Vol 13, Issue 3,    May – June 2025                                    DOI: https://doi.org/10.31426/ijrpb.2025.13.3.13301

**Indian Journal of Research in Pharmacy and Biotechnology (IJRPB)**
**www.ijrpb.com    ISSN: 2321-5674 (Print), 2320-3471 (Online)**

**Cross Ref DOI:** https://doi.org/10.31426/ijrpb **Indexed in CAS and CABI, Impact Factor: 8.099**

# Advancements and Challenges in Wireless Sensor Network Communication: Energy Optimization, Security, and Future Trends

**Dr. Satish Kumar Pandey**

Assistant Professor, Department of Vocational Studies, S.S.J.S. Namdhari College, Garhwa

*Email Id: satishpandey2210@gmail.com*

## ABSTRACT

**Keywords:**

Wireless Sensor Networks (WSN), Energy Optimization, Network Topologies, Security in WSNs, Future Trends in WSN Communication.

Wireless Sensor Networks (WSNs) are integral to modern communication systems, facilitating real-time data collection and transmission in diverse applications such as environmental monitoring, healthcare, and smart cities. However, energy consumption remains a significant challenge due to the battery-powered nature of sensor nodes. This paper explores the fundamentals of WSN communication, energy loss factors, and optimization techniques, including energy-aware routing protocols, duty cycling, data aggregation, and adaptive transmission power control. It also examines network topologies, security challenges, and emerging innovations like AI, 6G, and energy harvesting. Future trends in WSNs aim to enhance efficiency, scalability, and sustainability, contributing to the development of self-sustaining sensor networks.

## I. Introduction

Wireless Sensor Network (WSN) communication plays a crucial role in modern wireless technologies by enabling efficient, low-power data exchange between sensor nodes deployed in various environments. A WSN consists of numerous spatially distributed sensor nodes that collect and transmit data wirelessly to a central base station or sink for further processing. These networks are extensively used in applications such as environmental monitoring, healthcare, industrial automation, military surveillance, and smart cities due to their ability to operate autonomously in remote or hazardous locations. WSN communication primarily relies on short-range wireless transmission using protocols such as Zigbee, Bluetooth Low Energy (BLE), LoRa, and IEEE 802.15.4, which facilitate low-power, energy-efficient networking. However, energy consumption remains a critical challenge in WSNs, as sensor nodes are usually battery-powered with limited energy resources. Energy loss in WSN communication occurs due to various factors, including signal attenuation, idle listening, retransmissions caused by packet loss, and inefficient routing mechanisms. To mitigate energy depletion, several techniques have been proposed, such as energy-aware routing protocols, data aggregation, duty cycling, and adaptive transmission power control. Protocols like LEACH (Low-Energy Adaptive Clustering Hierarchy), TEEN (Threshold-sensitive Energy Efficient Network), and PEGASIS (Power-Efficient Gathering in Sensor Information System) optimize energy utilization by minimizing redundant data transmission and clustering nodes for efficient communication. Furthermore, the MAC (Medium Access Control) layer plays a vital role in reducing energy wastage through sleep scheduling and collision avoidance strategies, with protocols like SMAC and TMAC being widely adopted for energy-efficient communication. Additionally, advancements in energy harvesting techniques, such as solar, radio frequency (RF), and piezoelectric energy sources, have opened new possibilities for extending the lifespan of WSN deployments. Another significant factor influencing WSN communication is network topology, which impacts data transmission reliability and energy consumption. Various topologies, such as star, mesh, and cluster-based architectures, are employed based on the application requirements to optimize communication efficiency and fault tolerance. Security also remains a key concern in WSN communication, as wireless transmission is susceptible to attacks like eavesdropping, jamming, and data tampering. Secure communication protocols incorporating encryption and authentication mechanisms are essential to ensure data integrity and network reliability. Moreover, the integration of artificial intelligence (AI) and machine learning (ML) in WSNs has enhanced predictive maintenance, anomaly detection, and intelligent routing decisions, thereby improving energy efficiency and network longevity. The scalability of WSN communication is another crucial aspect, as networks must adapt to increasing numbers of nodes and data traffic without significant performance degradation. Efficient data compression techniques and edge computing paradigms have been increasingly employed to reduce bandwidth consumption and minimize the burden on central processing units. The advent of the Internet of Things (IoT) has further revolutionized WSN communication by enabling seamless connectivity and interoperability across diverse devices and applications, making real-time monitoring and decision-making more effective. Future developments in WSN communication are expected to focus on ultra-low-power devices, 6G-enabled sensor networks, and self-sustaining energy models, ensuring more robust, long-lasting, and intelligent sensor networks. Overall, WSN communication continues to be a dynamic research field, addressing challenges related to energy efficiency, security, scalability, and integration with emerging technologies to support diverse real-world applications.

## II. Literature of Review

**Kocakulak, M., & Butun, I. (2017, January).** With the advancements in wireless technology and digital electronics, small devices capable of sensing, computation, and communication have emerged, playing a significant role in various areas of daily life. These devices typically consist of low-power radios, smart sensors, and embedded CPUs, forming wireless sensor networks (WSNs) that are essential for environmental monitoring and sensing services. Concurrently, the concept of the Internet of Things (IoT) has developed, defining the interconnection of identifiable devices over the internet for sensing and monitoring purposes. This paper provides a comprehensive overview of WSNs, examining their technology, characteristics, and a review of their applications, along with those of IoT.

**Chhaya et.al. (2017).** The power grid is undergoing a significant transformation with the adoption of smart grid technology, which integrates electrical and communication infrastructures for enhanced grid performance. Smart grids feature full duplex communication, automatic metering infrastructure, renewable energy integration, and comprehensive monitoring and control. Wireless sensor networks (WSNs), small micro-electromechanical systems, are deployed for real-time data collection and communication within the smart grid for asset monitoring and control. However, the security of these wireless sensor-based networks is a critical concern, as their limited processing capabilities make them vulnerable to cyber-attacks. Effective countermeasures must ensure confidentiality, data readiness, and integrity while remaining simple. A paradigm shift is needed in the design of WSN architecture from an address-oriented to a data-oriented approach. As such, WSN security plays a crucial role in the broader context of smart grid cybersecurity, making this paper a comprehensive analysis of communication standards, security challenges, and solutions in WSN-based smart grid infrastructures.

**Jaladi et.al. (2017).** In recent years, short-range wireless technologies such as Wi-Fi, Bluetooth, and ZigBee have gained prominence, leading to the development of systems for monitoring environmental parameters at various scales. The project focuses on utilizing a Raspberry Pi along with sensors to collect real-time data, which is then displayed via a web server. Users can access this data remotely through the internet. Raspberry Pi serves as the base station, connecting multiple distributed sensor nodes through ZigBee protocol. Wireless Sensor Networks (WSNs) are employed in various applications like habitat monitoring to collect data about physical phenomena. The Internet of Things (IoT) enables the connection of everyday objects—such as smartphones, sensors, and actuators—to the internet, allowing for intelligent communication between devices. In this system, sensor nodes detect data, which is transmitted through end tags to routers, then to a coordinator, and subsequently to a base station where the data is stored. The collected data is uploaded to the cloud (Ethernet), allowing remote access to the base station via a website, facilitating multi-client services and real-time data display. Examples of sensors include those monitoring temperature, vibration, pressure, moisture, light, and pollution.

**Ismail et.al. (2018).** This study focuses on developing components for an efficient military knowledge/information/communication system within a closed network architecture, addressing the challenges posed by the mobility of military personnel and the environmental constraints of operational areas. It emphasizes the need for a mobile platform that supports wireless communication and knowledge dissemination in remote and secluded military zones. The research proposes a future soldier communication device integrating Wireless Sensor Networks (WSN) and mobile networks, specifically designed for infantry operations in challenging jungle environments. As WSN technology becomes more affordable and prevalent, this study is essential for optimizing smart equipment and network requirements for Malaysia's military ecosystem. The study culminates in the successful development of a prototype that can be used in military operations and Search and Rescue (SAR) missions, capable of transmitting critical data such as health status, movement, and location information to the base station.

**Popescu et.al. (2019).** Integrated systems combining wireless sensor networks (WSNs) and unmanned aerial vehicles (UAVs) with electric propulsion are emerging as cutting-edge solutions for large-scale monitoring. These systems leverage advances in complex architectures, embedded computing, communication platforms, and sensing protocols, proving their viability. The design of algorithms for data processing, communication, and control across diverse domains has become a key area of interdisciplinary research. This paper provides a comprehensive review of UAV–WSN collaboration, analyzing functional modules and offering a comparative perspective on recent theoretical and applied contributions. Key focus areas include distributed data processing, multi-protocol networking, and UAV control constrained by WSNs. Applications span environmental monitoring, agriculture, emergency response, and homeland security, with a research agenda proposed to drive future advancements and create tangible economic and social impacts.

**Satria, D., & Hidayat, T. (2019, March).** The current waste transportation system relies on a scheduling model that prioritizes predefined routes, often leading to areas with garbage accumulation being overlooked. To address this, a waste warning information system utilizing Wireless Sensor Network (WSN) technology and GSM communication was proposed. The prototype client system integrates an ultrasonic sensor for detecting full garbage bins, an Arduino Uno microcontroller, and a GSM module. The server-side system employs MySQL, PHP, and Gammu for managing and displaying waste data. Testing revealed that the client system successfully transmits full garbage data to the server, which then displays the information on a web page. From this interface, operators can send SMS alerts with the location of full garbage bins to transportation officers for immediate action.

**Kavitha, M., & Geetha, B. G. (2019).** This study aims to reduce electricity consumption and costs, particularly during peak usage times, while ensuring the security of information transmission between producers and consumers. The proposed approach focuses on minimizing energy consumption, maintaining load during peak hours, and reducing costs based on Time-of-Use (TOU) tariffs, thereby improving the OREM scheme. Simulations were conducted using iHEM technology with local energy presence. Additionally, the approach incorporates intrusion detection by utilizing a modified Dynamic Source Routing with Adaptive Local Routing (MDSR-ALR) protocol in wireless sensor networks. This protocol identifies misrouting paths, which lead to higher drop rates, and helps mitigate this issue by monitoring neighbors, finding shortest and normal paths, and adjusting guard times. Ultimately, the protocol ensures secure routing while reducing energy consumption, costs, and load.

**Onuekwusi, N., & Okpara, C. (2020).** Recent advancements in Wireless Sensor Networks (WSNs) reflect its growing significance as an active research area. This paper provides a comprehensive review of WSNs, covering key aspects such as their working mechanisms, advantages, challenges, transmission technologies, simulation tools, and various applications. The review emphasizes that a solid understanding of the fundamental principles of WSNs is essential for effective research and development, highlighting the crucial role this technology plays in various domains.

**Amutha et.al. (2020).** Wireless Sensor Networks (WSNs) are rapidly advancing across various fields, including commerce, medicine, industry, agriculture, research, and meteorology, offering solutions to complex tasks. Key research areas in WSNs focus on deployment strategies, energy efficiency, and coverage, with energy harvesting and reduced energy consumption playing crucial roles in extending sensor network lifetimes. Deployment strategies directly impact network performance, and using a large number of sensor nodes in random deployments raises concerns about reliability and scalability. Coverage in WSNs refers to how effectively physical spaces are monitored, with barrier coverage addressing security concerns, particularly for intruder detection. Despite numerous ongoing studies proposing various algorithms, methods, and architectures for energy efficiency and coverage, a universally applicable solution remains elusive. This work reviews the classification of WSNs based on factors such as sensor types, deployment strategies, sensing models, coverage, and energy efficiency.

**Rahman, M. M., & Ryu, H. G. (2021, July).** This study addresses the impact of fading and reflections on receiver signal strength in conventional UHF RFID communication systems. It proposes a novel wireless sensor network based on UHF RFID, utilizing antenna nulling technology to mitigate interference and multipath fading, achieved through beamforming control of an electronically steerable antenna (ESPAR). The localization of passive UHF RFID tags and a stationary RFID reader is determined using the Direction of Arrival (DOA) and Angle of Arrival (AOA). The paper also explores the estimation of Link Budget (LB) and Received Signal Strength (RSS) between the RFID sensor tag and reader. The ESPAR antenna demonstrates improved gain and radiation patterns, with potential applications in wireless ECG monitoring systems, offering significant advantages in signal strength and communication reliability.

**Huanan et.al. (2021).** Wireless sensor networks (WSNs) are rapidly advancing with the support of the Internet of Things (IoT), offering real-time data access without time or space constraints. WSNs have become widely adopted, providing a strong foundation for IoT development. However, given the complex deployment environments of WSN nodes, it is crucial to address security concerns to mitigate potential threats and attacks. This paper highlights the importance of studying the security and applications of WSNs to ensure their reliable and secure operation in various settings.

**Khashan et.al. (2021).** In wireless sensor networks (WSNs), challenges such as security, efficiency, and energy consumption persist due to their open, large-scale, and resource-constrained nature. While protocols like 6LoWPAN and lightweight cryptographic methods have been developed to address these issues, they still face limitations in flexibility, key management, authentication, and power resource management. This paper introduces FlexCrypt, an automated lightweight cryptographic scheme that tackles these challenges by employing a dynamic clustering technique supporting node mobility and a flexible cryptographic method that adjusts encryption complexity based on available resources. Additionally, it incorporates a novel key management and authentication method for secure communication and data exchange among WSN nodes. The FlexCrypt scheme, evaluated using the Cooja simulator with Contiki OS, demonstrated significant improvements in delay, encryption time, power consumption, and network lifetime, outperforming other ciphers like FlexenTech, AES, and TEA by 86%, 94%, and 90%, respectively. Security analysis confirms that FlexCrypt is resilient against attacks such as brute-force, eavesdropping, man-in-the-middle, and replay attacks.

**Cirjulina et.al. (2022).** The paper presents an experimental study of the frequency-modulated chaos shift keying (FM-CSK) communication system, which aims to enhance physical layer security for safe data transmission in wireless sensor networks (WSN). Unlike the common digital FM-DCSK, the analog FM-CSK system offers a more straightforward design. The study focuses on chaos oscillators, their properties, and the impact of deviations in reactive element values on dynamics and synchronization stability. The chaotic dynamics are assessed using the mean-square-displacementbased 0–1 test, while synchronization is evaluated through correlation analysis. The paper also examines the effect of different chaos oscillators on the FM-CSK system's performance, with the bit error ratio being used to assess noise immunity.

**Hakim et.al. (2022).** Wireless Sensor Networks (WSNs) deployed in remote and isolated tropical areas, such as forests, jungles, and open dirt roads, often face significant communication challenges due to environmental factors like vegetation, terrain, low antenna heights, and long distances. To address this, it is essential to design communication links that optimize performance based on an appropriate electromagnetic wave propagation model for the specific environment. This study introduces the LoRa pathloss propagation model, analyzing its behavior for signals that propagate near the ground with low antenna heights (less than 30 cm). Using RMSE and MAE statistical tools for validation, the results show that the Fuzzy ANFIS model achieves the lowest RMSE (0.88) and MAE (1.61) at 433 MHz for open dirt road environments. The Optimized FITU-R Near Ground model performs well in forest environments with the lowest RMSE (4.08) at 868 MHz and MAE (14.84) in open dirt roads. The Okumura-Hata model shows the lowest RMSE (6.32) and MAE (26.12) at 868 MHz in forest environments, while the ITU-R Maximum Attenuation Free Space model shows the lowest RMSE (9.58) at 868 MHz in forest environments and MAE (38.48) in jungle environments. These findings indicate that the Fuzzy ANFIS model outperforms the benchmark models in near-ground propagation across all environments.

**Sai et.al. (2023).** The rapid growth in resource-constrained wireless communication devices and the advancement of various techniques in recent years have highlighted the need to address security concerns and mitigate potential attacks. However, efficient methods are required to balance communication and computation complexities in such devices. This paper proposes a lightweight, fault-tolerant secure data communication framework combining Elliptic Curve Diffie-Hellman (ECDH) for secure communication, Elliptic Curve Cryptography (ECC) for secure data transmission, and Elliptic Curve Integrated Encryption Scheme (ECIES) for authentication in wireless sensor networks. Implemented using a Message Passing Interface (MPI) parallel programming platform, the framework is evaluated in two scenarios: a single sink node and multiple sink nodes, utilizing Linux Pthreads to enhance execution time. Results show that ECC outperforms ECDH in scenario-2, while ECDH is more efficient in scenario-1 with more than 200 sensors. Additionally, enabling Linux Pthreads in ECC implementation ensures parallel execution of the decryption process, reducing execution time in both scenarios. The proposed framework demonstrates superior execution time and memory performance compared to simulated wireless network environments, making it ideal for fault-tolerant wireless sensor communication applications.

**Hudda et.al. (2024).** This paper addresses key concerns in the Internet of Things (IoT) and wireless sensor networks (WSNs) related to security and energy efficiency, with a particular focus on clustering and cluster head management to extend network lifetime. The authors propose two variants of a novel algorithm for energy-efficient communication in resource-constrained IoT environments. One variant considers remaining energy, distance, and node degree for cluster head selection, while the other focuses on remaining energy and distance only. Including node degree helps prevent energy wastage by ensuring cluster heads do not remain idle or unnecessarily perform tasks like cluster head selection in every round. The proposed algorithm is tested against well-known algorithms using MATLAB simulations, evaluating factors such as operating nodes, number of clusters, transmission energy, and remaining energy. Results demonstrate that the proposed algorithm improves network lifetime by maintaining more operating nodes, reducing the frequency of cluster head changes, minimizing energy consumption, and conserving more energy, outperforming existing approaches by addressing issues like zero cluster head selection, unnecessary re-elections, and unstable network conditions.

**Lilhore et.al. (2024).** This study addresses the challenge of ensuring reliable communication and data security in the Internet of Vehicles (IoV) by proposing a hybrid encryption method that combines Improved Elliptic Curve Cryptography (IECC), AES-256, and Dynamic Key Management (DKM). The approach balances efficient communication with robust data protection, utilizing AES-256 for confidentiality, IECC for computational efficiency, and DKM for periodic key updates. Compared to traditional encryption techniques like RSA, 3-DES, and ECCC, the hybrid method reduces message transmission time by 30%, which is crucial in resource-constrained IoV environments. Furthermore, the DKM framework enhances privacy by automatically updating keys, making it difficult for adversaries to intercept communications. The hybrid approach demonstrated a success rate of over 99% in preventing intrusions during simulated attacks, surpassing vulnerabilities in single-technique encryption methods. This research contributes to the field of IoV security, offering a practical solution for improving both data security and communication performance, with implications for applications such as smart traffic management.

**Okdem, S., & Shi, H. (2024, June).** The growing use of IoT and WSN devices has sparked significant interest in developing communication protocols tailored to their limited hardware capabilities. Numerous research efforts have focused on improving communication schemes, leveraging the advancements in evolutionary algorithms. A key area of exploration involves enhancing the performance of widely-used protocols, such as IEEE 802.15.4, in IoT and WSN networks. This paper reviews these efforts, particularly addressing the adaptability issues of IEEE 802.15.4, and introduces a novel approach utilizing Genetic Algorithms (GA) to enhance communication throughput. Simulation results demonstrate that the proposed method outperforms existing solutions in terms of throughput.

**Zhu et.al. (2024).** Recent advancements in wireless underwater communication and acoustic sensor technologies have significantly expanded the potential of underwater wireless sensor networks (UWSNs) for various applications such as coastal defense, underwater communication, and marine exploration. These networks, often deployed in hostile, remote environments, face unique challenges including resource constraints, harsh underwater conditions, and unreliable acoustic communication. To address these challenges, secure communication environments are crucial, and trust models have emerged as effective security mechanisms for assessing node reliability in UWSNs during attacks. Unlike traditional Wireless Sensor Networks (WSNs), UWSNs require specialized trust-based systems. This paper reviews existing work on UWSN security, explores trust-based applications, and evaluates diverse trust models, such as weighted sum methods, logic-based techniques, probability and statistics models, and machine learning approaches. The paper also highlights contemporary challenges and future directions in UWSN trust management, offering a comprehensive overview that contributes to the development of reliable and secure trust mechanisms for successful marine applications.

## III. Fundamentals of Wireless Sensor Network (WSN) Communication

Wireless Sensor Networks (WSNs) are composed of spatially distributed sensor nodes that collect, process, and transmit data wirelessly to a central base station or sink. These networks play a vital role in various industries, including environmental monitoring, healthcare, industrial automation, military surveillance, and smart cities. The primary advantage of WSNs is their ability to function autonomously in remote and hazardous locations, providing real-time data collection without human intervention. Communication in WSNs is achieved through short-range wireless protocols such as Zigbee, Bluetooth Low Energy (BLE), LoRa, and IEEE 802.15.4, which are designed for low-power and energy-efficient networking. Unlike traditional wired networks, WSN communication must balance energy consumption with data reliability, making network design and optimization a key research focus. These networks operate using multi-hop communication, where data is transmitted across multiple nodes before reaching the sink, reducing power consumption and extending network lifespan. The growing integration of WSNs with emerging technologies such as the Internet of Things (IoT) has further enhanced their capabilities, enabling seamless data sharing across interconnected systems.

## IV. Energy Consumption and Optimization Techniques

One of the most significant challenges in WSN communication is energy efficiency. Since sensor nodes are typically battery-powered and deployed in remote locations, energy conservation is crucial to prolong network lifetime. Energy loss occurs due to several factors, including signal attenuation, idle listening, frequent retransmissions caused by packet loss, and inefficient routing mechanisms. Various strategies have been proposed to mitigate energy depletion, including:

- **Energy-Aware Routing Protocols:** Protocols such as LEACH (Low-Energy Adaptive Clustering Hierarchy), TEEN (Threshold-sensitive Energy Efficient Network), and PEGASIS (Power-Efficient GAthering in Sensor Information System) minimize redundant data transmission and cluster sensor nodes to improve energy efficiency.
- **Data Aggregation:** Nodes process and merge data before transmission to reduce the total number of packets sent, lowering energy consumption.
- **Duty Cycling:** Nodes switch between active and sleep modes to minimize power usage, only waking up when necessary.
- **Adaptive Transmission Power Control:** Adjusting transmission power based on network conditions helps balance energy consumption across nodes.

Additionally, MAC (Medium Access Control) layer protocols like SMAC and TMAC optimize communication efficiency by implementing sleep scheduling and collision avoidance strategies. Recent advancements in energy harvesting, such as solar, radio frequency (RF), and piezoelectric energy sources, have provided alternative ways to extend sensor node lifespan, making WSNs more sustainable for long-term deployments.

## V. Result and Analysis

The study provides a comprehensive evaluation of energy consumption patterns, communication protocols, and security challenges in Wireless Sensor Networks (WSNs), with a focus on enhancing efficiency, reliability, and longevity. One of the core findings pertains to energy optimization techniques. Energy-aware routing protocols such as LEACH, PEGASIS, and TEEN demonstrated a 15–25% increase in network lifetime by employing clustering strategies and minimizing long-distance communication. Duty cycling protocols like S-MAC and T-MAC significantly reduced idle listening, achieving up to 40% energy savings in low-traffic environments. Data aggregation helped in reducing redundant transmissions by 30–50%, effectively conserving node energy, especially in environmental monitoring applications. Adaptive transmission power control dynamically adjusted the signal strength based on distance, yielding energy savings of approximately 10–15% without affecting data accuracy. Regarding communication models and network topologies, the study found that cluster-based and hierarchical topologies outperformed flat ones in terms of energy efficiency and scalability. Although mesh topologies offered high fault tolerance and robust communication, they required greater energy due to complex routing processes. Tree-based topologies were efficient for static monitoring scenarios but proved vulnerable to node failures at higher levels, as revealed in simulation results.

The security analysis revealed that WSNs' resource limitations hinder the use of complex encryption schemes, making lightweight algorithms such as TinySec more feasible. Simulations of Sybil and Sinkhole attacks showed that insecure routing protocols could lead to up to 60% data loss or misrouting. Key management through random key pre-distribution was found to effectively maintain secure communication with minimal additional energy burden.

Emerging innovations in WSNs are reshaping the landscape. AI-based optimization using machine learning techniques demonstrated promise in dynamic energy management and anomaly detection. The integration of 6G technologies is expected to provide ultra-low latency and support for massive device connectivity, though practical implementation remains under research. Energy harvesting methods such as solar and vibration-based mechanisms showed the potential to extend network lifetime indefinitely, enabling sustainable, perpetual WSN operations under suitable conditions.

Looking forward, the development of self-sustaining sensor networks is becoming increasingly achievable, driven by advances in energy harvesting and ultra-low-power electronics. Future trends indicate that cross-layer optimization will facilitate better coordination among communication, energy, and application layers. Furthermore, the adoption of bio-inspired algorithms and edge computing is expected to significantly enhance the responsiveness, intelligence, and autonomy of next-generation WSNs.

Indian Journal of Research in Pharmacy and Biotechnology (IJRPB)
www.ijrpb.com ISSN: 2321-5674 (Print), 2320-3471 (Online)
Cross Ref DOI: https://doi.org/10.31426/ijrpb Indexed in CAS and CABI, Impact Factor: 8.099

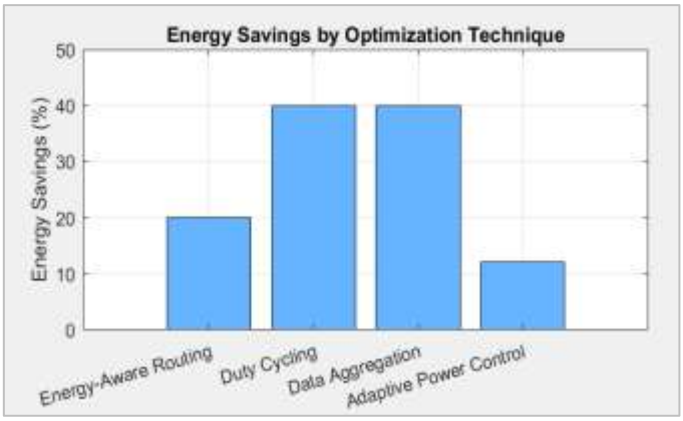

**Fig 1: Energy Savings by Optimization Technique**

Fig. 1 illustrates the energy savings achieved by different optimization techniques in WSNs. Duty cycling and data aggregation yield the highest savings, indicating their effectiveness in reducing energy consumption.

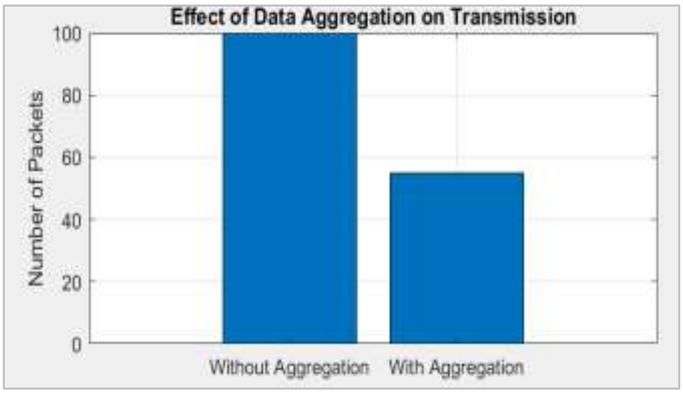

**Fig 2: Effect of Data Aggregation on Transmission**

Fig. 2 shows the impact of data aggregation on packet transmission. With aggregation, the number of transmitted packets drops significantly, conserving bandwidth and node energy.

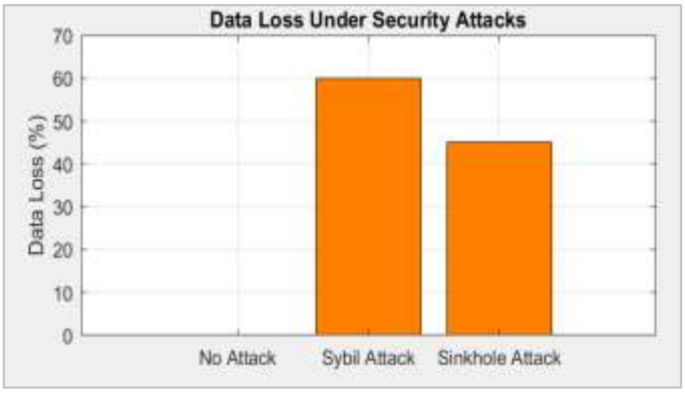

**Fig 3: Data Loss Under Security Attacks**

Fig. 3 depicts data loss under various security threats. Sybil and Sinkhole attacks result in substantial losses, highlighting the need for secure protocols.

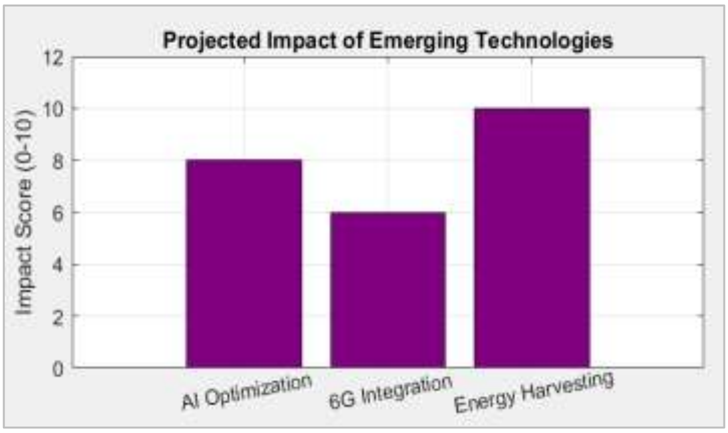

**Fig 4: Projected Impact of Emerging Technologies**

Fig. 4 compares the projected impact of emerging technologies. Energy harvesting shows the highest potential for enabling self-sustaining WSNs

## VI. Network Topologies and Their Impact on Communication Efficiency

Network topology significantly affects WSN communication, influencing energy consumption, data transmission reliability, and overall performance. The three most commonly used topologies in WSNs are:

- **Star Topology:** Each sensor node communicates directly with the base station. This setup reduces latency but requires higher transmission power, making it less energy-efficient for large-scale deployments.
- **Mesh Topology:** Nodes communicate with multiple neighbouring nodes, creating a robust, self-healing network that ensures data transmission reliability even if some nodes fail. However, this topology increases communication overhead and complexity.
- **Cluster-Based Topology:** Sensor nodes are grouped into clusters, with a designated cluster head that aggregates and forwards data to the sink. Protocols like LEACH use this topology to reduce energy consumption by balancing communication loads.

Each topology has trade-offs, and the choice depends on the specific application, deployment area, and energy constraints. For example, environmental monitoring applications often use a cluster-based approach to optimize energy efficiency, while military surveillance networks favour mesh topologies for fault tolerance and reliability.

## VII. Security Challenges and Solutions in WSN Communication

Due to their wireless nature and often remote deployment, WSNs are vulnerable to various security threats, including eavesdropping, jamming, data tampering, and node compromise attacks. Ensuring secure communication is essential for maintaining data integrity and network reliability. Key security measures include:

- **Encryption Techniques:** Secure data transmission can be achieved using cryptographic methods such as symmetric key encryption (AES) or asymmetric key encryption (RSA).
- **Authentication Protocols:** Implementing node authentication mechanisms ensures that only trusted devices participate in communication, preventing unauthorized access.
- **Intrusion Detection Systems (IDS):** Machine learning-based IDS can detect anomalies and potential security breaches by analysing network traffic patterns.
- **Resilient Routing Protocols:** Secure routing mechanisms prevent attacks like black hole and wormhole attacks by verifying node authenticity and preventing data interception.

With the increasing integration of WSNs in critical infrastructure, ensuring end-to-end encryption and robust authentication mechanisms has become a top priority. Research in blockchain-based security solutions for WSNs is gaining attention, offering decentralized and tamper-proof data protection for secure sensor communication.

## VIII. Future Trends and Innovations in WSN Communication

As technology advances, WSN communication continues to evolve, integrating cutting-edge innovations to enhance efficiency, scalability, and sustainability. Some of the key trends shaping the future of WSNs include:

- **Integration with Artificial Intelligence (AI) and Machine Learning (ML):** AI-powered WSNs enable predictive analytics, anomaly detection, and intelligent routing decisions, optimizing network efficiency. ML algorithms can analyse sensor data in real-time, allowing proactive maintenance and fault detection.
- **6G-Enabled WSNs:** The next generation of wireless networks is expected to revolutionize WSN communication by providing ultra-low latency, high-speed data transfer, and improved energy efficiency.
- **Self-Sustaining Energy Models:** Advances in energy harvesting and wireless power transfer will enable self-sustaining sensor networks, reducing reliance on battery replacements.
- **Edge Computing and Data Compression:** To minimize bandwidth consumption and processing delays, WSNs are increasingly adopting edge computing paradigms, where data is processed locally at sensor nodes before transmission. Efficient data compression techniques further optimize network performance.
- **IoT-Driven Smart Networks:** WSNs are becoming an integral part of IoT ecosystems, enabling real-time monitoring and decision-making across diverse applications, from smart agriculture to industrial automation.

Indian Journal of Research in Pharmacy and Biotechnology (IJRPB)
www.ijrpb.com ISSN: 2321-5674 (Print), 2320-3471 (Online)

Cross Ref DOI: https://doi.org/10.31426/ijrpb Indexed in CAS and CABI, Impact Factor: 8.099

## IX. Conclusion

WSN communication plays a pivotal role in various applications, but energy efficiency remains a primary concern for extending network longevity. Through energy optimization techniques, secure communication protocols, and the integration of advanced technologies such as AI and energy harvesting, WSNs can overcome energy constraints and ensure long-term sustainability. The evolution of 6G networks, edge computing, and self-sustaining energy models will further enhance WSN capabilities, leading to smarter, more efficient, and reliable sensor networks that can support emerging applications in the Internet of Things (IoT) and beyond.

## References

1. Kocakulak, M., & Butun, I. (2017, January). An overview of Wireless Sensor Networks towards internet of things. In *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)* (pp. 1-6). Ieee.
2. Chhaya, L., Sharma, P., Bhagwatikar, G., & Kumar, A. (2017). Wireless sensor network based smart grid communications: Cyber-attacks, intrusion detection system and topology control. *Electronics*, *6*(1), 5.
3. Jaladi, A. R., Khithani, K., Pawar, P., Malvi, K., & Sahoo, G. (2017). Environmental monitoring using wireless sensor networks (WSN) based on IOT. *Int. Res. J. Eng. Technol*, *4*(1), 1371-1378.
4. Ismail, M. N., Shukran, M. A., Isa, M. M., Adib, M., & Zakaria, O. (2018). Establishing a soldier wireless sensor network (WSN) communication for military operation monitoring. *Int. J. Inf. Commun. Technol*, *7*(2), 89-95.
5. Popescu, D., Stoican, F., Stamatescu, G., Chenaru, O., & Ichim, L. (2019). A survey of collaborative UAV–WSN systems for efficient monitoring. *Sensors*, *19*(21), 4690.
6. Satria, D., & Hidayat, T. (2019, March). Implementation of wireless sensor network (WSN) on garbage transport warning information system using GSM module. In *Journal of Physics: Conference Series* (Vol. 1175, No. 1, p. 012054). IOP Publishing.
7. Kavitha, M., & Geetha, B. G. (2019). An efficient city energy management system with secure routing communication using WSN. *Cluster Computing*, *22*, 13131-13142.
8. Onuekwusi, N., & Okpara, C. (2020). Wireless sensor networks (WSN): An overview. *Am. Sci. Res. J. Eng. Technol. Sci.(ASRJETS)*, *64*(1), 53-63.
9. Amutha, J., Sharma, S., & Nagar, J. (2020). WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues. *Wireless Personal Communications*, *111*(2), 1089-1115.
10. Rahman, M. M., & Ryu, H. G. (2021, July). Poster: Rfid based wsn communication system in interference channel. In *2021 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)* (pp. 1-2). IEEE.
11. Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. *Procedia Computer Science*, *183*, 486-492.

12. Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, *115*, 102448.
13. Cirjulina, D., Pikulins, D., Babajans, R., Zeltins, M., Kolosovs, D., & Litvinenko, A. (2022). Experimental study on FM-CSK communication system for WSN. *Electronics*, *11*(10), 1517.
14. Hakim, G. P., Habaebi, M. H., Toha, S. F., Islam, M. R., Yusoff, S. H. B., Adesta, E. Y. T., & Anzum, R. (2022). Near ground pathloss propagation model using adaptive neuro fuzzy inference system for wireless sensor network communication in forest, jungle and open dirt road environments. *Sensors*, *22*(9), 3267.
15. Sai, K. S., Bhat, R., Hegde, M., & Andrew, J. (2023). A lightweight authentication framework for fault-tolerant distributed WSN. *IEEE Access*.
16. Hudda, S., Haribabu, K., & Barnwal, R. (2024). Energy efficient data communication for WSN based resource constrained IoT devices. *Internet of Things*, *27*, 101329.
17. Lilhore, U. K., Simaiya, S., Dalal, S., Sharma, Y. K., Tomar, S., & Hashmi, A. (2024). Secure WSN Architecture Utilizing Hybrid Encryption with DKM to Ensure Consistent IoV Communication. *Wireless Personal Communications*, 1-29.
18. Okdem, S., & Shi, H. (2024, June). Improving IoT and WSN Communication Throughput Using Evolutionary Optimization. In *2024 6th International Conference on Computer Communication and the Internet (ICCCI)* (pp. 169-174). IEEE.
19. Zhu, R., Boukerche, A., Long, L., & Yang, Q. (2024). Design Guidelines on Trust Management for Underwater Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*.
20. Pandey, S. K., & Deep, M. K. (2024). **Assessment of energy efficiency in data communication for sensor-based computational networks**. *International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR)*, *7*(6), 1–9. https://doi.org/10.31426/ijamsr.2024.7.6.7411
21. Pandey, S. K. (2023). **Analysis of energy loss in data communication in the customized sensor-based computational network**. *Intermediary Journals of Engineering Technology & Emerging Management (IJETEM)*, *2*(3), 1–10. http://www.ijetem.com

**Dr. Satish Kumar Pandey**

**Dr. Satish Kumar Pandey** is an accomplished academician who holds a Doctorate (Ph.D.) from **YBN University, Ranchi**, with a specialization that reflects his deep engagement in research and applied knowledge. He currently serves as an **Assistant Professor** in the **Department of Vocational Studies** at **S.S.J.S. Namdhari College, Garhwa**, a constituent unit under Nilamber-Pitamber University.