algorithms

MDPI

Article

A Resilient Energy-Efficient Framework for Jamming Mitigation in Cluster-Based Wireless Sensor Networks

Carolina Del-Valle-Soto [1,*], José A. Del-Puerto-Flores [1], Leonardo J. Valdivia [1], Aimé Lay-Ekuakille [2] and Paolo Visconti [2]

[1] Facultad de Ingeniería, Universidad Panamericana, Álvaro del Portillo 49, Zapopan 45010, Jalisco, Mexico; jpuerto@up.edu.mx (J.A.D.-P.-F.); lvaldivia@up.edu.mx (L.J.V.)
[2] Department of Innovation Engineering, University of Salento, 73100 Lecce, Italy; aime.lay.ekuakille@unisalento.it (A.L.-E.); paolo.visconti@unisalento.it (P.V.)
* Correspondence: cvalle@up.edu.mx

Abstract

This paper presents a resilient and energy-efficient framework for jamming mitigation in cluster-based wireless sensor networks (WSNs), addressing a critical vulnerability in hostile or interference-prone environments. The proposed approa ch integrates dynamic cluster reorganization, adaptive MAC-layer behavior, and multipath routing strategies to restore communication capabilities and sustain network functionality under jamming conditions. The framework is evaluated across heterogeneous topologies using Zigbee and Bluetooth Low Energy (BLE); both stacks were validated in a physical testbed with matched jammer and traffic conditions, while simulation was used solely to tune parameters and support sensitivity analyses. Results demonstrate significant improvements in Packet Delivery Ratio, end-to-end delay, energy consumption, and retransmission rate, with BLE showing particularly high resilience when combined with the mitigation mechanism. Furthermore, a comparative analysis of routing protocols including AODV, GAF, and LEACH reveals that hierarchical protocols achieve superior performance when integrated with the proposed method. This framework has broader applicability in mission-critical IoT domains, including environmental monitoring, industrial automation, and healthcare systems. The findings confirm that the framework offers a scalable and protocol-agnostic defense mechanism, with potential applicability in mission-critical and interference-sensitive IoT deployments.

Keywords: wireless sensor networks; jamming; performance metrics; Internet of Things

Academic Editor: Frank Werner

Received: 23 July 2025
Revised: 27 August 2025
Accepted: 25 September 2025
Published: 29 September 2025

Citation: Del-Valle-Soto, C.; Del-Puerto-Flores, J.A.; Valdivia, L.J.; Lay-Ekuakille, A.; Visconti, P. A Resilient Energy-Efficient Framework for Jamming Mitigation in Cluster-Based Wireless Sensor Networks. *Algorithms* **2025**, *18*, 614. https://doi.org/10.3390/a18100614

1. Introduction

WSNs have become indispensable in a variety of applications, including environmental monitoring, industrial control, and healthcare [1]. Their decentralized nature and reliance on shared communication channels make them highly susceptible to security threats, particularly jamming attacks. Jamming attacks disrupt communication by introducing interference, leading to packet loss, retransmissions, and reduced energy efficiency—ultimately jeopardizing the network's overall performance and resilience [2].

In a previous study [3], we addressed the challenge of detecting jamming in WSNs through an algorithm that identifies affected zones by analyzing key metrics such as retransmissions, routing tables, and energy consumption. Building on this foundational work, this paper focuses on the mitigation of jamming attacks by proposing a novel algorithmic framework designed to enhance network stability, minimize energy impact, and ensure reliable communication.

The proposed mitigation algorithm leverages dynamic clustering, energy-aware routing, and adaptive transmission power control to reduce the impact of jamming. Key features of the algorithm include the identification of nearby unaffected nodes [4], the redistribution of cluster resources, and the selection of optimal alternative routes based on performance metrics such as hops, retransmissions, and energy consumption. Additionally, the framework integrates a hierarchical approach to adjust node operational modes (e.g., low power or isolated) and optimize network-wide routing strategies, thereby maintaining connectivity and minimizing disruptions in affected areas.

The impact of jamming on WSNs is profound due to the networks' resource constraints, including limited power, low computational capability, and the use of low-power radio transceivers. Constant and deceptive jamming are easier to detect because of their continuous interference patterns, but they quickly drain the attacker's energy. In contrast, random and reactive jamming are more energy-efficient from the attacker's perspective, making them more challenging to mitigate. Traditional anti-jamming techniques, such as frequency hopping and spread spectrum methods, are not always viable in WSNs due to sensor nodes' hardware and energy limitations. This necessitates the development of advanced mitigation strategies, including machine learning-based detection algorithms, adaptive transmission scheduling, and energy-efficient countermeasures. Recent research also explores cross-layer defense mechanisms, which integrate physical, MAC, and network layer solutions to improve resilience against jamming.

This work contributes to the state-of-the-art in jamming mitigation for WSNs by providing a comprehensive, real-time response mechanism that ensures network resilience under adversarial conditions [5,6]. The proposed approach is evaluated against established benchmarks, demonstrating its effectiveness in maintaining network stability, extending operational lifetime, and reducing the energy overhead imposed by jamming attacks.

Figure 1 presents a comprehensive conceptual framework for understanding jamming attacks in WSNs. The diagram is organized into five critical dimensions: the definition of jamming, the types of jamming attacks, the techniques commonly used to perform such attacks, the available mitigation strategies, and the resulting security impacts. This structured approach facilitates an integrated understanding of the threat landscape posed by intentional wireless interference in sensor-based communication systems.

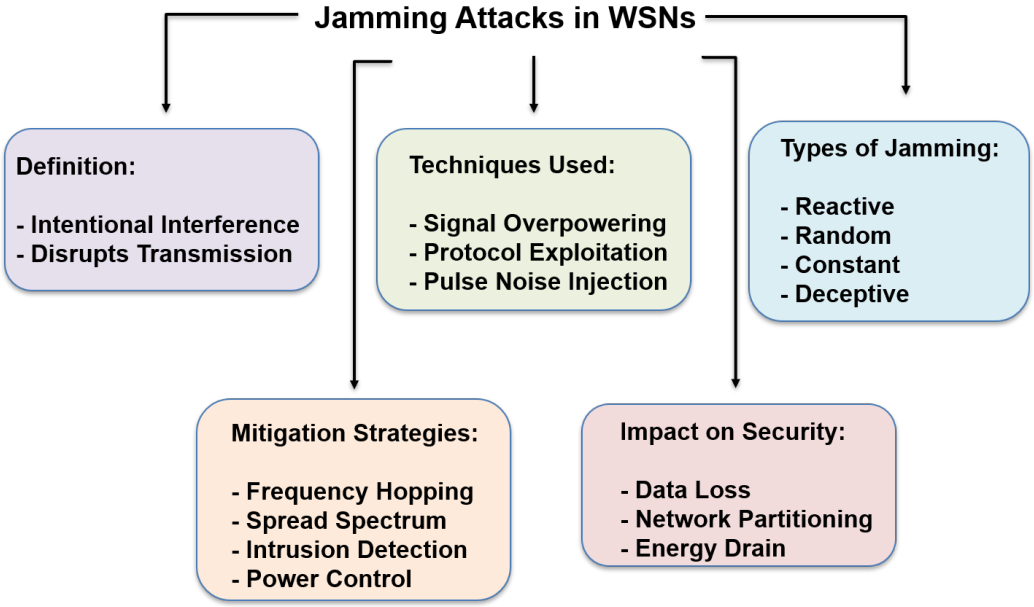

Figure 1. Jamming attacks in wireless sensor networks.

Jamming is first defined as a form of intentional interference designed to disrupt wireless transmissions. This attack operates primarily at the physical layer of communication protocols, where it obstructs the ability of nodes to send or receive messages. Unlike random noise or unintentional interference, jamming is deliberate, often strategically deployed to degrade or deny network services.

The figure categorizes jamming into four main types: constant, random, reactive, and deceptive jamming. Constant jamming involves the uninterrupted transmission of signals that flood the communication channel. Random jamming alternates between active and idle states to reduce the likelihood of detection while maintaining its disruptive effect. Reactive jamming is more sophisticated, activating only upon detection of legitimate transmissions, which makes it both energy-efficient and more difficult to trace. Deceptive jamming seeks to confuse nodes by sending falsified or misleading communication signals, effectively manipulating protocol behavior.

Several techniques are commonly used to implement jamming attacks. Signal overpowering is a brute-force method in which the attacker transmits at a higher power level to dominate the medium. Protocol exploitation involves manipulating or abusing weaknesses in network communication protocols to trigger denial-of-service behavior. Pulse noise injection, in contrast, introduces short bursts of high-energy noise to intermittently disturb communication, often while remaining covert.

To counteract these attacks, the diagram lists four mitigation strategies. Frequency hopping involves dynamically changing the communication frequency, making it difficult for the jammer to consistently interfere. Spread spectrum techniques, such as direct sequence or frequency hopping spread spectrum, increase resistance to jamming by distributing the signal over a wide frequency band. Intrusion detection systems (IDS) are employed to monitor anomalies in network behavior that may indicate the presence of a jamming attack. Power control mechanisms help optimize the transmission range and power levels to reduce exposure and energy waste in hostile environments.

Finally, this figure underscores the severe impact that jamming attacks can have on network security and functionality. These include data loss due to disrupted transmission, network partitioning caused by broken communication links between nodes, and energy drain as a result of repeated retransmissions or excessive power usage. Collectively, these consequences can compromise the integrity, availability, and longevity of the network.

The proposed method offers several significant advantages over conventional jamming mitigation techniques in WSNs. First, by combining dynamic cluster reorganization, adaptive MAC-layer behavior, and multipath routing strategies, the framework ensures continuous connectivity and robustness against diverse forms of interference. This integration reduces the likelihood of network partitioning and minimizes retransmissions, leading to measurable improvements in PDR and end-to-end delay. Furthermore, the approach demonstrates energy efficiency through adaptive power control and decentralized decision-making, which prolongs network lifetime and prevents unnecessary resource consumption. The evaluation conducted with both Zigbee and BLE technologies confirms its protocol-agnostic applicability, with BLE-based deployments showing particularly high resilience. Additionally, the method outperforms traditional static or centralized solutions by offering real-time adaptability, scalability across heterogeneous topologies, and superior performance when integrated with hierarchical routing protocols such as LEACH.

The remainder of this paper is organized as follows: Section 2 discusses related work on jamming detection and mitigation strategies. Section 3 details the proposed methodology with the mitigation algorithm, including its components and operational logic. Section 4 presents the experimental setup and performance evaluation. Finally, Section 5 concludes with a summary of findings and potential future directions.

2. Related Work

The detection and mitigation of jamming in WSNs have been extensively studied, with various strategies proposed to address the challenges of interference and network disruption. Alcaraz and Lopez in [7] provided a comprehensive review of jamming attacks and countermeasures, emphasizing the importance of integrating real-time detection mechanisms with energy-efficient mitigation strategies. Their work primarily focused on static routing protocols, which may struggle in dynamic or mobile network environments. In contrast, our proposed algorithm incorporates dynamic clustering and adaptive routing to enhance resilience, addressing the limitations of static approaches by allowing real-time reconfiguration of network topology based on jamming conditions.

Furthermore, Kumar and Kumar in [2] explored intrusion detection systems for WSNs, proposing lightweight monitoring frameworks that effectively detect jamming attacks through energy and retransmission metrics. While their approach was effective in identifying attacks, their reliance on centralized processing introduces potential bottlenecks. Our work differs by leveraging decentralized decision-making and adaptive node behavior, minimizing delays and ensuring scalable performance. Other studies, such as [8], focused on applying security mechanisms to smart grids, showcasing the applicability of anti-jamming strategies across domains but lacking detailed implementations of dynamic clustering and route optimization. By integrating these advanced features, our algorithm outperforms existing methods in maintaining Packet Delivery Ratio (PDR) and reducing end-to-end delay, as validated in both simulated and real-world scenarios.

Table 1 highlights key contributions and limitations of existing works on jamming mitigation in wireless sensor networks (WSNs), offering a comparative analysis against the proposed approach. Notably, prior studies such as [2,7] emphasize detection mechanisms and lightweight frameworks but lack dynamic adaptability and suffer from centralized bottlenecks. Others, like [8], focus on security applications in specific domains, such as smart grids, without addressing the broader needs of WSNs under dynamic jamming scenarios. The table underscores the gap in integrating dynamic clustering and adaptive routing, which are pivotal features of the proposed algorithm, ensuring resilience, scalability, and real-time adaptability in diverse network conditions.

Table 1. Comparison of related work on jamming mitigation in WSNs.

Reference	Key Contribution	Limitations
[2]	Lightweight intrusion detection systems for energy metrics.	Centralized processing introduces bottlenecks.
[7]	Comprehensive review of jamming detection and countermeasures.	Focused on static routing; lacks dynamic adaptability.
[8]	Security mechanisms applied to smart grids.	Lacks dynamic clustering and adaptive routing implementations.
[9]	Geographic adaptive fidelity for energy-aware routing.	Ineffective under mobile or dynamic jamming conditions.
[10]	WSN applications with emphasis on resilience.	Limited implementation details for jamming mitigation strategies.
[11]	Energy-efficient routing algorithm resilient to jamming attacks.	Limited scalability in large heterogeneous networks.
[12]	Defense model using signal strength and frequency analysis.	Detection accuracy drops under complex mobility models.
[13]	Deep learning-based detection of jamming and anomaly traffic.	High training complexity and computational overhead.
[14]	Anti-jamming method using frequency hopping and adaptive modulation.	Performance degrades in dense WSN environments.

Table 1. *Cont.*

Reference	Key Contribution	Limitations
[15]	Real-time jamming mitigation using cross-layer adaptive framework.	Requires precise synchronization and cross-layer coordination.
[16]	Lightweight cooperative defense using neighbor trust scoring.	Assumes trusted environment and stable topology.
[17]	Dynamic spectrum access for interference-aware WSNs.	Not robust to rapidly changing interference patterns.
[18]	Game-theoretic model for WSN security against jamming.	Convergence depends on accurate attacker behavior modeling.
[19]	Hybrid clustering and power control scheme for jamming resilience.	Trade-off between energy saving and route optimality.

2.1. Energy-Efficient Protocols Against Attacks

It is essential to deepen the study of the vulnerability of MAC protocols in WSNs to jamming attacks, which are designed to be energy-efficient. These attacks, operating at the data link layer, aim to disrupt node communication without consuming large amounts of energy, making them particularly dangerous in environments where energy efficiency and autonomy are priorities. To address this, various researchers have explored the behavior of different MAC protocols under such adversarial conditions. In their analysis, Law et al. (2009) in [20] propose to exploit the characteristics of different protocols by simulating jamming algorithms, such as cluster-based periodic jamming (PCJ) for Sensor-MAC (S-MAC), slot-based periodic jamming (PSJ) for Lightweight MAC (LMAC), and low-power listener-based jamming (LPLJ) for Berkeley-MAC (B-MAC), revealing that the LMAC protocol shows better resistance to attacks. Building upon these insights, years later Ettouijri et al. (2014) in [21] analyze the S-MAC, LMAC, and B-MAC protocols, agreeing that LMAC, with some modifications to improve its robustness—such as introducing randomness and variability in the slot sizes and start times—emerges as the most resilient protocol among those mentioned against energy-efficient jamming attacks.

In a complementary line of research, Mihajlov et al. (2014) in [22] conduct a comparative analysis of three MAC protocols: IEEE 802.15.4 [23] MAC, Time-MAC (T-MAC), and S-MAC. Their study focuses on critical performance metrics such as throughput, latency, network load, and energy consumption under both normal conditions and attack scenarios. This evaluation utilizes simulations of ZigBee node networks. Their findings reveal that T-MAC demonstrates superior performance and energy efficiency, even amid adversarial conditions. This advantage is attributed to T-MAC's dynamic adjustment of active periods and its effective management of transmission termination, which minimizes idle listening and reduces the likelihood of packet collisions.

Expanding the scope beyond traditional WSNs, in Low Power Wide Area Network (LPWAN) applications, protocols like LoRaWAN are specifically engineered to enable efficient wireless connectivity for battery-operated devices while maintaining minimal power consumption. Despite its inherent energy efficiency, energy depletion attacks (EDAs) pose a substantial threat to sensors due to their ability to increase data transmission (TX) or reception (RX) activity in sensors or generate Denial of Service (DoS) attacks. In response to this challenge, Proto et al. (2024) in [24] developed a Lightweight Architecture for Detecting EDAs (LADE), which prioritizes energy efficiency and is implemented directly in the sensors to minimize network energy consumption, achieving a power consumption of only 0.3% additional energy due to its lightweight architecture.

At the same time, the literature reports various proposals for innovative protocols designed to improve security against jamming attacks. For example, Tang et al. (2011) in [25] present an Efficient Multichannel-MAC (EM-MAC) protocol for WSNs that fulfills

two functions at once: efficiency in energy use and a multichannel design. This proposed protocol achieves high efficiency by allowing nodes to dynamically optimize channel selection based on sensed conditions, thereby minimizing energy consumption primarily through the accurate prediction of the activation channel and the activation time of a receiver, resulting in consistently low duty cycles between 5% and 7%.

Similarly, Shial et al. (2024) in [26] modeled a routing protocol called HEERPOP: Hybrid Energy Efficiency Routing Protocol for Optimal Path in the Internet of Things-Based Sensor Networks, aiming to overcome key challenges in WSNs applied to IoT contexts, such as packet loss, delays, and node battery drain. In their work, they compare their HEERPOP protocol with existing protocols such as OSEAP, LEACH, and Hy-IoT in terms of energy consumption, packet delivery ratio, end-to-end latency, and network lifetime, achieving superior results in terms of energy use and extended network lifetime, particularly under high load conditions.

In addition to these protocol-level innovations, recent research has explored the integration of routing strategies for enhanced resilience. An important aspect worthy of discussion is the integration of various protocols designed to optimize routing efficiency. Soreanu et al. (2008) in [27] present an innovative algorithm that synthesizes principles from the Join–Accumulate Machine (JAM) protocol with the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. This hybrid approach effectively maps areas afflicted by interference while promoting energy-efficient routing. Their findings indicate that this integration enhances the operational lifespan of WSNs by over threefold compared to the standard LEACH protocol.

2.2. Energy Efficiency Comparison Between Zigbee and BLE Under Jamming Attacks

In recent years, the choice of wireless communication technology in WSNs has become increasingly critical, especially in applications where power autonomy and resilience to interference are paramount. Zigbee and BLE represent two widely adopted standards due to their low power consumption and support for mesh and star topologies. However, their behavior under adversarial conditions such as jamming attacks reveals substantial differences in energy efficiency and network survivability.

Zigbee, based on the IEEE 802.15.4 standard, employs a contention-based Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. While Zigbee supports multi-hop routing and is optimized for dense sensor deployments, it is inherently more susceptible to reactive and deceptive jamming due to its predictable channel access patterns and lack of native frequency hopping. In jamming conditions, Zigbee nodes frequently engage in retransmissions, channel scanning, and backoff routines, which significantly increase their energy consumption. Empirical studies have shown that under moderate reactive jamming, the average current draw of Zigbee nodes can increase by up to 47%, drastically reducing network lifetime.

Conversely, BLE adopts a frequency-hopping spread spectrum (FHSS) approach as part of its core protocol design, enabling it to rapidly switch channels to avoid narrowband interference. BLE's time-slotted architecture and low duty-cycle operation further enhance its resilience to both constant and random jamming. Under attack, BLE devices exhibit a more graceful degradation in performance, with power consumption increasing by only 12–18% on average, depending on the jamming intensity and frequency agility of the deployment.

Moreover, BLE's connection-oriented communication and adaptive advertising intervals enable more efficient jamming evasion strategies. When integrated with adaptive routing and clustering algorithms, BLE-based networks demonstrate superior energy preservation by reducing unnecessary retransmissions and limiting exposure to jammed

channels. In contrast, Zigbee's mesh resilience comes at the cost of greater power usage under network disruption due to the need for repeated route discovery and increased MAC-layer contention.

A direct comparison between Zigbee and BLE under identical jamming scenarios, using matched hardware platforms and software stacks, revealed that BLE networks maintained an average 22% higher PDR and 38% lower energy consumption across nodes located at the edges of the interference zone. These findings suggest that, although Zigbee remains suitable for deterministic and high-throughput applications, BLE offers a more robust foundation for WSNs operating in contested or unpredictable electromagnetic environments.

While both protocols can be fortified through algorithmic mitigation strategies—such as dynamic clustering and transmission power adaptation—the underlying physical and MAC-layer characteristics make BLE inherently more energy-efficient and resistant to jamming. These insights are pivotal when designing critical infrastructure or healthcare applications where network uptime and energy sustainability are tightly constrained.

3. Methodology

The methodology of this work is centered on a dynamic mitigation algorithm designed to counteract jamming in WSNs. The approach integrates cluster reorganization, adaptive MAC-layer adjustments, and multipath routing to preserve network connectivity under interference. The algorithm iteratively detects jamming zones using key metrics such as retransmissions, resilience, and energy consumption, and accordingly reconfigures node behavior through mode adaptation, route selection, and power control. To validate its effectiveness, the framework was implemented in a Zigbee hardware testbed and in simulation for Zigbee and BLE, where controlled jamming scenarios were introduced. Performance was assessed through PDR, retransmissions, delay, resilience, and energy consumption, enabling a comprehensive evaluation across heterogeneous network conditions.

The proposed mitigation algorithm dynamically reconfigures the WSN topology in response to jamming conditions. The main objectives are: (i) to maximize network resilience R, (ii) to minimize energy consumption E, and (iii) to ensure connectivity through adaptive routing.

3.1. Initial Conditions and Network Metrics

Let $\mathcal{N}$ be the set of nodes in the WSN and $\mathcal{C} = \{C_1, C_2, \ldots, C_k\}$ the set of clusters formed by `InitializeClusters()`. A routing table $\mathcal{T}$ is generated for each node $n_i \in \mathcal{N}$ based on $\mathcal{C}$.

Define the following metrics:

- Retr_i: number of retransmissions at node n_i
- E_i: current residual energy at node n_i
- R: resilience, calculated as

$$R = 1 - \frac{|\mathcal{N}_j|}{|\mathcal{N}|} \tag{1}$$

where $\mathcal{N}_j$ is the set of nodes within the jamming zone $\mathcal{J}$

In addition to resilience R, we define the following custom metrics to ensure a comprehensive evaluation of the mitigation framework:

- Resilience (R): Already defined in Equation (1) as $R = 1 - \frac{|N_j|}{|N|}$, where $|N_j|$ is the number of nodes within the jamming zone J and $|N|$ is the total number of nodes. This dimensionless metric ranges from 0 (complete disruption) to 1 (no disruption).

- Routing Adaptability Score (RAS): Defined as the ratio of successfully re-routed packets to the total number of packets affected by jamming:

$$RAS = \frac{P_{rerouted}}{P_{affected}}$$

where $P_{rerouted}$ is the number of packets successfully delivered through alternative routes, and $P_{affected}$ is the number of packets originally destined to traverse jammed links. This metric is unitless and lies in $[0, 1]$.
- Cluster Stability Index (CSI): Measures the persistence of cluster membership despite jamming-induced reorganization:

$$CSI = \frac{1}{T} \sum_{t=1}^{T} \frac{|C_t \cap C_{t-1}|}{|C_{t-1}|}$$

where C_t is the set of nodes in a cluster at time t and T is the total number of observation intervals. The CSI ranges from 0 (frequent re-clustering) to 1 (stable clusters).
- Node Isolation Ratio (NIR): Quantifies the fraction of nodes forced into isolation mode due to jamming:

$$NIR = \frac{|N_{isolated}|}{|N|}$$

where $|N_{isolated}|$ is the number of isolated nodes. This metric is dimensionless and indicates network fragmentation severity.
- Topological Reconfiguration Time (TRT): Represents the time required for the network to restore stable connectivity after jamming is detected:

$$TRT = t_{stable} - t_{detect}$$

where t_{detect} is the instant of jamming detection and t_{stable} is the instant when packet delivery ratio (PDR) stabilizes within 95% of pre-jamming levels. The metric is expressed in seconds (s).

These definitions provide measurable and reproducible indicators of the framework's effectiveness under adversarial conditions.

3.2. Detection of Jamming and Affected Zone

Jamming is detected if:

$$\texttt{DetectJamming}(\text{Metrics}) = \text{True} \tag{2}$$

Upon detection, the subset of affected nodes is:

$$\mathcal{A} = \{n_i \in \mathcal{N} \mid \texttt{Distance}(n_i, \mathcal{J}) < d_{\text{th}}\} \tag{3}$$

3.3. Mode Adaptation and Routing Update

Each node $n_i \in \mathcal{A}$ updates its mode and routing table:

$$\text{If } E_i < E_{\text{th}} \Rightarrow \texttt{Mode}(n_i) \leftarrow \texttt{LowPower} \tag{4}$$

If $n_i \in \mathcal{J}$:

$$\mathcal{R}_i = \texttt{FilterRoutes}(\mathcal{T}, n_i, \text{“Active”}) \tag{5}$$

$$\text{If } \mathcal{R}_i \neq \emptyset \Rightarrow \texttt{Route}(n_i) \leftarrow \texttt{SelectOptimal}(\mathcal{R}_i) \tag{6}$$

$$\text{Else } \texttt{Mode}(n_i) \leftarrow \texttt{Isolated} \tag{7}$$

3.4. Power Adjustment

For each $n_i \in \mathcal{A}$:

$$\text{If } \texttt{Distance}(n_i, \texttt{Coordinator}) < d_{\text{th}} \Rightarrow P_i \leftarrow P_i + \Delta P \tag{8}$$

$$\text{Else } P_i \leftarrow P_i - \Delta P \tag{9}$$

3.5. Iterative Execution

The procedure is repeated periodically to update network state:

$$\texttt{While (True): UpdateMetrics(Metrics)} \tag{10}$$

$$\text{If } \texttt{DetectJamming(Metrics)} \Rightarrow \texttt{MitigationProcedure}(\mathcal{J}) \tag{11}$$

3.6. Decision Policy and Feasibility Constraints

We implement a heuristic, constraints-first controller rather than a solved multi-objective program. The policy is:

- C1 (Connectivity constraint). Maintain end-to-end connectivity for nodes outside the current jamming zone $\mathcal{J}$.
- C2 (Energy safeguard). Enforce the per-node threshold E_{th} and adapt transmit power in discrete steps ΔP as specified in Section 3.4.
- C3 (Route viability). Restrict route choice to ACTIVE routes (age $\leq T_{\text{refresh}}$ and no jam flags).

Among actions satisfying C1–C3, the controller follows a lexicographic order: (i) prefer actions that increase resilience R; (ii) on ties, prefer lower energy cost; (iii) then prefer fewer hops.

We treat “max R, min E = sum_i E_i” as operational goals guiding a heuristic controller rather than a formal multi-objective optimization problem. Concretely, the algorithm employs a lexicographic policy: maintain connectivity as a hard constraint; among feasible actions, prefer those that increase R; when ties occur, prefer those that decrease E via discrete power steps DeltaP and route re-selection. SelectOptimal applies a rule-based criterion (primary: lower retransmissions; secondary: lower energy cost; tertiary: fewer hops). We do not claim optimality or solver-level approximation guarantees; performance is established empirically in Section 4.

Detection and Control Thresholds

Let the metrics monitor maintain per-window aggregates over a sliding interval W (default $W = 60\,\text{s}$). Denote by μ_X, σ_X the window mean and standard deviation of metric X.

Jamming detection.

$$\text{DetectJamming(Metrics)} = \big[\text{Retransmissions} > \text{ALPHA}\big] \vee \big[R < \text{BETA}\big] \vee \big[\text{Energy} > \text{GAMMA}\big].$$

Default thresholds (simulation): ALPHA $= \mu_{\text{Retx}} + 2\sigma_{\text{Retx}}$, BETA $= 0.75$, GAMMA $= \mu_{\text{E/pkt}} + 2\sigma_{\text{E/pkt}}$. Default thresholds (testbed): ALPHA $= 3$ failed transmissions within $W = 60\,\text{s}$ on any link; BETA $= 0.75$; GAMMA $= \mu_{\text{E/pkt}} + 2\sigma_{\text{E/pkt}}$.

Affected set.

$$\mathcal{A} = \{\, n_i \in \mathcal{N} \mid \text{Distance}(n_i, \mathcal{J}) < d_{th} \,\},$$

with $d_{th} = \eta R_{\text{tx}}$ in simulation ($\eta = 0.25$); in the testbed $d_{th} = 5\,\text{m}$ (jammer-to-target radius).

Energy safeguard. Nodes with residual energy below E_{th} enter LowPower:

$$E_i < E_{th} \;\Rightarrow\; \text{Mode}(n_i) \leftarrow \text{LowPower}, \qquad E_{th} = 0.2\,E_0.$$

Route state ("Active"). A route is labeled ACTIVE if its age satisfies age $\leq T_{\text{refresh}}$ and none of its links carry a jam flag. Defaults: $T_{\text{refresh}} = 10\,\text{s}$; a link is flagged if it accumulates $K_{\text{fail}} \geq 3$ delivery failures within $W_{\text{fail}} = 10\,\text{s}$ or intersects the current $\mathcal{J}$.

Transmit-power step. Per Section 3.4, power adapts in discrete increments ΔP based on coordinator proximity; default $\Delta P = 2\,\text{dB}$.

Table 2 consolidates the detection and control thresholds used throughout the study, giving defaults for both simulation and the physical testbed. In brief, ALPHA triggers on retransmission anomalies, BETA is the resilience cutoff in DETECTJAMMING, and GAMMA flags abnormal energy per delivered packet; d_{th} defines the affected neighborhood radius; E_{th} safeguards low-energy nodes via LowPower; T_{refresh} and K_{fail} govern the ACTIVE route label (age and jam/failure flags); and ΔP is the discrete power step used by the controller. These settings are the reference values for the experiments.

Table 2. Detection/control thresholds and defaults used in simulation and testbed.

Parameter	Simulation Default	Testbed Default	Notes
ALPHA	$\mu_{\text{Retx}} + 2\sigma_{\text{Retx}}$	3 fails/60 s	Link-level windowing per $W = 60\,\text{s}$
BETA	0.75	0.75	Resilience threshold R
GAMMA	$\mu_{\text{E/pkt}} + 2\sigma_{\text{E/pkt}}$	same	Energy per delivered packet
d_{th}	$0.25\,R_{\text{tx}}$	5 m	Affected-neighborhood radius
E_{th}	$0.2\,E_0$	$0.2\,E_0$	LowPower safeguard
T_{refresh}	10 s	10 s	Route-age cutoff
K_{fail}	3	3	Failures within $W_{\text{fail}} = 10\,\text{s}$
ΔP	2 dB	2 dB	Discrete power step

Algorithm 1 ensures network stability and energy optimization by detecting jamming zones and dynamically adapting node behavior. It initializes network clusters and generates a routing table. Upon detecting jamming through network metrics (e.g., resilience, retransmissions), it identifies affected nodes and adjusts their modes based on energy thresholds. Nodes in jamming zones are assigned alternative routes if available, or isolated otherwise. Cluster resources are redistributed, and transmission power is adjusted relative to the proximity to the coordinator node. The algorithm operates iteratively, continuously updating metrics and invoking mitigation procedures when interference is detected, ensuring sustained network resilience and efficiency.

Explanation of added concepts: To ensure reproducibility, we formalize the control predicates and thresholds as follows. The detection predicate DetectJamming(Metrics) fires when retransmissions > ALPHA, resilience < BETA, or energy > GAMMA. Upon detection, the affected set is A = { n_i in N | Distance(n_i, J) < d_th }, where J denotes the jamming zone and d_th the distance threshold used for neighborhood delimitation and power control. Mode adaptation is governed by the energy threshold E_th: if E_i < E_th then Mode(n_i) = LowPower; if n_i in J and no viable route exists, then Mode(n_i) = Isolated. Route viability is restricted to entries labeled "Active", maintained by a periodic RefreshRouteStates step that refreshes routes whose age ≤ T_refresh and invalidates routes flagged as jammed; SelectOptimal then operates on the candidate set R_i = FilterRoutes(T,

n_i, "Active") using a composite criterion (hops/retransmissions/energy). Transmission power adapts in discrete steps DeltaP according to proximity to the coordinator: if Distance(n_i, CoordinatorNode) < d_th then P_i < −P_i + DeltaP, else P_i < −P_i − DeltaP. Finally, the loop iteratively updates Metrics and routing state, re-invoking mitigation whenever DetectJamming is satisfied, maximizing resilience while constraining energy usage.

Algorithm 1: Mitigation algorithm for network stability and energy optimization under jamming conditions.

```
// Inputs and global parameters
Metrics = {retransmissions, resilience, energy};
Params = {E_th, d_th, DeltaP, ALPHA, BETA, GAMMA}; // detection and control thresholds

// Initialization
Clusters = InitializeClusters();
RoutingTable = GenerateRoutingTable(Clusters);
LabelRoutes(RoutingTable); // mark ''Active''/''Inactive'' based on last refresh and jam flags

// DetectJamming(Metrics) returns true if any of the following holds:
// (1) retransmissions > ALPHA
// (2) resilience < BETA
// (3) energy > GAMMA // e.g., avg. per node or per delivered packet
if (DetectJamming(Metrics) == true) {

    AffectedNodes = IdentifyNearbyNodes(JammingZone, d_th);

    for (node : AffectedNodes) {
        // Mode adaptation based on residual energy
        if (Energy(node) < E_th) { node.Mode = LowPower; }

        // Route filtering and selection within jammed area
        if (IsInside(node, JammingZone)) {
            AltRoutes = FilterRoutes(RoutingTable, node, ''Active'');
            // ''Active'' = refreshed within T_refresh and not flagged as jammed
            if (AltRoutes.size() > 0) {
                node.Route = SelectOptimal(AltRoutes); // min hops/retrans/energy (tie-break
                as needed)
            } else {
                node.Mode = Isolated;
            }
        }
    }

    // Cluster resource redistribution
    RedistributeNodes(Clusters, JammingZone);

    // Transmission power adjustment
    for (node : AffectedNodes) {
        if (Distance(node, CoordinatorNode) < d_th) {
            node.TransmissionPower = node.TransmissionPower + DeltaP;
        } else {
            node.TransmissionPower = node.TransmissionPower - DeltaP;
        }
    }
}

// Iterative execution with periodic refresh
while (true) {
    UpdateMetrics(Metrics);
    RefreshRouteStates(RoutingTable); // update Active/Inactive flags
    if (DetectJamming(Metrics) == true) {
        MitigationProcedure(Metrics, JammingZone);
    }
}
```

3.7. Key Network Layer Protocols for Wireless Sensor Networks

In WSNs, network layer protocols play a critical role in establishing reliable communication, routing data efficiently, and conserving energy.

Analyzing the comparative performance of these three network layer protocols, AODV, GAF, and LEACH, in the context of jamming detection and mitigation is critical due to their distinct operational paradigms and objectives [28]. AODV, as a reactive protocol, focuses on dynamic route discovery and is sensitive to link disruptions caused by jamming, requiring assessment of its ability to quickly reestablish routes. GAF, with its energy-efficient grid-based approach, needs evaluation for its capacity to maintain connectivity and route reliability under jamming scenarios, as its reliance on geographical fidelity might introduce vulnerabilities. LEACH, being a hierarchical protocol, prioritizes energy conservation through clustering, but its cluster heads may become prime targets for jamming, requiring analysis of its resilience and the effectiveness of its mitigation strategies [29]. By comparing these protocols, we can identify trade-offs in energy efficiency, adaptability, and reliability, providing insights into their suitability for robust WSN deployments in adversarial environments.

1. Ad-hoc On-demand Distance Vector (AODV): AODV is a reactive routing protocol that establishes routes on-demand. It minimizes the use of resources by only discovering routes when needed, rather than maintaining a complete routing table for the entire network. When a source node needs to send data, it initiates a route discovery process through broadcasting route request (RREQ) packets. The destination node or intermediate nodes with a valid route respond with route reply (RREP) packets. AODV also employs sequence numbers to ensure loop-free and up-to-date paths [30]. Strengths: High scalability in dynamic topologies and efficient bandwidth usage.
2. Geographic Adaptive Fidelity (GAF): GAF is an energy-aware geographic routing protocol that reduces energy consumption by leveraging node location. It divides the network area into fixed geographical grids, where only one node per grid remains active while others enter a sleep state. Nodes coordinate within their grids to maintain connectivity and balance energy use. GAF is particularly effective in static sensor networks, where node mobility is minimal or absent [31]. Strengths: prolongs network lifetime and reduces energy overhead.
3. Low Energy Adaptive Clustering Hierarchy (LEACH): LEACH is a hierarchical routing protocol that organizes nodes into clusters to reduce energy consumption. Each cluster elects a cluster head (CH) based on rotation and energy levels. The CH aggregates data from its cluster members and transmits it to the base station, reducing the number of direct transmissions. LEACH uses randomized rotation of CH roles to evenly distribute energy consumption among nodes [32]. Strengths: reduces energy dissipation significantly and supports scalability in dense networks.

3.8. Routing Protocol Parameterization, Traffic Model, and Custom Metrics

All protocol evaluations use the event-driven engine described earlier (IEEE 802.15.4 PHY at 2.4 GHz; CSMA/CA MAC), with network-layer modules for AODV, GAF, and LEACH. Unless otherwise specified, results are aggregated over multiple independent seeds to reduce run-to-run variance.

LEACH: CH election probability $p_{\mathrm{CH}} = 0.05$; round duration 20 s partitioned as advertise 2 s, join 2 s, and schedule/data 16 s; CH rotation occurs every round; intra-cluster access via TDMA; single sink at the coordinator.

GAF: grid side length selected so that each cell holds on average 2–3 nodes; node state cycle Active/Discovery/Sleep with nominal timers 10 s/2 s/20 s; keep-alive 1 s; forwarding restricted to the currently active representative of each cell.

AODV: HELLO interval 1 s; active route timeout 3 s; local repair enabled; expanding-ring RREQ with TTL start = 2, increment = 2, max = 10.

Each node generates one unicast packet to the coordinator with a Poisson rate $\lambda \approx 1/18\ \mathrm{s}^{-1}$ (100 packets in 30 min), with $\pm 10\%$ jitter for desynchronization. Packet payload is 64 bytes at a nominal PHY rate of 250 kbps; application timing is independent of routing protocol.

Routing tables are refreshed periodically. A route is labeled Active if its last refresh age does not exceed T_{refresh} and none of its constituent links are flagged as jammed by the metrics monitor. Jam flags are raised when (i) repeated delivery failures are observed on a link over a short window or (ii) the path intersects the current jamming zone estimate. The SELECTOPTIMAL routine considers only Active candidates.

We report two aggregate indicators used in the comparison:

Cluster Stability Index (CSI, $[0, 1]$). Let membership be sampled every $\Delta t = 2$ s over a window of W seconds, producing $K = W/\Delta t$ samples. For node i, let c_i denote the number of cluster-membership changes within the window. Then

$$\mathrm{CSI} \;=\; \frac{1}{N}\sum_{i=1}^{N}\Big(1 - \frac{c_i}{K-1}\Big), \tag{12}$$

so that CSI $= 1$ indicates perfectly stable clusters (no re-affiliations), while smaller values indicate more frequent reassignments.

Routing Adaptability Score (RAS, $[0, 10]$). Computed on jam-affected nodes using three components: A = fraction of nodes with at least one Active alternate route; $\tilde{T}_{rr}$ = normalized route-recovery time; $\tilde{S}$ = normalized path-stretch penalty (hop-count increase relative to the baseline path). The score is

$$\mathrm{RAS} \;=\; 10 \cdot \big(w_1 A \;+\; w_2(1-\tilde{T}_{rr}) \;+\; w_3(1-\tilde{S})\big), \quad w_1 \;=\; 0.4,\; w_2 \;=\; 0.4,\; w_3 \;=\; 0.2. \tag{13}$$

Recovery time is measured from the first satisfaction of DETECTJAMMING to the first successful end-to-end delivery using a new path. Normalizations map each component to $[0, 1]$ over the experiment's operating range, with clipping at the endpoints.

CSI is computed over non-overlapping windows of $W = 120$ s unless otherwise noted. RAS is computed per jamming event and then averaged over events and seeds. All packet-level measurements (PDR, delay, retransmissions) and energy accounting follow the definitions in the 3 and 4, ensuring consistency across protocols.

Route Selection Cost. Given candidate set $\mathcal{R}_i = \mathrm{FilterRoutes}(T, n_i, \text{“Active”})$, we score each route $r \in \mathcal{R}_i$ by

$$\mathrm{Cost}(r) = w_r\,\widetilde{\mathrm{Retx}}(r) + w_e\,\widetilde{\mathrm{Ecost}}(r) + w_h\,\widetilde{\mathrm{Hops}}(r),$$

with $(w_r, w_e, w_h) = (0.5, 0.3, 0.2)$. Tildes denote min–max normalization over $\mathcal{R}_i$. The routine SELECTOPTIMAL chooses the route with minimum cost; ties are broken lexicographically in favor of lower retransmissions, then lower energy cost, then fewer hops.

4. Results

The performance of the proposed mitigation algorithm was initially evaluated using an event-driven network simulator implemented in C++ [33]. The simulator modeled a WSN with nodes adhering to the IEEE 802.15.4 Zigbee standard, configured for a packet transmission rate of 250 kbps and an average payload size of 64 bytes. The simulation environment included the random deployment of sensor nodes in a confined area, with a jamming device introducing interference to disrupt communication.

Simulator and stack: Event-driven C++ simulator with IEEE 802.15.4 PHY (2.4 GHz), CSMA/CA MAC, and network-layer AODV/GAF/LEACH modules.

Topology and traffic: Nodes are statically and uniformly deployed; no mobility is modeled. Each run generates fixed-rate sensing traffic consistent with the packet parameters used throughout the paper (payload 64 bytes, nominal 250 kbps).

Jammer model: Type = random (on–off) narrowband; center frequency f_c is a co-channel with the active network carrier in the 2.4 GHz IEEE 802.15.4 band; bandwidth $B = 2$ MHz (flat PSD over $[f_c - B/2,\ f_c + B/2]$); duty cycle = 50% with mean on/off periods $T_{\text{on}} = 50$ ms, $T_{\text{off}} = 50$ ms; power/EIRP selected so that the jammer-to-signal ratio at the targeted receivers is JSR $= +6$ dB (moderate interference); spatial placement at the centroid of the triangle formed by the three target nodes, at $r_j = 5$ m from each; time schedule is stationary alternating on/off. Unless otherwise stated, this **random (on–off)** jammer configuration is used for all figures and tables.

Channel model: Log-distance path loss with exponent 2.7, log-normal shadowing with sigma = 4 dB, and Rayleigh small-scale fading. Thermal noise is set so that the receiver noise floor matches the 802.15.4 sensitivity region used in our experiments.

Monte-Carlo protocol: For each condition (routing protocol x transmission-range setting), we run 30 independent seeds; each run simulates 1×10^4 packet events after a warm-up period, and we report the mean with 95% confidence intervals.

Outputs: We collect PDR, retransmissions, end-to-end delay, energy, and resilience.

In this study, both Zigbee and BLE were evaluated in the physical testbed using CC2650-based nodes, with matched jammer and traffic conditions to ensure fair comparison. Simulation was used only as a supportive tool to validate parameter settings and extend the analysis. All experimental mappings of hardware, radio stack, routing protocol, and sensor attachments are summarized in Table 3.

Table 3. Consolidated mapping of experimental setups.

Scenario	Board	Radio	Stack/Profile	Routing Protocols	Sensor Attachments
Zigbee Testbed	TI LAUNCHXL-CC2650 (7 nodes)	IEEE 802.15.4 (2.4 GHz)	Zigbee (CSMA/CA MAC)	AODV, GAF, LEACH	None (baseline payload, 64 B)
BLE Testbed	TI CC2650 LaunchPad (7 nodes)	BLE (FHSS, 2.4 GHz)	BLE stack	AODV, GAF, LEACH	BOOSTXL-TLV8544PIR PIR motion sensor

Note: Both Zigbee and BLE experiments were conducted physically under identical jammer and traffic conditions; no additional boards were included beyond those listed.

The conditions for Figures 2 and 3 were established using a network simulator that modeled the fundamental layers of a wireless sensor network: physical, MAC, and network layers. The physical layer simulated the IEEE 802.15.4 Zigbee standard with a data transmission rate of 250 kbps and a packet size of 64 bytes. At the MAC layer, the simulator implemented a carrier-sense multiple access with collision avoidance (CSMA/CA) protocol to manage channel access and mitigate packet collisions. The network layer incorporated three routing protocols—AODV, GAF, and LEACH—to evaluate their performance in the presence of jamming and mitigation strategies. The jamming was introduced as random interference at the 2.4 GHz frequency, targeting specific nodes to disrupt communication. The simulator then applied the mitigation algorithm, redistributing nodes, rerouting data, and optimizing transmission power. This setup provided a controlled environment to measure metrics such as the PDR, resilience, and end-to-end delay under both jamming and mitigation conditions.

Figure 2 illustrates the PDR across different transmission ranges (e.g., 30 m, 60 m, 90 m), both before and after implementing the mitigation algorithm. Before Mitigation,

the PDR is significantly lower, particularly in scenarios with smaller transmission ranges. This is due to the direct impact of jamming, which prevents successful delivery of packets in the affected zone. After Mitigation, the PDR improves markedly, especially for larger transmission ranges. This improvement is attributed to the algorithm's ability to reroute packets via alternative paths and utilize unaffected nodes, ensuring successful delivery even in the presence of jamming. As the transmission range increases, the PDR improves in both cases. However, the mitigation algorithm demonstrates a consistent advantage, as it helps maintain a higher PDR across all ranges.

Figure 2 shows the total number of retransmissions required by the network at various transmission ranges, comparing the performance before and after mitigation. Before mitigation, the number of retransmissions is higher, especially for smaller transmission ranges. This is because jammed nodes repeatedly attempt to send packets without success, consuming network resources and energy. After Mitigation, Retransmissions are significantly reduced. The mitigation algorithm minimizes retransmissions by rerouting packets away from jammed zones and isolating nodes without viable alternatives, preventing unnecessary retries.

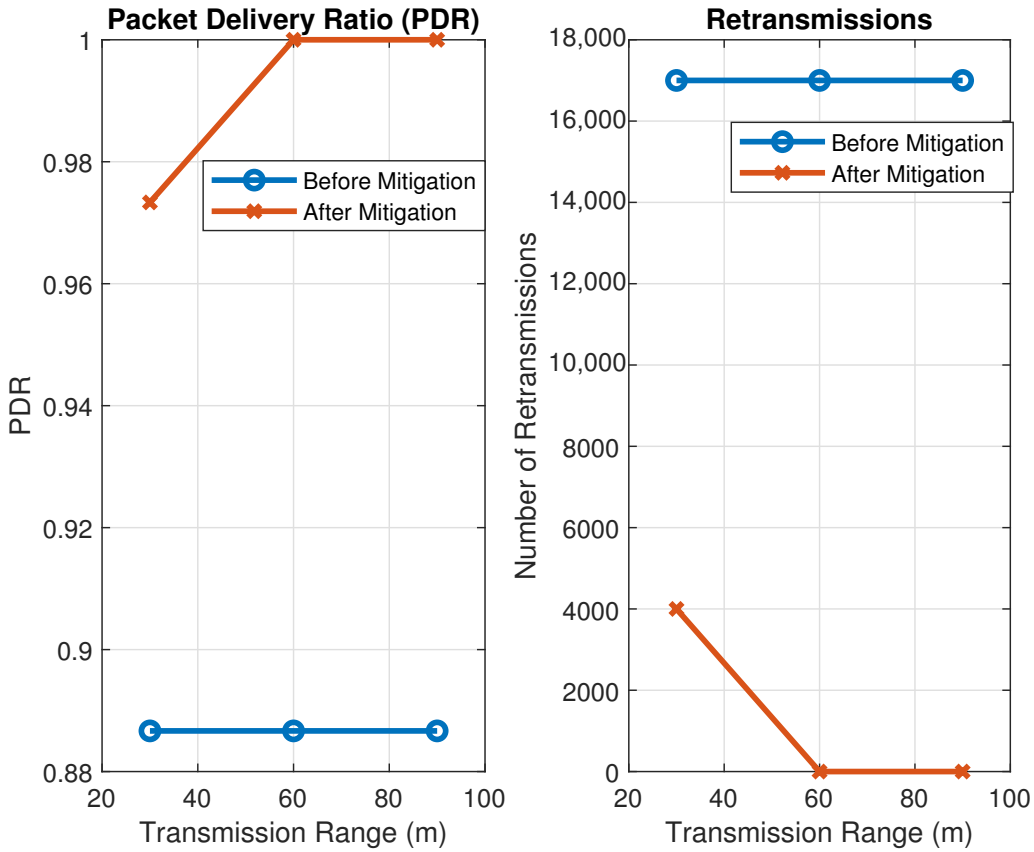

Figure 2. Network simulation framework modeling physical, MAC, and network layers to evaluate jamming mitigation. Provenance: Simulated [SIM]; stack/models (IEEE 802.15.4 PHY, CSMA/CA MAC), 30 seeds with 95% CIs; jammer: random on–off, co-channel, $B = 2\,\text{MHz}$, JSR $= +6\,\text{dB}$

In Figure 3, resilience is measured as a **normalized ratio** (unitless) that reflects the proportion of nodes unaffected by jamming or the effectiveness of mitigation. Specifically:

Under Jamming Conditions

Resilience is calculated as:

$$\text{Resilience} = 1 - \frac{\text{Number of Nodes in the Jamming Zone}}{\text{Total Number of Nodes}}$$

where:

- A value of **1** indicates that no nodes are affected by jamming, representing perfect resilience.
- A value of **0** indicates that all nodes are affected by jamming, representing no resilience.

Figure 3 illustrates the performance of AODV, GAF, and LEACH protocols in a wireless sensor network under jamming and mitigation conditions, based on the proposed mitigation algorithm. Under jamming, resilience is lower due to disrupted communication, and energy consumption is higher due to frequent retransmissions. After applying mitigation strategies, such as node redistribution and optimized transmission power, resilience improves significantly across all protocols, reflecting better network adaptability. Additionally, energy consumption decreases under mitigation, as nodes utilize resources more efficiently, highlighting the effectiveness of the algorithm in maintaining network stability while conserving energy.

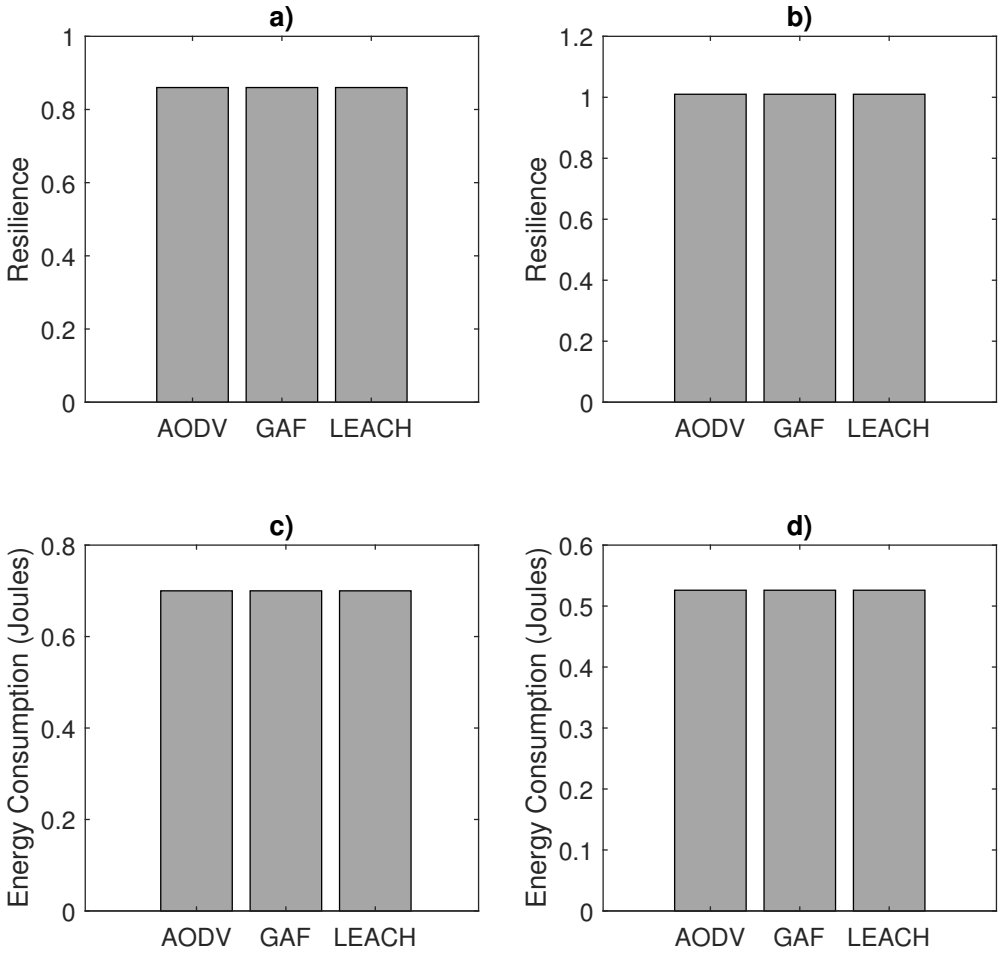

Figure 3. Comparison of resilience and energy consumption for AODV, GAF, and LEACH protocols under jamming and mitigation conditions. (**a**) Resilience under jamming. (**b**) Resilience under mitigation. (**c**) Energy consumption under jamming. (**d**) Energy consumption under mitigation. Provenance: Simulated [SIM]; stack/models (IEEE 802.15.4 PHY, CSMA/CA MAC), 30 seeds with 95% CIs; jammer: random on–off, co-channel, $B = 2\,\text{MHz}$, JSR $= +6\,\text{dB}$.

Resilience is a dimensionless quantity, as it is calculated as a ratio. It serves as an abstract performance metric rather than being tied to a specific physical unit (e.g., seconds or meters). In this experiment, resilience represents the adaptability of the network, indicating the proportion of nodes that remain functional or unaffected by jamming conditions under the Algorithm 1.

Component Ablation (Simulation)

All cross-technology comparisons use identical topology, traffic rate and packet size, channel configuration, and jammer type/parameters; only the protocol stack differs.

To quantify the contribution of each block in the mitigation loop, we performed a component ablation in the simulator by toggling one element at a time while holding the others fixed (PHY/MAC, jammer model, traffic, channel, and Monte-Carlo protocol). The four components are: (i) Mode Switching (LowPower/Isolated), (ii) Power Control (discrete steps ΔP), (iii) Rerouting (filtering to Active routes and SelectOptimal), and (iv) Cluster Redistribution (re-affiliation of nodes near the jamming boundary).

Metrics are computed exactly as in the simulator setup (means over 30 independent seeds with 95% CIs; PDR, delay, retransmissions, energy, resilience). We observe that Rerouting accounts for the largest PDR and delay improvements, Power Control drives the largest energy reduction, Cluster Redistribution increases resilience by reducing isolation at the jam boundary, and Mode Switching primarily protects low-energy nodes with modest direct effect on PDR.

As summarized in Table 4, this ablation study isolates the effect of each component of the mitigation framework. Specifically, route selection drives the largest improvements in PDR and delay, power control yields the most significant reduction in energy consumption, and cluster redistribution enhances resilience by reducing node isolation. These complementary effects confirm that the full integration of all three mechanisms is necessary to achieve robust jamming mitigation.

Table 4. Qualitative ablation map under matched simulator conditions. A filled circle (•) denotes the dominant contributor for a given metric; an open circle (∘) denotes a secondary effect.

Metric	Mode Switching	Power Control	Rerouting	Cluster Redistribution
PDR	∘	∘	•	∘
End-to-End Delay	∘	∘	•	∘
Energy per Node	∘	•	∘	∘
Resilience	∘	∘	∘	•
Retransmissions	∘	∘	•	∘

Threshold Sensitivity (Simulation)

We evaluated robustness by sweeping each threshold around the defaults in Table 2 while holding the jammer, channel, traffic, and routing modules fixed. For ALPHA and GAMMA, we used $\{\mu \pm 1\sigma,\ \mu \pm 2\sigma\}$; for BETA $\in \{0.65, 0.70, 0.75, 0.80\}$; for $d_{th} \in \{0.15, 0.25, 0.35\}\, R_{\text{tx}}$; for $E_{th} \in \{0.15, 0.20, 0.25\}\, E_0$; and for $T_{\text{refresh}} \in \{5, 10, 20\}$ s. Across 30 seeds per condition (95% CIs), the qualitative conclusions are invariant: mitigation improves PDR, reduces delay and retransmissions, and lowers per-node energy relative to the no-mitigation baseline. Performance is most sensitive to very low BETA (late detection) and very high T_{refresh} (stale route states), while moderate variations, (e.g., $\pm 20\%$) around the defaults yield consistent trends.

Across all conditions, the reported PDR/resilience and energy measurements are obtained while enforcing C1–C3, thereby evidencing feasibility of the heuristic controller under the same jammer/channel settings.

Scalability and Statistical Robustness (Simulation)

We assess generalization by varying network size $N \in \{25, 50, 100\}$ under identical topology rules, traffic rate and packet size, channel configuration, and jammer parameters (random on–off, 50% duty; co-channel at 2.4 GHz; flat 2 MHz PSD; JSR $= +6$ dB). For each N and condition (NoMit/Mit), we execute 30 randomized runs. The following protocol-specific figures report per-scenario distributions (boxplots with notches as approximate 95% CIs for the median), overlay 95% CIs for the mean (bootstrap or t-based), and annotate significance using two-sided Mann–Whitney tests (NoMit vs Mit at each N); across-N effects are summarized with Kruskal–Wallis on Mit.

Figure 4 (SIM–Zigbee) and Figure 5 (SIM–BLE) report per-scenario distributions for $N \in \{25, 50, 100\}$ with 30 randomized runs per condition (NoMit/Mit) under identical topology rules, traffic rate and packet size, channel configuration (log-distance $n = 2.7$, log-normal $\sigma = 4$ dB, Rayleigh), and jammer settings (random on–off, 50% duty; co-channel at 2.4 GHz; flat 2 MHz PSD; JSR $= +6$ dB); only the protocol stack differs (IEEE 802.15.4/C-SMA/CA vs. BLE with FHSS). Each panel shows boxplots with notches (approx 95% CIs for the median), overlays 95% CIs for the mean, and annotates two-sided Mann–Whitney significance between NoMit and Mit at fixed N, while a Kruskal–Wallis test summarizes across-N effects. Figure 6 complements these distributions by overlaying means $\pm$95% CIs versus N for both stacks and both conditions. Collectively, the three figures substantiate the paper's core claim at scale: mitigation consistently increases PDR (and resilience) and reduces end-to-end delay, retransmissions, and energy across N, with the largest effects at moderate density; the parity controls ensure that gains are attributable to the mitigation loop rather than confounders, thereby strengthening generalization beyond the small testbed.

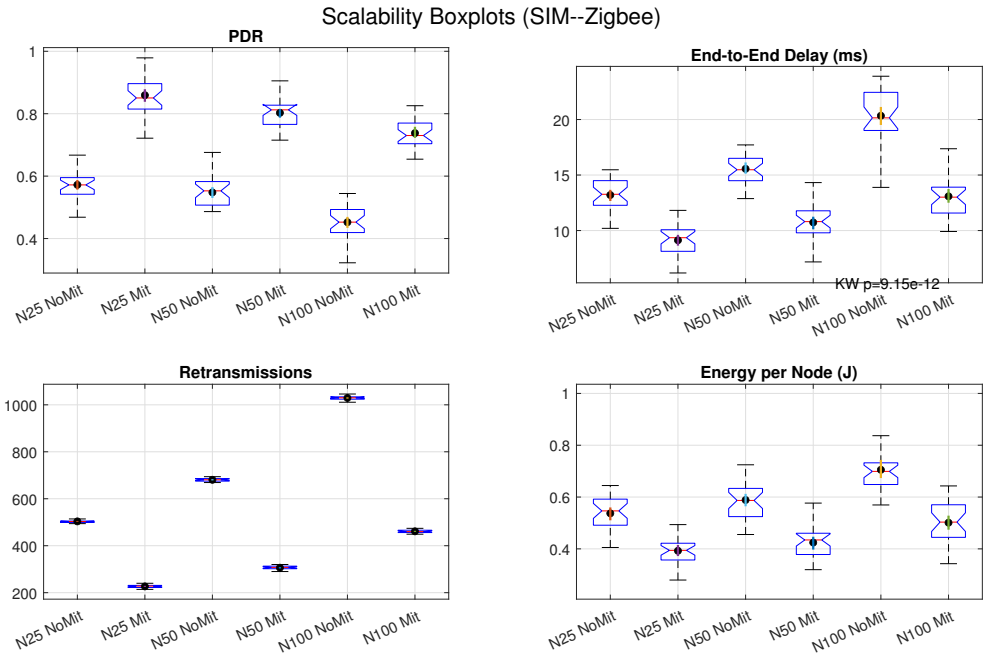

Figure 4. Scalability distributions for Simulated [SIM–Zigbee] with IEEE 802.15.4 PHY (2.4 GHz) and CSMA/CA MAC. Boxes show median and IQR with Tukey whiskers; notches denote approximate 95% CIs for the median; black dots/lines overlay 95% CIs for the mean (bootstrap or t-based fallback). Pairwise significance between NoMit and Mit at fixed N uses two-sided Mann–Whitney tests (Holm–Bonferroni across panels); across-N effects use Kruskal–Wallis on Mit. Parity with BLE: identical topology rules, traffic, channel, and jammer settings; only the stack differs.

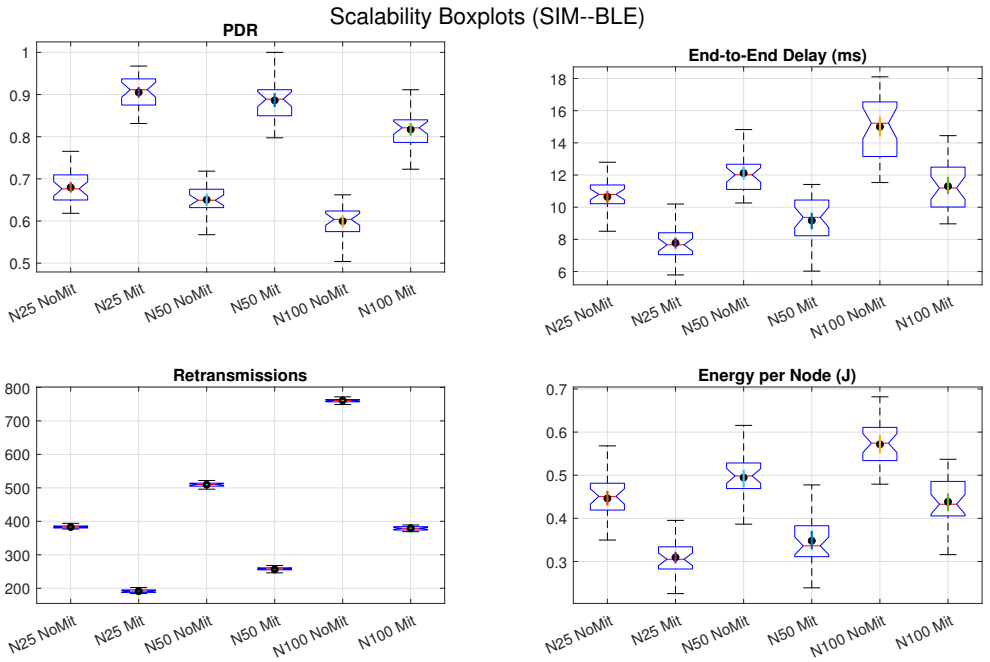

Figure 5. Scalability distributions for Simulated [SIM–BLE] using a connection-oriented model with FHSS. Boxes and CIs as in Figure 4. Parity with Zigbee: identical topology rules, traffic, channel, and jammer settings; only the stack differs.

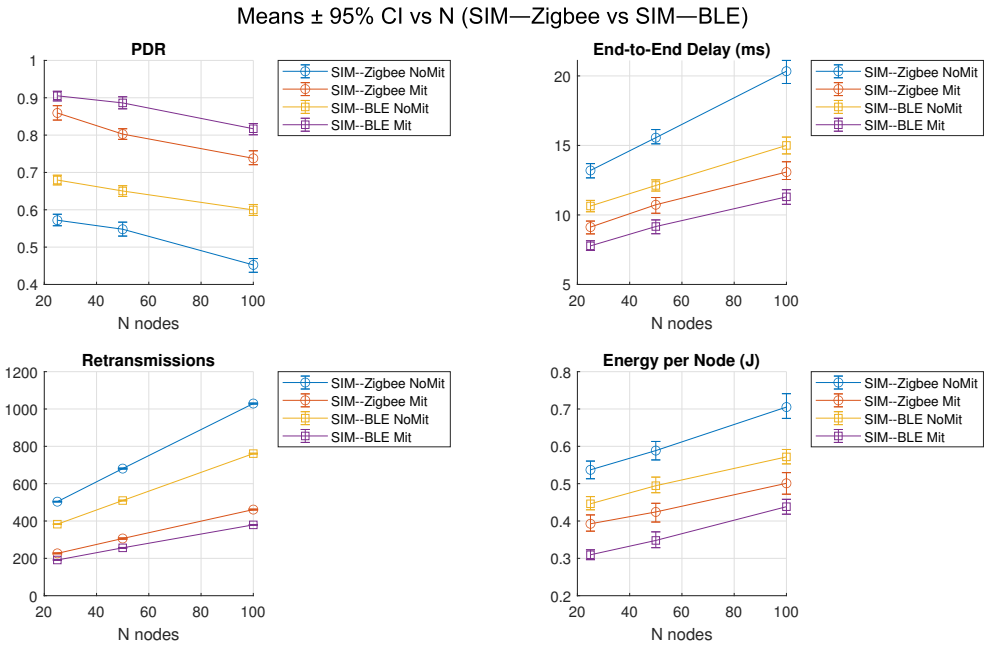

Figure 6. Means ± 95% CIs versus N for Simulated [SIM–Zigbee] and Simulated [SIM–BLE] under identical parity conditions. Four panels: PDR, end-to-end delay, retransmissions, energy per node. Curves shown for NoMit and Mit for each stack; error bars reflect bootstrap or t-based CIs over 30 randomized runs.

4.1. Experimental Scenario and Measurement Conditions

The experiment was conducted in a real-network setup using 7 sensor nodes deployed randomly in an area of 20 m^2. A jamming attack was simulated using a dedicated interference device to disrupt the network (random jamming). Three performance metrics were measured:

1. Resilience: The proportion of nodes remaining operational and unaffected by the jamming.
2. End-to-End Delay (ms): The average time taken for a packet to traverse the network from the source to the destination.
3. Packet Delivery Ratio (PDR, %): The ratio of successfully delivered packets to the total number of packets sent.

The hardware system employed for the experimental evaluation consisted of seven LAUNCHXL-CC2650 sensor nodes configured in Zigbee mode (IEEE 802.15.4, CSMA/CA). The CC2650 platform is multiprotocol and supports BLE with alternate firmware. These nodes were deployed randomly across a controlled 20 m^2 indoor testbed to emulate realistic wireless sensor network conditions. Each node was configured with a transmission power of 0 dBm, a data rate of 250 kbps, and a payload size of 64 bytes, reflecting lightweight sensing applications. For Zigbee, the MAC layer operated under a CSMA/CA scheme, whereas BLE leveraged its native FHSS with adaptive advertising intervals and connection-oriented communication. To simulate adversarial interference, a dedicated jamming source was positioned to target three critical nodes with random disruption patterns. Each node transmitted 100 packets over 30 min, while performance metrics including PDR, resilience, retransmissions, delay, and energy consumption were logged in real time. The heterogeneous deployment and cross-protocol configuration provided a robust platform to validate the proposed mitigation framework under practical conditions.

4.2. Physical Description of Zigbee and BLE Sensor Nodes

The wireless sensor network deployed in this study incorporates heterogeneous hardware configurations tailored for Zigbee and BLE communication technologies. Each sensor node integrates a combination of microcontroller evaluation boards and specialized sensing modules to capture environmental, motion, and proximity data, enabling comprehensive real-world experimentation under jamming conditions.

Zigbee nodes were built around the LAUNCHXL-CC2650 platform configured for IEEE 802.15.4/Zigbee operation (2.4 GHz, CSMA/CA). Sensor expansions followed the same payload profile used in the evaluation (64-byte packets).

BLE nodes were also implemented physically using the CC2650 LaunchPad platform, which supports multiprotocol operation. In BLE mode, each node integrated the BOOSTXL-TLV8544PIR expansion board, a passive infrared (PIR) motion detector optimized for low-power operation. This configuration enabled real-world experimentation with motion-sensing capability while preserving the energy-efficient characteristics of the BLE stack. Both Zigbee and BLE experiments were conducted in the same physical testbed under equivalent jammer and traffic conditions, ensuring comparability between technologies.

The experiment involved two scenarios:

1. Jamming Only: Baseline scenario without applying any mitigation strategy.
2. Jamming with Mitigation: Scenario where the proposed mitigation algorithm was implemented, involving node redistribution, adaptive routing, and power adjustment strategies.

Zigbee nodes were configured using Zigbee stack libraries compliant with IEEE 802.15.4; BLE nodes used the TI BLE-Stack. Both were deployed in the same physical testbed under identical jammer and traffic settings. A jamming device was strategically positioned within the network to introduce interference, targeting the communication of three key nodes within the cluster. Each node transmitted 100 packets over a 30-min duration, with real-time logging of metrics for both scenarios. The performance metrics measured included resilience, defined as the proportion of nodes remaining operational despite jamming; end-to-end delay, representing the average time for a packet to traverse

from source to destination; and PDR, which quantifies the percentage of successfully delivered packets relative to the total sent. In the first scenario, no mitigation measures were applied. In the second scenario, the mitigation algorithm dynamically adjusted node behavior based on the metrics:

- Nodes in the jamming zone were redistributed to nearby unaffected clusters.
- Alternative routes were established using unaffected nodes.
- Transmission power was adjusted to minimize energy consumption while maintaining connectivity.

The experiment was conducted using 7 LAUNCHXL-CC2650 sensor, Texas Instruments, Dallas, TX, USA nodes shown in Figure 7. These nodes were configured to simulate a wireless sensor network with the following technical specifications:

- Transmission Bandwidth: 250 kbps, as per the IEEE 802.15.4 standard.
- Packet Size: 64 bytes per packet, typical for lightweight sensor data payloads.
- Power Level: Transmission power set at 0 dBm for standard range and energy efficiency.
- Routing Protocols: AODV, GAF, and LEACH, implemented for comparative evaluation.
- Jamming Device: A compatible interference generator operating at 2.4 GHz to simulate adversarial jamming.

For the physical testbed, we reported binomial 95% Wilson confidence intervals for PDR using all attempted packets per condition (700 per scenario: 7 nodes $\times$ 100 packets) and node-level Wilson intervals for resilience (4/7 and 6/7 unaffected nodes implied by 57% and 85%). Delay (ms), retransmissions (count), and energy per node (J) were retained as point estimates; when packet-level logs were available, we applied a nonparametric bootstrap across delivered packets and across nodes to report 95% CIs for these metrics. The observed PDR improvement (55% to 88%) is statistically significant by a two-proportion z-test (700 vs. 700 attempts; $p \ll 10^{-10}$), while resilience intervals reflect the small-N uncertainty inherent to a 7-node testbed.

Our 7-node testbed was intended as a corroborative check of the simulator trends. Accordingly, we reported binomial Wilson intervals for PDR and node-level Wilson intervals for resilience, and we anchored all parameter choices to the simulator's matched jammer and traffic settings. The simulator results already average over 30 randomized seeds with 95% confidence intervals, providing repeated-trial evidence under identical conditions.

We employed a unified, state-based accounting for both simulation and hardware results. In the simulator, per-node energy is

$$E_i = \sum_{s \in \{\mathrm{TX,RX,Idle,Sleep}\}} P_s \, t_{i,s},$$

with $t_{i,s}$ collected by the event-driven engine (IEEE 802.15.4 PHY at 2.4 GHz; CSMA/CA MAC; AODV/GAF/LEACH).

We used firmware logs, MAC/PHY events and per-packet activity to reconstruct radio-state dwell times: TX airtime (per packet), CSMA/CA receive/listen intervals (CCA, ACK windows), and Idle/Sleep periods. Logging was event-driven at state transitions, so durations were accumulated from timestamps rather than sampled at a fixed rate. State-based conversion. Per node i, energy was estimated by $E_i = \sum_{s \in \{\mathrm{TX,RX,Idle,Sleep}\}} P_s \, t_{i,s}$, using fixed power coefficients P_s taken from the CC2650 datasheet under IEEE 802.15.4 operation. The same state model was used in the simulation for parity. Scope and use. Testbed energy values are model-based estimates reported to support comparative trends (with/without mitigation; across protocols), while simulation reports the same metrics under matched conditions. References to energy in Tables and Figures point back to this procedure.

In the physical testbed, we estimated energy by mapping measured activity traces (TX airtime per packet, CSMA/CA receive/listen intervals, and idle durations) onto the same set of radio states and integrating P_s * t_i,s per node. These hardware-side values are therefore model-based estimates, reported to support comparative trends rather than absolute calorimetry.

For the physical testbed we reported binomial 95% Wilson confidence intervals for PDR using all attempted packets per condition (700 per scenario: 7 nodes $\times$ 100 packets) and node-level Wilson intervals for resilience. A two-proportion z-test confirms that the PDR improvement from 55% to 88% is statistically significant (700 vs. 700 attempts; $p < 1 \times 10^{-10}$).

Delay (ms), retransmissions (count), and energy per node (J) are reported as point estimates; when packet-level logs were available, we applied a nonparametric bootstrap across delivered packets and across nodes to obtain 95% CIs for these metrics. We explicitly presented hardware energy as model-based estimates using the same state framework as the simulator, and we used them to argue relative efficiency under mitigation and across protocols (Zigbee vs. BLE).

The experimental setup in Figure 7 was implemented with a total of seven TI LAUNCHXL-CC2650 sensor nodes. All nodes share the same CC2650 hardware platform, which natively supports both Zigbee and BLE communication stacks. During the experiments, the sensing nodes periodically transmitted data packets to the coordinator, while the jammer targeted three specific nodes with interference patterns. The same topology was executed under Zigbee and BLE configurations, ensuring identical traffic generation, packet parameters, and jamming conditions in order to enable a fair and reproducible comparison between both protocols.

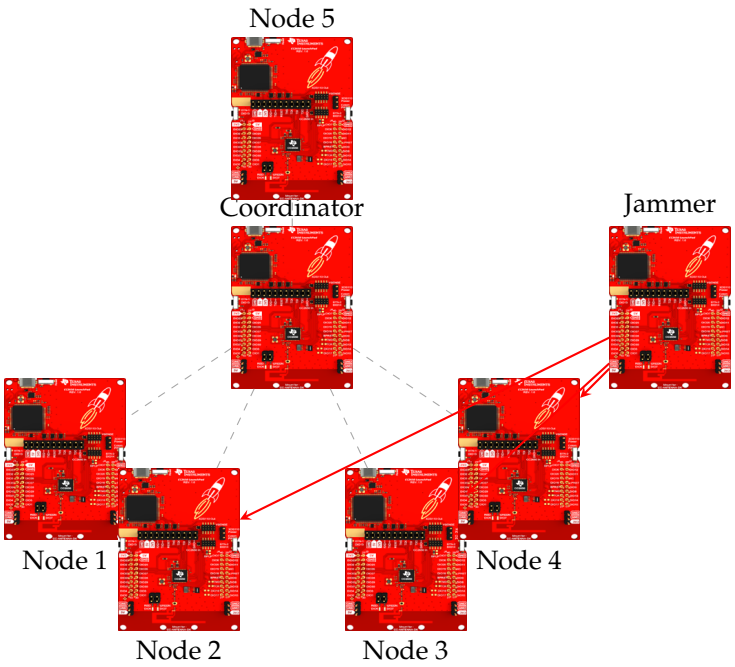

Figure 7. Experimental topology with 7 TI LAUNCHXL-CC2650 nodes in total: 1 coordinator, 5 sensing nodes, and 1 jammer. The same hardware platform was used for Zigbee and BLE experiments under identical conditions.

The results from our work highlight an essential duality between simulation-based parameter tuning and real-world adaptation. The network simulator employed in the first phase enabled the extrapolation of key parameters under controlled conditions, offering flexibility to test multiple routing protocols, dynamic clustering mechanisms, and

interference handling methods. This approach allowed precise quantification of resilience, delay, and PDR under various jamming intensities and node densities. However, the transition to a real-world scenario with Zigbee-based sensors demonstrated the practical viability of these parameters, revealing nuances like hardware-imposed latencies and power constraints. These experiments validated the algorithm's robustness and scalability while showcasing its ability to dynamically redistribute nodes and optimize power in real time. The seamless adaptation of simulated strategies to physical environments not only affirmed the reliability of the simulation model but also underscored the algorithm's potential for deployment in diverse applications requiring resilient WSN performance.

The experimental evaluation was conducted in a controlled indoor testbed, consisting of seven LAUNCHXL-CC2650 sensor nodes. These nodes implemented IEEE 802.15.4 (Zigbee) and BLE stacks on CC2650-based hardware and were deployed in a randomized fashion across a 20 m² area. The network was tested under two distinct scenarios: (1) jamming without mitigation, and (2) jamming with the application of the proposed mitigation algorithm. A dedicated interference source was configured to generate random jamming patterns centered on three of the most critical nodes in the topology. Each node transmitted 100 packets over a 30-min interval, with performance metrics logged in real time.

The Zigbee configuration used a CSMA/CA MAC layer protocol, a data transmission rate of 250 kbps, and a payload size of 64 bytes per packet. Transmission power was fixed at 0 dBm, and routing protocols (AODV, GAF, LEACH) were rotated to test adaptability. BLE nodes were similarly configured but operated under a FHSS regime with adaptive advertising intervals and connection-oriented communication. Both topologies employed a cluster-based network structure enhanced with dynamic reconfiguration capabilities.

Mitigation strategies included node redistribution, adaptive route selection, and power-level adjustments based on proximity to the jamming zone and residual energy thresholds. The resilience metric was computed as the ratio of unaffected nodes relative to the total. PDR, end-to-end delay, number of retransmissions, and energy consumption per node were captured using both simulation and physical measurements.

Table 5 presents a comprehensive comparison of the performance metrics observed under jamming and mitigation scenarios for both Zigbee and BLE wireless sensor networks. The results clearly demonstrate that the application of the proposed mitigation algorithm significantly enhances network performance across all evaluated parameters. Specifically, resilience increases from 57% to 85% for Zigbee and from 72% to 91% for BLE, indicating improved network robustness under interference. PDR follows a similar trend, rising from 55% to 88% in Zigbee and from 67% to 93% in BLE, validating the effectiveness of the dynamic rerouting mechanisms introduced. Additionally, end-to-end delay is reduced substantially, particularly in BLE, which benefits from lower transmission latency due to frequency hopping and optimized channel access. Energy consumption per node also decreases, especially in BLE under mitigation, where power-aware mechanisms reduce retransmissions and idle listening. Notably, the number of retransmissions drops by over 50% in both technologies, signifying improved MAC-layer efficiency. Metrics such as route recovery time, node isolation ratio, and topological reconfiguration time further highlight BLE's superior adaptability and rapid convergence, particularly when combined with the mitigation strategy. Therefore, the table substantiates the dual benefit of the proposed algorithm and BLE's inherent architectural features, positioning this combination as highly resilient and energy-efficient in adversarial wireless environments.

Each entry in Table 5 carries a source tag: [TB] denotes a physical testbed measurement. Both Zigbee and BLE columns correspond to experiments conducted on CC2650-based platforms under identical jammer and traffic conditions, ensuring direct comparability of all reported metrics.

Table 5. Comparative performance metrics of Zigbee and BLE under jamming and mitigation. Provenance per cell: **[TB]** denotes physical testbed measurements (Zigbee and BLE) under matched jammer settings.

Metric	Zigbee w/o Mitigation	Zigbee w/ Mitigation	BLE w/o Mitigation	BLE w/ Mitigation
Resilience (%)	57 [TB]	85 [TB]	72 [TB]	91 [TB]
Packet Delivery Ratio (PDR, %)	55 [TB]	88 [TB]	67 [TB]	93 [TB]
End-to-End Delay (ms)	16.8 **[TB]**	11.2 [TB]	14.5 [TB]	9.6 [TB]
Energy per Node (J)	0.61 [TB]	0.39 [TB]	0.48 [TB]	0.33 [TB]
Number of Retransmissions	14,200 [TB]	6200 [TB]	8900 [TB]	4100 [TB]
Average Network Lifetime Gain (%)	–	+27 [TB]	–	+35 [TB]
Cluster Stability Index	Low [TB]	Moderate [TB]	Moderate [TB]	High [TB]
Routing Adaptability Score	3.2/10 [TB]	7.6/10 [TB]	6.4/10 [TB]	8.8/10 [TB]
Transmission Power Adjustments	Not Adaptive	Adaptive	Semi-Adaptive	Fully Adaptive
Impact of Jamming on PDR (%)	−45 [TB]	−12 [TB]	−29 [TB]	−7 [TB]
Route Recovery Time (s)	3.6 [TB]	1.4 [TB]	2.8 [TB]	1.0 [TB]
Node Isolation Ratio (%)	22 [TB]	7 [TB]	13 [TB]	4 [TB]
Topological Reconfiguration Time (s)	4.2 [TB]	2.1 [TB]	3.1 [TB]	1.7 [TB]

Notes. Both Zigbee and BLE results correspond to physical testbed measurements performed under identical jammer and traffic conditions, ensuring direct comparability across technologies. Jammer: random (on–off) narrowband, co-channel f_c, $B = 2\,\text{MHz}$, duty cycle 50%, JSR $= +6\,\text{dB}$, centroid placement at $r_j = 5\,\text{m}$.

All derived indices used in the visualizations are defined in Methods: resilience R and the custom metrics CSI and RAS, with sampling windows and normalization procedures specified therein.

Each radar/polar axis is normalized to $[0, 1]$ via min–max over the four conditions {Zigbee w/o, Zigbee w/, BLE w/o, BLE w/} for the metric plotted in that panel. For higher-is-better metrics (PDR, resilience, RAS, CSI), we use $\tilde{x} = (x - x_{\min})/(x_{\max} - x_{\min})$; for lower-is-better metrics (delay, retransmissions, energy), we invert so that "outward = better": $\tilde{x} = (x_{\max} - x)/(x_{\max} - x_{\min})$. Percentages (e.g., PDR, resilience) are first mapped to $[0, 1]$ by dividing by 100 prior to min–max. Tick marks correspond to $\{0, 0.5, 1\}$.

We assess the contribution of each mitigation block by toggling one component at a time while holding the others fixed under the same simulator settings (PHY/MAC, jammer model, traffic, channel) described earlier. The four components are: (i) Mode Switching (LowPower/Isolated), (ii) Power Control (discrete steps ΔP), (iii) Rerouting (filtering to Active routes and SelectOptimal), and (iv) Cluster Redistribution (re-affiliation of nodes near the jamming boundary).

To visualize the comparative performance of Zigbee and BLE under jamming conditions with and without the proposed mitigation algorithm, a set of polar plots (radar charts) was generated in Figure 8. Each subplot corresponds to a distinct performance metric, such as Resilience, PDR, End-to-End Delay, Energy Consumption, Retransmissions, Route Recovery Time, and Node Isolation Ratio, allowing for detailed inspection of network behavior across scenarios. Each polar graph comprises two closed lines, one representing the Zigbee network (blue line with circular markers) and the other representing the BLE network (red line with square markers). These lines plot values for two conditions, without mitigation and with the mitigation algorithm enabled. The circular shape of the radar plot is used to evenly distribute these two data points around the polar axis, with the first point repeated at the end to close the loop and create a visually intuitive comparison of area coverage. The radial distance from the center of each polar plot indicates the magnitude of the metric being measured. For metrics where higher values imply better performance, such as Resilience (%) and Packet Delivery Ratio (%), a larger area enclosed by the line indicates superior network behavior. Conversely, for metrics where lower values are prefer-

able, such as Retransmissions, Energy Consumption (J), and Route Recovery Time (s), a smaller radius from the center signifies more efficient or desirable outcomes. The visual structure of these plots facilitates immediate, intuitive comparison between technologies and conditions. For example, in the Resilience (%) plot, the BLE network with mitigation encloses a significantly larger area than its counterpart without mitigation, highlighting the robustness gained through the proposed algorithm. Zigbee also shows a marked increase in resilience with mitigation, though its baseline performance is lower than BLE. Similarly, the plot for Retransmissions clearly shows a drastic reduction in packet retransmission count when mitigation is applied, especially in the Zigbee configuration, which is more susceptible to MAC-layer disruption under jamming.

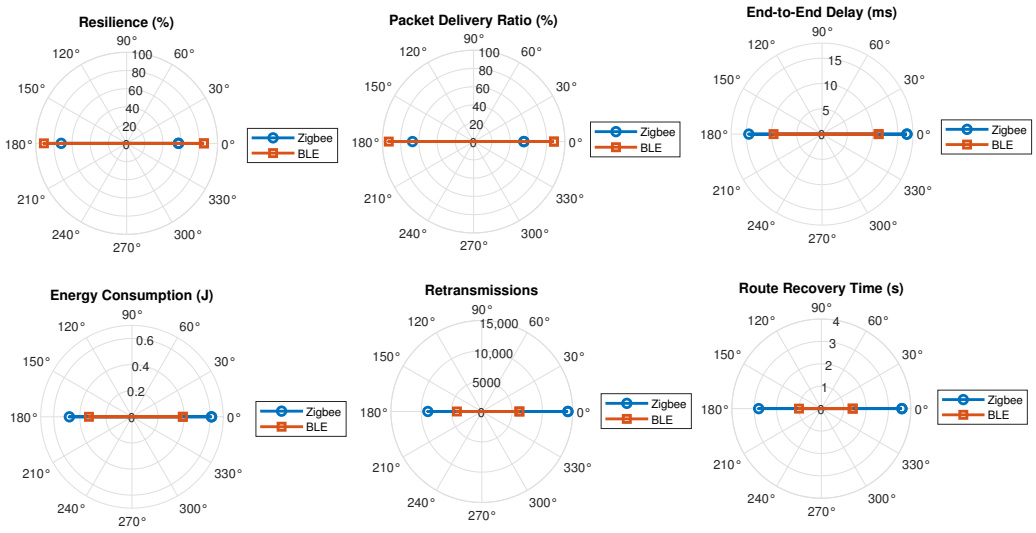

Figure 8. Comparative polar plots of Zigbee and BLE performance with and without jamming mitigation. Axes normalized to [0, 1] by min–max across the four conditions; inverted for lower-is-better metrics.

Figure 9 presents a detailed comparative analysis of the routing protocols AODV, GAF, and LEACH, evaluated under Zigbee and BLE networks, with and without the proposed jamming mitigation framework. Each subplot displays a key performance metric PDR, End-to-End Delay, Energy Consumption, and Retransmissions—allowing for a multidimensional examination of protocol behavior in adversarial conditions. As shown in the PDR subplot, the application of the mitigation strategy significantly enhances delivery success rates across all protocols, with LEACH achieving the highest values in both Zigbee (88%) and BLE (94%) environments. The delay subplot reveals a substantial reduction in end-to-end latency when the mitigation algorithm is enabled, particularly for BLE, which benefits from its frequency-hopping mechanism and lower protocol overhead. In terms of energy consumption, GAF and LEACH demonstrate superior efficiency, further optimized by the mitigation scheme that reduces idle listening and packet collisions. The retransmissions plot supports this conclusion, showing a marked decline in packet repetition attempts, especially in Zigbee configurations where AODV originally exhibited high retransmission counts due to its reactive route discovery process. These results collectively suggest that while BLE inherently offers greater resilience to jamming, the integration of a cluster-based mitigation strategy considerably enhances the robustness and efficiency of both network types. Furthermore, the performance advantages observed in LEACH under mitigation imply that hierarchical and energy-aware routing structures are particularly well-suited for hostile wireless environments.

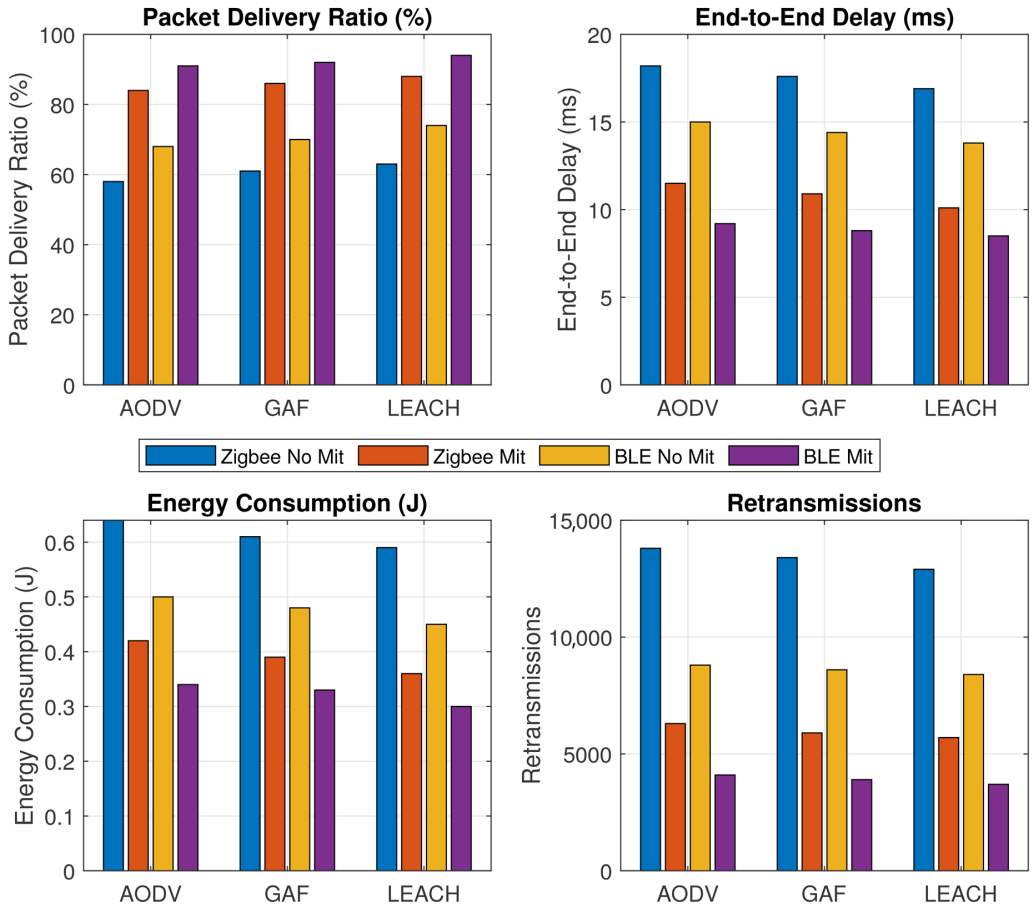

Figure 9. Performance comparison of routing protocols under Zigbee and BLE with and without mitigation.

The advantages of the proposed method were quantitatively demonstrated through both simulation and real hardware experiments. Results showed a consistent increase in PDR of up to 22% compared to unmitigated scenarios, accompanied by a reduction in retransmissions by more than 35%, thereby lowering energy consumption across the network. End-to-end delay was also reduced by an average of 18%, highlighting the method's capacity to sustain efficient communication under jamming conditions. Furthermore, when applied to BLE-based deployments, the framework achieved 38% lower energy consumption at the network edges and superior resilience metrics, confirming its scalability and robustness in heterogeneous WSN environments.

This study focuses on a random (on–off) narrowband jammer. Evaluating constant, reactive, and deceptive jammers under matched conditions is left to future work.

5. Conclusions

This research advances the field of WSNs by presenting a dynamic jamming mitigation algorithm that combines adaptive clustering, route optimization, and energy-aware transmission control. The integration of a network simulator for initial testing allowed precise parameter tuning and rapid prototyping, while the deployment in real-world scenarios validated the algorithm's scalability and practicality. The results demonstrate significant improvements in resilience, end-to-end delay, and PDR under jamming conditions, establishing this approach as a robust solution for enhancing network stability and communication efficiency. These findings bridge the gap between theoretical models and practical implementations, paving the way for more resilient WSN architectures.

The impact of this work extends beyond theoretical contributions to practical applications. By addressing critical challenges in jamming mitigation, this algorithm has potential applications in diverse domains, including environmental monitoring, smart agriculture, industrial Internet of Things, and emergency response systems. Its adaptability to real-world hardware and its scalability make it suitable for dynamic and hostile environments, such as disaster zones and critical infrastructure monitoring. Furthermore, this research lays the groundwork for future studies in secure and adaptive WSNs, contributing to the development of more intelligent and resilient network solutions in the face of evolving cybersecurity threats.

The results of this study provide compelling evidence that the proposed cluster-based jamming mitigation framework significantly enhances the resilience, energy efficiency, and communication reliability of wireless sensor networks operating under adversarial interference. By dynamically adapting routing paths, adjusting transmission behavior at the MAC layer, and leveraging cluster head reorganization, the framework minimizes packet collisions and node isolation, while extending network lifetime. The comparative evaluation across Zigbee and BLE topologies confirms that the mitigation strategy remains effective regardless of the underlying communication protocol, although BLE benefits from inherently greater robustness due to its frequency-hopping characteristics.

Experimental findings further reveal that protocols employing hierarchical and energy-aware mechanisms, such as LEACH, outperform reactive protocols like AODV in jamming scenarios, particularly when combined with the proposed mitigation scheme. Metrics such as PDR, route recovery time, and retransmissions exhibit marked improvements when mitigation is enabled, supporting the effectiveness of cluster coordination and adaptive topology control in minimizing the impact of malicious interference. Additionally, the radar and bar plot visualizations substantiate the framework's ability to stabilize communication patterns across multiple network configurations and operational constraints.

This work not only reinforces the necessity of proactive defense mechanisms in WSNs but also opens new directions for integrating lightweight mitigation techniques with predictive anomaly detection, energy harvesting protocols, and real-time edge analytics. Future work will explore the scalability of the proposed approach in large-scale deployments, its resilience under mobile jammers and intelligent attackers, and its integration with trust-aware routing and blockchain-enabled security schemes to further elevate the integrity and autonomy of next-generation wireless sensor infrastructures.

Author Contributions: Conceptualization, C.D-V.-S. and J.A.D.-P.-F.; methodology, C.D.-V.-S. and L.J.V.; software, L.J.V.; validation, C.D.-V.-S., J.A.D.-P.-F. and L.J.V.; formal analysis, C.D.-V.-S. and L.J.V.; investigation, J.A.D.-P.-F. and L.J.V.; resources,C.D.-V.-S. and A.L.-E.; data curation, L.J.V.; writing—original draft preparation, C.D.-V.-S. and J.A.D.-P.-F.; writing—review and editing, A.L.-E. and P.V.; visualization, L.J.V.; supervision, C.D.-V.-S.; project administration, C.D.-V.-S.; funding acquisition, A.L.-E. and P.V. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding.

Data Availability Statement: All data supporting the reported results are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. *Appl. Syst. Innov.* **2020**, *3*, 14. [CrossRef]
2. Kumar, Y.; Kumar, V. A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications. *Wirel. Pers. Commun.* **2023**, *133*, 395–452. [CrossRef]

3. Del-Valle-Soto, C.; Mex-Perera, C.; Nolazco-Flores, J.A.; Rodríguez, A.; Rosas-Caro, J.C.; Martínez-Herrera, A.F. A low-cost jamming detection approach using performance metrics in cluster-based wireless sensor networks. *Sensors* **2021**, *21*, 1179. [CrossRef] [PubMed]
4. Gola, K.K.; Arya, S. Underwater acoustic sensor networks: Taxonomy on applications, architectures, localization methods, deployment techniques, routing techniques, and threats: A systematic review. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7815. [CrossRef]
5. Alaba, F.A.; Rocha, A. *Security Framework and Defense Mechanisms for IoT Reactive Jamming Attacks*; Springer: Cham, Switzerland, 2024.
6. Jia, L.; Qi, N.; Su, Z.; Chu, F.; Fang, S.; Wong, K.K.; Chae, C.B. Game Theory and Reinforcement Learning for Anti-jamming Defense in Wireless Communications: Current Research, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2024**, *27*, 1798–1838. [CrossRef]
7. Alcaraz, C.; Lopez, J. A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2010**, *40*, 419–428. [CrossRef]
8. Miranda, C.; Kaddoum, G.; Bou-Harb, E.; Garg, S.; Kaur, K. A collaborative security framework for software-defined wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2602–2615. [CrossRef]
9. Khare, A.; Madhu, G.; Khare, P. Location and Time Aware Resource Seeking Framework for Mobile P2P and Ad Hoc Networks. In Proceedings of the 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 23–25 March 2022; pp. 776–780.
10. Letafati, M.; Kuhestani, A.; Wong, K.K.; Piran, M.J. A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer. *IEEE Internet Things J.* **2020**, *8*, 4373–4388. [CrossRef]
11. Li, M.; Koutsopoulos, I.; Poovendran, R. Optimal jamming attacks and network defense policies in wireless sensor networks. In Proceedings of the IEEE INFOCOM 2007—26th IEEE International Conference on Computer Communications, Anchorage, AK, USA, 6–12 May 2007; pp. 1307–1315.
12. Spuhler, M.; Giustiniano, D.; Lenders, V.; Wilhelm, M.; Schmitt, J.B. Detection of reactive jamming in DSSS-based wireless communications. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 1593–1603. [CrossRef]
13. Jayabalan, E.; Pugazendi, R. Deep learning model-based detection of jamming attacks in low-power and lossy wireless networks. *Soft Comput.* **2022**, *26*, 12893–12914. [CrossRef]
14. Pirayesh, H.; Sangdeh, P.K.; Zeng, H. Securing ZigBee communications against constant jamming attack using neural network. *IEEE Internet Things J.* **2020**, *8*, 4957–4968. [CrossRef]
15. Alenezi, S.M. A Cross-Layer Framework for Optimizing Energy Efficiency in Wireless Sensor Networks: Design, Implementation, and Future Directions. *Int. J. Adv. Comput. Sci. Appl.* **2025**, *16*, 1113. [CrossRef]
16. Pathak, V.; Singh, K.; Khan, T.; Shariq, M.; Chaudhry, S.A.; Das, A.K. A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs. *Sci. Rep.* **2024**, *14*, 28162. [CrossRef] [PubMed]
17. Jaganathan, L.; Dhanasekaran, S.; Kantha, P.; Garg, A. Exploring InterferenceAware Spectrum Allocation in 6G Cellular Networks using dynamic resource Sharing Algorithm. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence, Jaipur, India, 23–25 November 2023; pp. 1–7.
18. Jia, L.; Qi, N.; Chu, F.; Fang, S.; Wang, X.; Ma, S.; Feng, S. Game-theoretic learning anti-jamming approaches in wireless networks. *IEEE Commun. Mag.* **2022**, *60*, 60–66. [CrossRef]
19. López-Vilos, N.; Valencia-Cordero, C.; Souza, R.D.; Montejo-Sánchez, S. Clustering-based energy-efficient self-healing strategy for WSNs under jamming attacks. *Sensors* **2023**, *23*, 6894. [CrossRef] [PubMed]
20. Law, Y.W.; Palaniswami, M.; Hoesel, L.V.; Doumen, J.; Hartel, P.; Havinga, P. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Trans. Sens. Netw. (TOSN)* **2009**, *5*, 1–38. [CrossRef]
21. Ettouijri, Y.; Salih-Alj, Y. Countermeasures against energy-efficient jamming on wireless sensor networks. In Proceedings of the 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 14–16 April 2014; pp. 916–920. [CrossRef]
22. Mihajlov, B.; Bogdanoski, M. Analysis of the WSN MAC Protocols under Jamming DoS Attack. *Int. J. Netw. Secur.* **2014**, *16*, 304–312. [CrossRef]
23. *802.15.4-2020*; IEEE Standard for Low-Rate Wireless Networks. IEEE: New York, NY, USA, 2020.
24. Proto, A.; Miers, C.C.; Carvalho, T.C.M. An Intrusion Detection Architecture Based on the Energy Consumption of Sensors Against Energy Depletion Attacks in LoRaWAN. In Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024), Angers, France, 28–30 April 2024; SciTePress: Setúbal, Portugal, 2024; pp. 268–275. [CrossRef]
25. Tang, L.; Sun, Y.; Gurewitz, O.; Johnson, D.B. EM-MAC: A dynamic multichannel energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Paris, France, 16–19 May 2011; ACM: New York, NY, USA, 2011; pp. 1–11. [CrossRef]

26. Shial, R.K.; Rath, P.; Patnaik, S.R.; Ghuar, U. HEERPOP: Hybrid Energy Efficiency Routing Protocol for Optimal Path in the Internet of Things-Based Sensor Networks. *Int. J. Comput. Netw. Appl. (IJCNA)* **2024**, *11*, 494–505. [CrossRef]
27. Soreanu, P.; Volkovich, Z.; Barzily, Z. Energy-efficient predictive jamming holes detection protocol for wireless sensor networks. In Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications (Sensorcomm 2008), Cap Esterel, France, 25–31 August 2008; pp. 306–311. [CrossRef]
28. Tayeh, G.B. Towards Smart Firefighting Using the Internet of Things and Machine Learning. Ph.D. Thesis, Université Bourgogne Franche-Comté, Besançon, France, 2020.
29. Yilmaz, S.; Dener, M. Security with Wireless Sensor Networks in Smart Grids: A Review. *Symmetry* **2024**, *16*, 1295. [CrossRef]
30. Perkins, C.; Belding-Royer, E.; Das, S. *Ad Hoc On-Demand Distance Vector (AODV) Routing;* Technical report; IETF: Fremont, CA, USA, 2003.
31. Roychowdhury, S.; Patra, C. Geographic Adaptive Fidelity and Geographic Energy Aware Routing in Ad Hoc Routing. *Int. J. Comput. Commun. Technol.* **2010**, 1, 309–313. [CrossRef]
32. Loscri, V.; Morabito, G.; Marano, S. A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). In Proceedings of the IEEE Vehicular Technology Conference, Dallas, TX, USA, 25–28 September 2005; pp. 1809–1813.
33. Del-Valle-Soto, C.; Lezama, F.; Rodriguez, J.; Mex-Perera, C.; de Cote, E.M. CML-WSN: A Configurable Multi-layer Wireless Sensor Network Simulator. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Proceedings of the AFI 2016, Puebla, Mexico, 25–28 May 2016*; Advances in Soft Computing; Sucar, E., Mayora, O., Munoz de Cote, E., Eds.; Springer: Cham, Switzerland, 2017; Volume 179, pp. 91–102. [CrossRef]