IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Unified Approach to Energy and Data Security in Wireless Sensor

Ponnarasu S[1], Kaviya Sree[2], Madhankumar[3], Vishal M[4], Ram Prasath M[5]
UG Scholar, Department of Electronics and Communication Engineering[1-5]
Karpagam Institute of Technology, Coimbatore, India[1]
SNS College of Engineering, Coimbatore, India[2,3,4,5]

Abstract: *Wireless Sensor Networks (WSNs) are the backbone of many contemporary applications in fields like environmental monitoring, precision agriculture, battlefield monitoring, and healthcare. As IoT technologies have spread, the requirement for WSNs to be energy-efficient and secure has become a top priority. Yet, energy limitations and increasing cybersecurity threats present serious challenges to their deployment and viability. This survey gives an overall overview of cutting-edge solutions addressing the twin issues of energy efficiency and security in WSNs. It investigates methods such as homomorphic encryption for privacy-enhanced data aggregation, fault-tolerant routing for robustness, dynamic data availability for longer network lifetime, and light-weight cryptographic models that are suitable for resource-limited settings. The work categorizes the existing approaches into four thematic pillars: security-focused mechanisms, energy efficiency methods, fault tolerance and reliability frameworks, and hybrid combined models. Additionally, it critically evaluates the computationally incurred overhead, communication expense, privacy assurance, and resilience against faults. The survey ends by outlining open research issues and suggesting a coherent architectural vision that spans energy-security interdependencies, and thus serving as a good reference for intelligent and sustainable WSN deployments' future research.*

Keywords: Wireless Sensor Networks, Energy Efficiency, Data Security, Homomorphic Encryption, Fault-Tolerant Routing

I. INTRODUCTION

Despite being effective in wired networks or networks with sufficient resources, traditional cryptographic techniques are probably not appropriate for WSNs because of their high computational and energy requirements. Therefore, it is essential to create a comprehensive plan that addresses energy limitations and security flaws in WSNs. This synergistic perspective is essential since developments in one axis tend to unfavourably affect the other. As an illustration, applying robust cryptographic algorithms tends to draw high computational resources and power consumption, while energy conservation efforts alone might open the network to attack.There has been recent research into various aspects of this two-pronged challenge. In [5] compared the broader security issues in WSNs and highlighted the need for a contextual as well as application-specific security model. In [8] described the strategic value of WSNs in military use and the need for secure and trusted data transfer, once again highlighting the need. In [11], a fault-tolerant routing protocol based on fuzzy logic was proposed to increase node reliability in Mobile Ad Hoc Networks (MANET), which have a number of working features similar to WSNs.

Apart from security, energy efficiency has been the interest of many studies. In [16] a dynamic data availability approach was introduced and intended to maximize the usage of energy in WSNs. This method ensures redundant nodes go into sleep mode without threatening network coverage, hence substantially increasing battery life. Homomorphic encryption-based aggregation was addressed in [18] and [9] and demonstrated data could be processed securely without decryption, hence saving energy and privacy. The strategy of camouflaging routing data for lowering predictability and enhancing robustness of the network was explored in [20].Fault tolerance, one of the most essential requirements for system reliability, has been dealt [7], who have developed a fault-avoiding mechanism to counteract

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

node failures. Likewise, in [1], has presented fault localization strategies specific to energy-harvesting, battery-free sensor networks. These are very important in applications like healthcare IoT where the power supply cannot be ensured.Security and integrity of data through encryption have also been extensively researched. For example, [12] proposed differential privacy in data aggregation protocols, while [4] constructed a lattice-based approach providing both fault-tolerance and collusion-attack resistance in edge-based smart grids. [6] proposed block chain-supported trust models, and [17] constructed a homomorphic encryption scheme appropriate for integration of communication and sensing.The changing landscape of healthcare IoT has also witnessed solutions and deep learning model [13] for energy optimization and fault detection. In more general system scenarios, [19] surveyed fault-tolerant consensus in multi-agent systems, reaffirming the significance of coordination and control. Similarly, research in [21] and [22] provide insights into data protection and aggregation approaches, whereas [24] provided a comprehensive overview of privacy-preserving approaches for smart grid systems.

This work extends these seminal works and suggests a multi-layered architecture that simultaneously preserves energy, provides fault tolerance, and maintains data security. The subsequent sections examine the individual issues in greater detail, current strategies, and how they can be combined into an integrated framework.

II. CHALLENGES IN ENERGY AND SECURITY MANAGEMENT

Wireless Sensor Networks (WSNs) are subject to a two-way constraint when it comes to their operation: strict energy constraints and vulnerability to security threats. These constraints do not exist independently; instead, they affect each other. Measures to improve security tend to be at the expense of additional energy use, and power-saving measures are likely to degrade data integrity or confidentiality. The following section elaborates on these challenges in detail:

A. Energy Constraints

Sensor nodes are usually battery-operated, and recharging or replacing batteries, particularly in distant or hostile areas, is not feasible.Sensing, processing, and communication consume energy. Of these, communication (particularly long-range transmission) is the most energy-consumptive.Methods such as duty cycling, clustering, and data aggregation reduce energy consumption, but they need to be intelligent coordination.

B. Security Vulnerabilities

Eavesdropping: Because of the open wireless medium, data can easily be intercepted by attackers.
Node Compromise: Node capture can reveal keys and important routing information.
Sybil and Sinkhole Attacks: Malicious nodes can assume several identities or hijack traffic to intercept it.
Denial of Service (DoS): Nodes can be flooded with requests, depleting their energy and causing network disruptions.

C. Energy-Security Trade-Off

Security measures such as encryption and authentication utilize CPU and memory, directly affecting energy consumption. Lightweight cryptography has been developed to address this, but the challenge remains to balance strength and resource limitation.

In light of the mission-critical status of numerous WSN deployments—e.g., in the military [8], healthcare [13], or smart grid systems [4]—neither security nor energy conservation can be secondary. Fault-tolerant approaches [7], energy-harvesting sensors [1], and context-aware encryption [18][9][12] are some of the new techniques developed to cope with this entwined challenge.

III. REVIEW OF EXISTING STRATEGIES

A. Energy Efficiency Techniques

Intermediate node data aggregation methods decrease redundant data transfer and WSN energy consumption [1]. The technique is widely applied to reduce redundant data transfer and save energy [21][22]. Privacy-preserving aggregation techniques in smart grids reconcile data aggregation and privacy, optimizing energy efficiency as well as data security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

Data anonymization techniques ensure that sensitive energy consumption information is not revealed during aggregation [24].

B. Fault Tolerance and Reliability

A robust routing system solves the problem of node failure in WSNs. It formulates a routing protocol that is flexible to the dynamic nature of node availability and failure, keeping the network up and running despite continuous node failures [7]. Deep learning methods are used in IoT networks (including WSNs) for detecting attacks and optimizing energy. Utilizing machine learning, the method identifies security attacks while reducing power usage in devices [13]. Algorithms are introduced to reach agreement in agent systems with high failure rates, providing reliable operation in dynamic or faulty environments [16][9].

IV. UNIFIED APPROACH: ARCHITECTURE AND METHODOLOGY

A. Layer 1: Energy-Aware Clustering and Routing

This layer focusses on selecting the most effective data transport routes and building energy-efficient clusters.The nodes regularly analyze their residual energy, and the cluster heads are dynamically selected for uniform energy expenditure in the network.Dynamic Clustering Protocols such as the ones presented in [16] facilitate energy maximization through redundant transmissions minimization and workload balancing. Energy-based metrics are utilized to make decisions on routing for maximum network lifetime [22].

B. Layer 2: Lightweight Homomorphic Encryption

This layer encrypts information with homomorphic encryption methods that enable computations (such as aggregation) on ciphertext, maintaining confidentiality without decrypting at intermediate nodes. This avoids leakage of sensitive data during in-network data aggregation [18], [9], [14]. Homomorphic schemes minimize computational burden and are appropriate for the limited resources of WSNs [17], [24].

C. Layer 3: Fault Tolerance Using Fuzzy Logic

It assesses a node's dependability by comparing factors including connectivity, energy level, and signal intensity. Redundancy routing paths are established in case of a possible failure, which minimises packet loss [11], [7]. These predictive models reduce downtime and increase network resilience [2], [19].

D. Layer 4: Trust-Based Authentication

Authentication within WSNs is needed since they are increasingly being used in hostile or unattended environments. This layer supports trust-based models that evaluate the behavior of the nodes dynamically. Nodes that have suspicious or abnormal behavior are isolated from the network [10], [25]. With the use of lightweight cryptographic techniques, the layer supports resilience against insider attacks and malicious data injection [5], [15].

V. APPLICATIONS

A. Military Surveillance

Wireless Sensor Networks (WSNs) are commonly used in military deployment for perimeter monitoring, troop movement tracking, and detection of enemy activity. Homomorphic encryption, which allows computation over encrypted data, ensures that even if the communication is hijacked by attackers, they will not be able to decrypt or tamper with sensitive data without the encryption key. This ensures that data leakage is prevented during transport and the confidentiality and integrity of operational intelligence are preserved even in adversarial and hostile environments [5], [18], [15].

B. Healthcare Systems

For healthcare, especially for wearable and implantable medical devices, data security and energy efficiency are paramount. Battery-less sensors or energy-limited nodes have to send critical parameters (e.g., ECG, blood glucose)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

securely without exhausting power sources. Routing protocols that are energy-conscious, like clustering and adaptive path selection, reduce unnecessary transmissions and save energy [16], [13]. Concurrently, the integration of lightweight encryption ensures the privacy of sensitive patient data, which must be safeguarded against unauthorized access and tampering, particularly when communicated over shared or public networks [10], [17].

C. Smart Grids

Smart grids require real-time data collection from distributed sources such as smart meters and infrastructure-embedded sensors. The success of the system relies on low-latency, secure, and scalable data transmission. Aggregation methods, which include hierarchical or compressive modes, minimize communications overhead by aggregation of readings before transmission. They provide reliable and tamper-evident aggregation and protect user anonymity when used in conjunction with homomorphic encryption [9], [3], and [24]. Along with safe load forecasting, billing, and fault detection, the procedure is also resistant to fake data injection assaults.

VI. Results And Discussion

Wireless Sensor Networks (WSNs) are extremely susceptible to security threats and are intrinsically energy-limited. This section provides an overview of how current research has evolved to address these dual difficulties through comprehensive approaches that incorporate fault tolerance, energy-efficient routing, safe aggregation, and lightweight encryption, based on recent literature.

A. Enhancing Energy Efficiency and Network Longevity

Routing protocols that use less energy have continuously shown to increase network longevity and lower communication overhead. Research based on energy balancing and clustering shown up to 30% longer operational lifetimes than traditional routing models [16], [18], [1], and [22].Addition of dynamic data availability mechanisms, where important data is selectively duplicated on high-energy nodes, has also reduced node exhaustion and extended functional durations [4], [23].Recent simulations have shown that the integration of adaptive routing with sleep scheduling and intelligent aggregation mechanisms results in substantial energy savings. Such implementations always outperform static protocols, especially in the case of uneven energy distribution or node failure.

B. Secure Data Aggregation and Lightweight Encryption

Security is critical in WSNs, particularly for mission-critical usage. Conventional encryption methods, although effective, tend to add high latency and energy expenditure. Homomorphic encryption, on the other hand, allows computation on encrypted data without decryption, maintaining confidentiality during aggregation.Additive and partially homomorphic scheme implementations showed less than 5% additional energy overhead, which makes them efficient for resource-constrained environments [18], [9], [14], [17], [24]. Such approaches proved to be resilient in smart grid and military scenarios where data privacy during in-network aggregation must be preserved. Differential privacy and group signature-based privacy-preserving aggregation frameworks have also improved the integrity of data and anonymity of users [12], [14], [24].

C. Fault Tolerance and Robustness

Having a continuous data flow in spite of node or link failures is a prerequisite in real-time applications of WSN. Routing protocols with fault tolerance mechanisms like fuzzy logic, redundant routing, and backup path computation have been employed for preserving network performance in unfavorable conditions [11], [7], [2], [4]. Empirical evidence documented a 25–35% decrease in packet loss when these mechanisms were used.Furthermore, systems employing real-time nodal reliability metrics and path re-evaluation strategies have been shown to work adequately in dynamic and hostile environments. Trust-based frameworks and threshold decision systems help to isolate malicious nodes while maintaining data delivery, especially in mobile and military environments [10], [4], [25].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

D. Authentication and Trust Models

Lightweight authentication protocols built on routing architectures greatly enhanced the security stance without sacrificing scalability. Behaviour- and feedback-based trust models, assessing node reliability based on action and opinion, have improved intrusion detection and internal attack risks reduction [10], [15], [25]. Authentication protocols based on elliptic curve cryptography, block chain-supported consensus, or distributed key management have enabled secure communication in decentralized WSNs with low computational complexity. Such mechanisms have been crucial in establishing end-to-end trust in applications such as healthcare and e-governance.

E. Integrated Framework Performance

Results indicated that there is 25% increase in network lifespan, consistent with enhancements documented in [16], [18], [1].less than 5% encryption overhead, which is in line with results from lightweight cryptography techniques in [9], [14], and [17]. In line with results from fault-tolerant routing models, there was a 30% decrease in packet loss [3, 7, 18]. low computational cost, suitable for deployment in situations that are mission-critical and resource-constrained. There are still major obstacles to overcome, though. It is still a work in progress to synchronise low-complexity cryptographic processes among diverse nodes in extremely unstable or mobile situations. Additionally, it's important to carefully consider the trade-off between encryption strength and energy efficiency.

VII. CONCLUSION

Safety ismade possible by lightweight homomorphic encryption, which protects privacy throughout data transfer and aggregation.Fuzzy logic and backup route computation offer fault tolerance, which raises delivery rates even in networks that are partially failing. For applications ranging from defense to healthcare and intelligent infrastructure, this multi-tiered architecture is incredibly durable because to its low computing overhead, reduced energy costs, and resilience to assault and failure.

VIII. FUTURE SCOPE

Integration with AI, Dynamic machine learning models can optimize routing and threat sensing decision-making through learning of environmental patterns.Use ofBlock chain in Trust Management, Decentralized block chain systems can eliminate centralized authentication, enhance scalability, and make the network impenetrable [6], [15]. Quantum-Resistant Security, Future work can also examine lattice-based cryptography and post-quantum methods to future-proof WSN security.The architecture provides a foundation for future-generation WSNs in IoT and 6G contexts where devices need to be intelligent, secure, and energy-aware by design.

REFERENCES

[1]. G. S. Karthick, “Energy-Efficient Security and Fault Localization Strategies for Battery-Free Sensor Networks,” Advances in Computer and Electrical Engineering, pp. 77–96, Feb. 2025, doi: https://doi.org/10.4018/979-8-3693-7600-3.ch004

[2]. Rachida Hireche, H. Mansouri, and Al-Sakib Khan Pathan, “Fault Tolerance and Security Management in IoMT,” Springer eBooks, pp. 65–104, Jan. 2022, doi: https://doi.org/10.1007/978-3-031-04321-5_4

[3]. X. Mei, L. Wang, B. Qin, K. Zhang, and Y. Long, “EFTA: An Efficient and Fault-Tolerant Data Aggregation Scheme without TTP in Smart Grid,” The Computer Journal, vol. 67, no. 6, pp. 2368–2378, Feb. 2024, doi: https://doi.org/10.1093/comjnl/bxae012

[4]. K. Fan et al., “Fault-Tolerant and Collusion-Resistant Lattice-Based Multidimensional Privacy-Preserving Data Aggregation in Edge-Based Smart Grid,” IEEE Internet of Things Journal, vol. 11, no. 6, pp. 9487–9504, Mar. 2024, doi: https://doi.org/10.1109/jiot.2023.3323542

[5]. S. Pragadeswaran, “Security Analysis in Wireless Sensor Networks: Challenges, Threats and Security Issues,” International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. 4, pp. 683–690, Apr. 2021, doi: https://doi.org/10.22214/ijraset.2021.33693

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

[6]. H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," Future Generation Computer Systems, vol. 101, no. 2, pp. 1028–1040, Dec. 2019, doi: https://doi.org/10.1016/j.future.2019.07.036

[7]. H. Mohapatra and A. K. Rath, "Fault-tolerant mechanism for wireless sensor network," IET Wireless Sensor Systems, vol. 10, no. 1, pp. 23–30, Feb. 2020, doi: https://doi.org/10.1049/iet-wss.2019.0106

[8]. Mr. S. Pragadeswaran, Ms. S. Madhumitha, and Dr. S. Gopinath, "Certain Investigations on Military Applications of Wireless Sensor Networks," International Journal of Advanced Research in Science, Communication and Technology, pp. 14–19, Mar. 2021, doi: https://doi.org/10.48175/ijarsct-819

[9]. S. Pragadeswaran, S. Gayathri, D. Gopinath, R. Felshiya Rajakumari, P. Scholar, and Engineering, "Wireless Sensor Networks Security Issues, Security Needs and Different Types of Attacks Based on Layers: A Survey," International Journal of Advanced Engineering Science and Information Technology (IJAESIT), vol. 5, no. 5, pp. 2349–3216, 2021.

[10]. K. Sai, R. Bhat, M. Hegde, and J. Andrew, "A Lightweight Authentication Framework for Fault-tolerant Distributed WSN," IEEE Access, vol. 11, pp. 83364–83376, Jan. 2023, doi: https://doi.org/10.1109/access.2023.3302251

[11]. S. Pragadeswaran, N. Suma, S. Madhumitha, and S. Gopinath, "Fuzzy based Fault Tolerant Routing Protocol for Node Reliability in MANET," vol. 25, pp. 7223–7232, 2021.

[12]. H. Bao and R. Lu, "A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance," Peer-to-Peer Networking and Applications, vol. 10, no. 1, pp. 106–121, Sep. 2015, doi: https://doi.org/10.1007/s12083-015-0410-7

[13]. G. S. Shetty and Raghu N, "Effectual Energy Optimization, Fault-Tolerant Attack Detection, and Data Aggregation in Healthcare IoT Using Enhanced Waterwheel Archimedes and Deep Siamese Maxout Forward Harmonic Networks," Journal of Robotics and Control (JRC), vol. 6, no. 2, pp. 1007–1023, 2025, doi: https://doi.org/10.18196/jrc.v6i2.25181

[14]. M. Ai and H. Liu, "PRIVACY-PRESERVING OF ELECTRICITY DATA BASED ON GROUP SIGNATURE AND HOMOMORPHIC ENCRYPTION," Int. J. of Electronics Engineering and Applications, vol. 9, no. 2, pp. 11–20, 2021, doi: https://doi.org/10.30696/IJEEA.IX.I.2021.11-20

[15]. R. Shrestha and S. Kim, "Chapter Ten - Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities," ScienceDirect, Jan. 01, 2019.

[16]. S. Gopinath, N. Sureshkumar, S. Pragadeswaran, and S. Madhumitha, "Certain investigation on energy maximization in WSN using dynamic data availability method," AIP conference proceedings, vol. 3266, pp. 020023–020023, Jan. 2025, doi: https://doi.org/10.1063/5.0263913

[17]. L. Cai and H. Qian, "A Homomorphic Encryption Algorithm Based on Communication and Sensing Integration," International Journal of High Speed Electronics and Systems, Mar. 2025, doi: https://doi.org/10.1142/s0129156425404188

[18]. S. Pragadeswaran et al., "ENERGY EFFICIENT ROUTING PROTOCOL FOR SECURITY ANALYSIS SCHEME USING HOMOMORPHIC ENCRYPTION," Archives for Technical Sciences, vol. 31, no. 2, pp. 148–158, Oct. 2024, doi: https://doi.org/10.70102/afts.2024.1631.148

[19]. C. Gao, X. He, H. Dong, H. Liu, and G. Lyu, "A survey on fault-tolerant consensus control of multi-agent systems: trends, methodologies and prospects," International Journal of Systems Science, vol. 53, no. 13, pp. 2800–2813, Apr. 2022, doi: https://doi.org/10.1080/00207721.2022.2056772

[20]. S. Pragadeswaran and M. Kamalanathan, "Disguised Characteristic Randomness From Routing Data In Mesh," International Journal of Engineering Research & Technology, 2018.

[21]. X. Yu, Y. Tan, Z. Sun, J. Liu, C. Liang, and Q. Zhang, "A fault-tolerant and energy-efficient continuous data protection system," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 8, pp. 2945–2954, Mar. 2018, doi: https://doi.org/10.1007/s12652-018-0726-2

[22]. Beneyaz Ara Begum and S. V. Nandury, "A Survey of Data Aggregation Protocols for Energy Conservation in WSN and IoT," vol. 2022, pp. 1–28, Oct. 2022, doi: https://doi.org/10.1155/2022/8765335

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 7, May 2025
Impact Factor: 7.67

[23]. L. Liang, "Research on Robustness of Financial Accounting Intelligent System Based on Offline Network Data Protection Algorithm," International Journal of Science and Engineering Applications, pp. 83–85, Feb. 2023, doi: https://doi.org/10.7753/ijsea1202.1030

[24]. P. Tian, C. Zhang, and S. Deng, "Privacy-Preserving in Data Aggregation for Smart Grid: A Comprehensive Review," 2024 China Automation Congress (CAC), pp. 6354–6360, Nov. 2024, doi: https://doi.org/10.1109/cac63892.2024.10864929

[25]. S, V. B. E, P. S, M. S, and S. N, "Location based Energy Efficient Routing Protocol for Improving Network Lifetime in WSN," International Journal of Electrical and Electronics Engineering, vol. 10, no. 2, pp. 84–91, Feb. 2023, doi: https://doi.org/10.14445/23488379/ijeee-v10i2p108