale, static topologies and simplified channels, leaving open questions about behaviour in realistic, large, and dynamic deployments. Totally, these gaps emphasize a strong research opportunity for integrated WSN–IoT frameworks that jointly optimize reliability, energy, QoS, and security, and that are validated under practical deployment scenarios.

REFERENCES

1. E. Hajian, M. R. Khayyambashi and N. Movahhedinia, "A Mechanism for Load Balancing Routing and Virtualization Based on SDWSN for IoT Applications," in IEEE Access, vol. 10, pp. 37457-37476, 2022, doi: 10.1109/ACCESS.2022.3164693.

2. M. A. Jamshed, K. Ali, Q. H. Abbasi, M. A. Imran and M. Ur-Rehman, "Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review," in IEEE Sensors Journal, vol. 22, no. 6, pp. 5482-5494, 15 March15, 2022, doi: 10.1109/JSEN.2022.3148128.

3. M. Elsharief, A. Emran, H. Hassan, S. R. Sabuj and H. -S. Jo, "Energy-Efficient Synchronization in Industrial Internet of Things: An Intelligent Neighbor-Knowledge Approach," in IEEE Transactions on Industrial Informatics, vol. 20, no. 6, pp. 8548-8558, June 2024, doi: 10.1109/TII.2024.3369236.

4. K. M. Bataihah, H. B. Salameh, H. Al-Obiedollah, M. Al-Nairat and Y. Jararweh, "Improving Connectivity in Urban IoT-Based Wireless Sensor Networks: A Nonorthogonal Cognitive-Based Power Allocation," in IEEE Sensors Journal, vol. 24, no. 5, pp. 5530-5538, 1 March1, 2024, doi: 10.1109/JSEN.2023.3301622.

5. M. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie and T. Shongwe, "Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications: A Survey," in IEEE Access, vol. 11, pp. 145813-145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

6. Y. Y. Ghadi et al., "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," in IEEE Access, vol. 12, pp. 12699-12719, 2024, doi: 10.1109/ACCESS.2024.3355312.

7. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review. *Sensors* **2022**, *22*, 2087. https://doi.org/10.3390/s22062087

8. G. A. López-Ramírez and A. Aragón-Zavala, "Wireless Sensor Networks for Water Quality Monitoring: A Comprehensive Review," in IEEE Access, vol. 11, pp. 95120-95142, 2023, doi: 10.1109/ACCESS.2023.3308905.

9. M. Trigka and E. Dritsas, "Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends," in IEEE Access, vol. 13, pp. 96365-96399, 2025, doi: 10.1109/ACCESS.2025.3572328.

10. L. Sahoo, S. S. Sen, K. Tiwary, S. Moslem and T. Senapati, "Improvement of Wireless Sensor Network Lifetime via Intelligent Clustering Under Uncertainty," in IEEE Access, vol. 12, pp. 25018-25033, 2024, doi: 10.1109/ACCESS.2024.3365490.

11. B. Mostefa and G. Abdelkader, "A survey of wireless sensor network security in the context of Internet of Things," 2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Münster, Germany, 2017, pp. 1-8, doi: 10.1109/ICT-DM.2017.8275691.

12. A. Ojha, P. Chanak and O. J. Pandey, "Energy Aware Obstacle Avoidance Data Routing Scheme for IoT Enabled Wireless Sensor Networks," in IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 2644-2653, May 2025, doi: 10.1109/TCE.2025.3576830.

13. K. L. Ranganayagi, S. P. Kumar, D. Lingaraja, T. Aravind, S. Ramya and G. D. Ram, "Energy-Efficient Communication Protocols for 6G Wireless Sensor Network," 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICNWC60771.2024.10537356.

14. S. Palarimath, P. Maran, W. B. N.R, T. Sujatha, S. Renuga and C. R.S, "Exploring the Role of Internet of Things in Wireless Sensor Networks for Industry 4.0 Applications," 2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT), Delhi, India, 2024, pp. 616-621, doi: 10.1109/IC2SDT62152.2024.10696702.

15. G. Tuteja, S. Rani, A. Sharma and S. Singla, "Integrating Wireless Sensor Networks with IoT for Enhanced Data-Driven Industry Solutions*," 2024 3rd International Conference for Advancement in Technology (ICONAT), GOA, India, 2024, pp. 1-6, doi: 10.1109/ICONAT61936.2024.10774682.

16. H. K. Sivaraman and R. L, "Minimizing the Energy Consumption and Enhancing the Network Lifetime in WSN using Advanced LEACH Protocol," 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 2022, pp. 1-6, doi: 10.1109/ICERECT56837.2022.10059740.

17. S. K. R, L. K, A. P. M and S. K, "Security Techniques in Wireless Sensor Networks - A Comprehensive Survey," 2021 Smart Technologies, Communication and Robotics (STCR), Sathyamangalam, India, 2021, pp. 1-6, doi: 10.1109/STCR51658.2021.9588872.

18. Nelli, Arundhati, Mangasuli, Sushant, Patel, Pratham,“ Wireless Sensor Networks: An Overview on Security Issues and Challenges”, SSRN Electronic Journal, Vol-3, Issue-3, Mar- 2017, ISSN: 2454-1311, https://dx.doi.org/10.24001/ijaems.3.3.10

19. A. Gupta, T. Gulati and A. K. Bindal, "WSN based IoT applications: A Review," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), Nagpur, India, 2022, pp. 1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791495.

20. N. Vishnoi and R. K. Dwivedi, "Comprehensive Survey on the Reliability of Wireless Sensor Networks," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 496-502, doi: 10.1109/SMART55829.2022.10047428.

AUTHORS

Manasa G pursued Bachelor of Engineering in Electronics & Communication from Sapthagiri College of Engineering (affiliated to VTU, Belagavi), Bengaluru, in the year 2015, M.Tech degree in Digital Electronics from VTU extension centre, UTL technologies, Bengaluru, in the year 2019. Currently she is pursuing Ph.D. under the faculty of electrical & electronics engineering sciences.

Rangaiah L pursued B.Tech in Electronics and Communication Engineering from NBKR Institute of Science and Technology (Affiliated to S V University), Vakadu, Nellore Dist, 1996, M.Tech in Communication Engineering from Bharath Institute of Higher Education and Research, Chennai,2005 and completed Ph. D in Electronics and Communication Engineering from University of Allahabad (Central University), Allahabad, 2011. He has 27 years of teaching experience. He is serving as Research guide in VTU and 5 scholars Awarded Ph.D., and Guiding 5 Ph. D Scholars in the area of wireless Communications from VTU, Belagavi. He is a Fellow member of IETE and many professional societies. Currently working as a Professor & Dean-academics in Rajarajeswari College of Engineering, Bengaluru.