STM JOURNALS

Recent Trends in
Sensor Research & Technology

ISSN: 2393-8765
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/RTSRT

https://journals.stmjournals.com/rtsrt

Review RTSRT

Security Challenges and Solutions in Wireless Sensor Networks: A Case Study of Afghanistan

Hafeezullah Sahibzda[1,*], Mohammad Salem Hamidi[2]

Abstract

Due to their ability to collect and relay data from locations without supervision, wireless sensor networks (WSNs) have become essential for numerous contemporary applications, such as environmental monitoring, smart cities, and healthcare. However, the open and resource-constrained nature of WSNs makes them particularly vulnerable to security threats. This paper reviews the key security issues faced by WSNs and the solutions proposed in recent literature. We examine the unique constraints of WSNs, including limited energy, computational capacity, and bandwidth, and how they complicate traditional security measures. Common attack types are surveyed, including routing attacks (e.g., wormhole, sinkhole, and Sybil attacks) and denial-of-service attacks (e.g., jamming and flooding). Countermeasures are classified into lightweight cryptography and authentication protocols, secure routing schemes, trust and reputation systems, intrusion detection methods, and emerging approaches such as machine learning and blockchain for anomaly detection and data integrity. This study assesses how effective these security mechanisms are across various network conditions and emphasizes the trade-offs among security strength, energy consumption, and network lifetime. Additionally, it addresses recent progress in energy-efficient security protocols and cross-layer design methods aimed at improving the overall resilience of systems. Our analysis highlights that no single solution fits all scenarios; instead, a combination of techniques is often required to balance security with WSN resource limitations. The review concludes with a discussion of open issues and recommendations for future research to achieve robust, energy-efficient security in WSNs.

Keywords: Wireless sensor networks (WSNs), network security, routing attacks, denial-of-service (DoS), lightweight cryptography, intrusion detection systems, energy efficiency, blockchain and machine learning

INTRODUCTION

Wireless sensor networks (WSNs) are networks composed of many small sensor nodes with low power and limited resources. These sensor nodes are used to observe physical or environmental conditions, such as temperature, humidity, pressure, and movement. After collecting data, the sensor nodes send this information wirelessly to a central location, called a base station. WSNs play an important role in many Internet of Things (IoT) applications, including industrial automation, healthcare monitoring systems, agriculture management, environmental monitoring, and smart city development [1].

In many cases, WSNs are deployed in remote or unattended environments where human supervision is limited or impossible. Therefore, these networks face several security risks. The use of wireless communication makes WSNs more vulnerable to attacks such as eavesdropping, message interception, data modification, and node capture. Unlike wired networks, WSNs do not have a fixed

***Author for Correspondence**
Hafeezullah Sahibzda
E-mail: hafeezullahsahibzada110@gmail.com

[1]Student, Department of Computer science, Jahan University, Kabul Afghanistan
[2]Lecturer, Department of Computer science, Jahan University, Kabul Afghanistan

Received Date: April 11, 2026
Accepted Date: April 17, 2026
Published Date: April 25, 2026

Citation: Hafeezullah Sahibzda, Mohammad Salem Hamidi. Security Challenges and Solutions in Wireless Sensor Networks: A Case study of Afghanistan. Recent Trends in Sensor Research & Technology. 2026; 13(1): 27–35p.

infrastructure, which further increases their exposure to security threats [2, 3].

Another major challenge in WSNs is the limited capabilities of the sensor nodes. Most sensor nodes operate on small batteries, have low processing power, and contain limited memory. Owing to these constraints, it is difficult to apply traditional security mechanisms, such as complex encryption algorithms and continuous monitoring techniques. Heavy security protocols can quickly drain battery power and reduce the overall network. Consequently, designing lightweight and efficient security solutions for WSNs is a difficult task [3, 4].

Despite these challenges, ensuring the security of WSNs is extremely important. The data collected by sensor nodes is often sensitive in nature, such as patient health data, environmental measurements, or location information. If this data is accessed or modified by unauthorized users, it can lead to serious consequences. For example, attackers may inject false data into the network, redirect traffic to malicious nodes, or disrupt communication between sensor nodes and the base station. Such attacks can damage the confidentiality, integrity, and availability of network data, which are the core principles of information security [5].

Security attacks on WSNs can also affect the reliability of an entire system. In critical applications, such as healthcare or industrial monitoring, incorrect or manipulated data may lead to incorrect decisions or physical harm. Therefore, protecting sensor data from unauthorized access and ensuring their accuracy are among the top priorities in WSN security research. Previous studies have emphasized that maintaining data integrity and preventing unauthorized access are essential requirements for secure WSN operations [6, 7].

In summary, the unique characteristics of WSNs—including their large-scale deployment, dynamic network topology, open wireless communication, and limited hardware resources—create a highly challenging security environment. These factors make WSNs different from traditional networks and require specialized security approaches [3, 8]. This paper reviews recent research published between 2020 and 2025, focusing on identifying security vulnerabilities in WSNs and analyzing the proposed solutions designed to protect these networks.

LITERATURE REVIEW

WSN Security Requirements and Constraints

Effective security in WSNs must focus on the basic security goals of confidentiality, integrity, and availability, along with proper authentication and ensuring that data are fresh and not reused by attackers. However, the unique limitations of WSNs strongly affect how security solutions are designed. Sensor nodes usually operate on batteries and are deployed for long periods; therefore, energy efficiency is extremely important [4]. Any security or communication protocol that uses excessive power can reduce the overall lifetime of the network.

In addition, sensor nodes have limited processing power and very small memory, which makes it difficult to use complex security algorithms in them. For example, although public-key cryptography offers strong protection, it is often too heavy and resource-consuming for small sensor devices. Because of this, lightweight cryptographic techniques, such as symmetric encryption, hash functions, and message authentication codes (MACs), are commonly used, as long as they still provide adequate security.

Key management is another major challenge in WSNs. Security protocols must be able to create, distribute, and update shared keys while using minimal energy and system resources [9]. Furthermore, WSNs are usually distributed and self-organizing, which means that there is often no fixed or central trusted authority. Some security approaches rely on a secure base station; however, if the base station is compromised, the entire network can become vulnerable [10]. In summary, WSNs require new and efficient security architectures that balance low resource usage with strong protection against attacks [6, 9].

COMMON ATTACKS ON WSNs

WSNs face a wide range of attacks across the protocol stack. Many surveys categorize these by layer (physical, data link, network, and transport) [9, 11]. We highlight the most frequently discussed threats in recent literature.

WSNs face many different types of attacks at various layers of the network protocol stack. Many studies classify these attacks based on network layers, such as the physical, data link, network, and transport layers [9, 11]. The most common security threats discussed in recent research are as follows:

Wormhole Attack

In this attack, two malicious nodes secretly create a tunnel between them and forward packets directly through it, skipping the normal multi-hop routing path [12]. This changes the routing structure of the network and may cause packets to follow incorrect paths. Attackers can drop, delay, or modify the data passing through the tunnel. As the packet contents are usually not changed, wormhole attacks are difficult to detect using standard security methods [5, 12].

Sinkhole Attack

A sinkhole attack happens when a malicious node claims it has the best or shortest route to the base station, attracting nearby nodes to send their data through it [10, 12]. Once the traffic is redirected, the attacker can monitor, change, or discard the packets. This attack increases the delay, packet loss, and overall network congestion, making it harmful to network performance [2, 4].

Sybil Attack

In a Sybil attack, one malicious node pretends to be multiple nodes by using many fake identities [13]. This can damage voting systems, routing decisions, and trust mechanisms because the attacker appears as many different nodes. Consequently, the network's assumption that one identity belongs to one node is broken [6, 7].

Blackhole and Grayhole Attacks

In a Blackhole attack, a malicious node advertises itself as having the best route and then drops all packets that it receives [7]. A grayhole attack is similar to a Blackhole attack but is harder to detect because the attacker drops only some packets instead of all. Both attacks reduce data delivery and can disable parts of the network by silently discarding the traffic [11].

Selective Forwarding Attack

This attack is a more controlled version of packet dropping. The malicious node forwards normal packets but drops important or selected packets, such as data from specific nodes or of a certain type. This allows attackers to target specific information while remaining undetected.

HELLO Flood Attack

In this attack, an attacker sends HELLO messages using a very high transmission power, making many nodes believe that it is their direct neighbor. This false neighbor information can break routing paths and isolate network areas. This is a common network layer attack in WSNs.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks aim to make networks unavailable. Common examples include flooding, where excessive packets are sent to drain node energy or bandwidth, and jamming, where radio signals block wireless communication [14]. Flooding drains battery power, while jamming disrupts the wireless channel completely [8, 14].

Spoofing and Man-in-the-Middle Attacks

In spoofing, attackers fake node identities or packet headers to appear as legitimate nodes. In man-in-the-middle (MITM) attacks, attackers intercept, modify, or relay messages between communicating nodes [8, 9]. These attacks damage data authenticity and confidentiality and are often combined with routing attacks.

Other Attacks

Additional threats include physical node capture, where attackers extract stored keys, traffic analysis through passive listening, and advanced attacks that amplify traffic to drain battery power.

Researchers agree that routing-layer attacks are among the most dangerous threats to WSNs [7, 12]. Wormhole attacks are especially harmful because they can redirect traffic without changing the packet data, making them difficult to detect [12, 10].

- *Wormhole:* A hidden tunnel that distorts routing; attackers can alter or delete data without detection [2].
- *Sinkhole:* A malicious node attracts all traffic; causes congestion and data loss [6, 14].
- *Sybil:* One node appears as many; breaks redundancy, votes, and routing integrity.
- *Blackhole/Grayhole:* Fake route advertisement and packet dropping (all or some).
- *Selective Forwarding:* Partial packet dropping targeting critical data [8].
- *HELLO Flood:* Powerful HELLO packets make false neighbors; causes routing failures (no reference).
- *Flooding (DoS):* Excessive traffic exhausts energy/resources [14].
- *Jamming (DoS):* Radio interference blocks communication [14].
- *Spoofing/MITM:* Impersonation or interception of packets undermines confidentiality and authenticity [7, 9].

EXISTING SECURITY SOLUTIONS

To counter these threats, various defenses have been proposed in literature. Owing to resource constraints, many solutions are lightweight or distributed. Key categories include the following.

Lightweight Encryption and Authentication

Symmetric-key encryption is commonly used in WSNs because it requires less processing power and energy. Security protocols such as SPINS (Security Protocols for Sensor Networks), LEAP (Localized Encryption and Authentication Protocol), TinySec, and MiniSec are designed specifically for sensor networks. These protocols provide data confidentiality and authentication while using very little battery power [4]. For example, TinySec protects data at the link layer with low energy use [4]. Each method balances security strength and power consumption. Stronger encryption provides better protection but consumes more energy. Key management is also important in this regard. Many systems use pre-shared or randomly distributed keys to ensure secure communication between nearby nodes. Recent studies emphasize that key management systems must support the addition or removal of nodes and must carefully handle base station attacks [9]. For example, LEAP depends on a base station for key setup, which works well unless the base station is captured [9].

Secure Routing Protocols

Normal routing protocols used in ad-hoc networks are not secure for WSNs. To solve this, researchers developed secure routing protocols such as SAODV (Secure Ad hoc On-Demand Distance Vector), ARAN (Authenticated Routing for Ad hoc Networks), and SEAD (Secure Efficient Ad hoc Distance Vector). These protocols protect routing messages using authentication and hashing methods to prevent the generation of fake routing information. They help defend against wormholes, sinkholes, and spoofing attacks. However, adding security increases the processing and communication overhead. To reduce this, many protocols secure only the important routing fields. Studies have shown that no single routing protocol is perfect, and the choice depends on the application requirements [2]. Using secure routing together with other security methods often gives better results [1].

Intrusion Detection Systems

As not all attacks can be prevented, intrusion detection systems (IDS) are used to detect suspicious behavior during network operations. Sensor nodes or cluster heads monitor nearby nodes by observing packet loss, collisions, and energy usage [2]. If a node behaves abnormally, it is marked as suspicious.

IDS learn normal behavior patterns and detect unusual activities, such as wormholes or selective forwarding attacks [4]. Some IDS use machine learning techniques to improve detection accuracy [2] [4]. These systems can detect Sybil and routing attacks, but machine learning needs high processing power and training data, which is difficult for sensor nodes. Therefore, IDS are often placed at the base station or designed to be very simple on sensor nodes [4].

Trust and Reputation Models

Trust-based systems assign a trust value to each node based on its behavior. Nodes observe their neighbors by checking packet forwarding, response time, and authentication success. If a node drops packets or behaves poorly, its trust score decreases. Nodes with low trust are removed from the routing paths. Trust systems are effective against internal attacks and can adapt over time. However, selecting the appropriate trust parameters depends on the application. Trust models work well together with IDS to block known malicious nodes [6, 7].

Secure Data Aggregation

To save energy, many WSNs combine data inside the network before sending it to the base station. Secure aggregation ensures that the data are not changed by malicious nodes. Some methods use homomorphic encryption, which allows calculations to be performed on encrypted data. Others have used multiple authentication codes to verify data accuracy [2]. Protocols such as ESPDA (Energy-efficient Secure Privacy-preserving Data Aggregation) and SDDA (Secure Data Dissemination and Aggregation) help ensure that aggregation nodes are trustworthy. Secure aggregation is important for applications that need accurate and private data [8].

Emerging Technologies

New technologies are being explored to improve the security of WSNs. Machine learning is used not only in IDS but also for predicting attacks and improving defense strategies [2]. Deep learning models have shown good results in detecting routing problems [3]. Another new approach is using blockchain to store sensor data or trust values securely. Blockchain helps prevent data tampering and improves trust [7, 9]. However, traditional blockchains are too heavy for WSNs; therefore, lighter versions are being developed to reduce energy use [9, 14]. These new methods are promising but must be carefully designed because of the limited resources in WSNs.

COMPARATIVE ANALYSIS

The reviewed literature summarizes common security attacks in WSNs along with the countermeasures proposed to mitigate them. A consistent finding across studies is that no single security solution can effectively defend against all WSN threats. Each mechanism targets specific attacks and has its strengths and weaknesses. Therefore, researchers strongly recommend using hybrid security approaches that combine multiple techniques to achieve better protection.

For instance, symmetric encryption is commonly applied to ensure data confidentiality because it is energy-efficient and suitable for resource-constrained sensor nodes. However, encryption alone cannot detect compromised nodes or insider attacks. To overcome this limitation, trust-based routing is used to avoid malicious nodes by evaluating their behavior, whereas IDS monitor network traffic to identify abnormal activities, such as selective forwarding or routing manipulation [2, 4]. When these techniques are combined, they provide stronger and more reliable security measures. However, the literature highlights important trade-offs. Increasing security often results in higher energy consumption, additional processing overhead, and increased latency. This performance versus security trade-off is a key concern in the design of WSNs. Therefore, security protocols must balance robustness against attacks with the strict energy and delay constraints of sensor networks [2]. Overly complex solutions may offer strong security but significantly reduce the network lifetime.

Overall, researchers emphasize a layered defense strategy for WSNs as shown in Table 1. This strategy integrates lightweight cryptography, secure routing protocols, and continuous monitoring mechanisms to provide comprehensive protection while operating within a limited resource budget.

Table 1. Summary of common WSN attacks, their impacts, countermeasures, and limitations.

Attack type	Impact on WSN	Typical countermeasures	Limitations
Wormhole	Distorts routing paths, enables packet dropping	Packet leashes, IDS, secure routing	Hard to detect, high overhead
Sinkhole	Attracts traffic to malicious node, data loss	Trust-based routing, authentication	Difficult to detect early
Sybil	One node uses multiple identities	Identity verification, trust models	Needs extra computation
Blackhole/ grayhole	Drops all or selected packets	IDS, multipath routing	Detection delay
Selective forwarding	Drops important packets only	IDS, redundancy	Extra energy use
HELLO Flood	Creates false neighbors	Bidirectional link checks	Limited effectiveness
Flooding (DoS)	Drains energy, network congestion	Rate limiting, IDS	Increased latency
Jamming (DoS)	Blocks communication channel	Frequency hopping	Hardware cost
Spoofing/MITM	Data modification and impersonation	Encryption, authentication	Key management complexity

OBJECTIVES

This study aims to survey and synthesize the recent literature on WSN security challenges and solutions, focusing on publications from 2020 to 2025. The specific objectives are as follows:

1. Identify key security challenges in WSNs (threats, vulnerabilities, and resource limitations).
2. Review and categorize defense mechanisms (including cryptographic schemes, secure protocols, and intrusion detection) reported in recent studies.
3. Compare the advantages and limitations of different security approaches for WSNs, considering the resource-constrained nature of sensors.
4. Highlight gaps and open issues, suggesting directions for future research to enhance WSN security.

RESEARCH METHODOLOGY

The findings presented in this paper are based on a structured literature review. We conducted comprehensive searches of academic databases (e.g., IEEE Xplore, ACM Digital Library, MDPI, Springer) using keywords like *"WSN security"*, *"sensor network attacks"*, *"secure routing WSN"*, *"intrusion detection"*, etc. We filtered peer-reviewed articles published between 2020 and 2025 to capture the latest developments. Each selected paper was examined for its contributions to WSN security, the type of attack addressed, the proposed solution, and any performance evaluation. We then organized the literature thematically (by attack type and defense technique), extracting key insights and metrics where reported. This qualitative analysis was used to identify common challenges (e.g., energy trade-offs and threat coverage) and compare different solution strategies. The citations from these sources are integrated throughout this paper to support the discussion and to show the basis for our conclusions.

DATA ANALYSIS AND DISCUSSION

Our analysis of the recent WSN security literature reveals several important trends.

Resource Constraints Dictate Solution Design

Nearly all studies emphasize that energy, computation, and memory limitations of sensor nodes are the primary bottleneck in applying security [4, 11]. For example, while public-key cryptography would simplify key management, its computational cost is prohibitive. Consequently, most solutions rely on symmetric-key ciphers and lightweight hash functions [4]. However, designers must minimize the message overhead. Illustrates that the proposed key management protocols often balance security features with memory and communication costs [9]. In practice, this means that protocols such as TinySec (a link layer security suite) that use optimized symmetric encryption are popular because of

their low overhead [4]. However, symmetric schemes require secure initial key distribution and periodic rekeying, which is a non-trivial task in dynamic networks [9].

Prevalence of Routing-Layer Defenses

A significant portion of the literature focuses on securing the routing process [2, 8]. As many attacks (wormhole, sinkhole, and blackhole) target routing, solutions often combine cryptographic routing protocols with trust metrics. For instance, trust-based routing can exclude nodes that frequently drop packets. Authentication extensions to routing (e.g., adding digital signatures or MACs to route advertisements) are used to prevent spoofing [2]. The analysis shows that effective routing security protocols must guarantee the integrity and authenticity of routing information while keeping energy use manageable. Some studies have noted that using *hybrid routing* (e.g., combining proactive and reactive elements or cluster-based vs. flat routing) can reduce the impact. However, there is no one-size-fits-all solution: protocols often assume specific network models (static vs. mobile nodes) and may not be easily generalizable [1].

Intrusion Detection and Anomaly Monitoring

Several recent studies have implemented IDS frameworks tailored to WSNs. These systems continuously monitor network traffic and resource usage to detect anomalies. For example, by tracking metrics such as collision rate, latency, or neighbor count, a node can infer suspicious behavior [2]. Our review confirms that machine learning models (Support vector machine (SVM), random forest, neural nets) have been used to classify traffic patterns as normal or malicious [2]. Studies have reported high detection accuracy for attacks such as wormholes or black holes using these models. However, a common limitation is resource consumption: on-node machine learning (ML) requires computation and data collection, which can drain batteries [2]. Therefore, some solutions offload processing to more capable nodes (cluster heads) or an external server. An alternative is a rule-based IDS, which uses simple thresholds (e.g., retransmission counts) to detect misbehaving neighbors [2]. Although less flexible than ML, rule-based systems have much lower overheads. Overall, intrusion detection is considered a necessary layer of defense, especially because it can detect attacks even if initial prevention fails [4].

Trust and Reputation Systems

Trust-based approaches are frequently cited as effective methods for countering insider threats. Our literature analysis found that trust models typically use simple evidence, such as packet delivery ratios or energy usage, to adjust trust scores [13]. A node that consistently forwards packets properly gains trust, whereas one that does not is penalized. These systems are often combined with IDS: for example, if the IDS flags a node, its trust score is lowered, leading other nodes to avoid it. The literature emphasizes that calibrating trust thresholds is application-specific and that mobility or dynamic topology changes can complicate trust tracking [10]. Importantly, trust schemes can adapt over time to changing conditions, which is valuable for long-lived WSN deployments.

Emerging Technologies

We observed a growing interest in advanced techniques. Machine learning is now not only used in IDS but also proposed for tasks like adaptive routing and power management to indirectly improve security. For example, some surveys suggest using adversarial learning to predict and counter new attack patterns. Blockchain integration is another active topic: authors report that recording sensor data on a blockchain can prevent tampering, and smart contracts can automate trust evaluation [12]. These approaches show promise for enhancing security guarantees, but our analysis notes that the high overhead remains a barrier [14, 5]. Researchers are experimenting with lightweight consensus and permissioned blockchain variants to reduce the energy costs.

Comparative Trade-Offs

The reviewed studies often compare solutions along the axes of energy use, detection accuracy, and latency [3, 4]. For instance, one analysis table shows that adding security features can increase packet size and delay processing, but strategic protocol design (e.g., only authenticating critical messages) can

mitigate this. In general, the analysis in the literature suggests that security versus performance trade-off is a central design theme [9]. Solutions that minimize communication (through aggregation or on-node decisions) tend to save energy but may sacrifice some detection capability. This trade-off underscores the importance of the application context: a high-stakes military sensor network may accept higher energy costs than a civilian environmental monitor.

FINDINGS

Based on the literature review, we highlight the following key findings regarding WSN security.

WSNs are Inherently Vulnerable

Due to their *open wireless medium*, lack of physical protection, and constrained resources [3, 8]. The distributed, often unattended deployment of sensor nodes means that attackers can exploit the physical and network layers. Ensuring the confidentiality and integrity of sensor data is especially challenging in such an environment [6, 7].

Routing Attacks Dominate the Threat Landscape

Wormhole, sinkhole, Sybil, and blackhole attacks continue to receive the most attention because they can critically disrupt network functionality [2, 7]. For example, wormholes distort routing without altering packet contents, making them difficult to detect using conventional cryptography [12, 10]. DoS attacks (flooding and jamming) also pose major threats to network availability.

Lightweight Cryptography and Authentication are Fundamental

Most proposed solutions rely on symmetric-key encryption and MACs to protect data packets [14]. Protocols such as SPINS, TinySec, and MiniSec exemplify this approach. These methods are effective but must be carefully tuned: for instance, TinySec's use of a small block cipher allows encryption without excessive energy use [4]. Key management remains a challenge, and dynamic node revocation and secure base station assumptions must be addressed [9].

Anomaly Detection and Trust Mechanisms are Effective Complements

IDS that learn normal network behavior can detect novel or internal attacks [4]. Trust-based routing can dynamically isolate malicious nodes, thereby improving resilience [8]. The literature shows that combining multiple methods, for example, using both encryption and IDS, yields better security at acceptable costs. As one review notes, *"security and performance challenges are often solved through a combination of different methods and protocols"* [2].

Emerging Approaches Offer Promise but Add Complexity

Machine learning techniques have proven to have high detection accuracy (e.g., SVMs or neural networks identifying anomalous traffic) [3]. Blockchain integration can enhance data integrity through immutable logging [9]. However, both technologies consume additional energy and computation. For example, blockchain consensus algorithms require significant processing, which is why new variants (PoS, PBFT) are being studied [1, 2]. These emerging solutions are promising for future WSNs; however, further research is required to make them practical in low-power networks.

CONCLUSION

WSNs present a unique security challenge: they must operate in potentially hostile, open environments while constrained by low power and limited hardware. This review surveyed the main vulnerabilities of WSNs (e.g., routing-level attacks, DoS, and identity spoofing) and the spectrum of proposed defenses (lightweight encryption, secure routing protocols, intrusion detection, and trust management). A common theme is that no single solution is sufficient; effective security typically involves multilayered approaches that balance protection with resource use. Traditional countermeasures like symmetric cryptography and MACs remain core components, while newer techniques (ML-based IDS, blockchain logging) are being explored to address evolving threats.

Looking forward, future work should focus on energy-efficient implementation of advanced defenses, robust trust evaluation in dynamic networks, and cross-layer strategies that link physical security with network security. Given the rapid growth of WSNs in critical systems, continued research on secure and lightweight protocols is essential. In particular, standardizing adaptive frameworks that can select appropriate security mechanisms based on application scenarios will be valuable. By combining insights from recent studies, designers can build WSNs that maintain data security without compromising network longevity and performance.

REFERENCES

1. Mosawi SZ, Qasimi M, Wadeed WM, Rahmani KR. Exploring Wi-Fi security challenges and proposing solutions: the case of Afghanistan. Eur J Electr Eng Comput Sci. 2023;7(5):14-19. doi:10.24018/ejece.2023.7.5.553.
2. Hussain RH. A survey on security challenges in wireless sensor networks. Univ Thi-Qar J. 2017;12(3):42-72.
3. Lee CC. Security and privacy in wireless sensor networks: advances and challenges. Sensors (Basel). 2020;20(3):744. doi:10.3390/s20030744.
4. Ahmad R, Wazirali R, Abu-Ain T. Machine learning for wireless sensor networks security: an overview of challenges and issues. Sensors (Basel). 2022;22(13):4730. doi:10.3390/s22134730.
5. Velliangiri A. Security challenges and solutions in IoT-based wireless sensor networks. J Wirel Sens Netw IoT. 2024;1(1):8-14.
6. Garg A, Kumar A, Singh AK. Machine learning-based security approaches for wireless body area networks. In: Security, Privacy, and Trust in WBANs and E-Healthcare. Boca Raton (FL): CRC Press; 2024. p.206-235. doi:10.1201/9781032635101-14.
7. Pathan ASK, Lee HW, Hong CS. Security in wireless sensor networks: issues and challenges. 2006 8th International Conference Advanced Communication Technology, Phoenix Park. 2006. p.6. doi:10.1109/ICACT.2006.206151.
8. Pathan ASK, Lee HW, Hong CS. Security in wireless sensor networks: issues and challenges. 2006 8th International Conference Advanced Communication Technology, Phoenix Park. 2006. p. 1043–1048. doi:10.1109/ICACT.2006.206151.
9. survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv [preprint]. 2009;arXiv:0909.0576.
10. Sharma K, Ghose MK. Complete security framework for wireless sensor networks. arXiv [preprint]. 2009;arXiv:0908.0122.
11. Adil M, Menon VG, Balasubramanian V, Alotaibi SR, Song H, Jin Z, et al. Survey: self-empowered wireless sensor networks security taxonomy, challenges, and future research directions. IEEE Sens J. 2023;23(18):20519-20535. doi:10.1109/JSEN.2022.3216824.
12. Nguyen DT, Trinh ML, Nguyen MT, Vu TC, Nguyen TV, Dinh LQ, et al. Security issues in IoT-based wireless sensor networks: classifications and solutions. Future Internet. 2025;17(8):350. doi:10.3390/fi17080350.
13. Zhukabayeva T, Zholshiyeva L, Mardenov Y, Buja A, Khan S, Alnazzawi N. Real-time detection and response to wormhole and sinkhole attacks in wireless sensor networks. Technologies (Basel). 2025;13(8):348. doi:10.3390/technologies13080348.
14. Wang L, Petrova K, Yang ML. Trust models in wireless sensor networks for defending against denial-of-service attacks: a literature review. Appl Sci (Basel). 2025;15(6):3075. doi:10.3390/app15063075.

