Peer-to-Peer Networking and Applications (2026) 19:97
https://doi.org/10.1007/s12083-026-02251-5

RESEARCH

Hybrid BLE–LoRa architectures for energy-efficient and resilient wireless sensor networks: Experimental validation and adaptive clustering strategies

Carolina Del-Valle-Soto[1] · Ramon A. Briseño[1] · Leonardo J. Valdivia[1] · José Varela-Aldás[2] · Paolo Visconti[3]

Received: 9 June 2025 / Accepted: 21 May 2026
© The Author(s) 2026

Abstract

Wireless Sensor Networks are increasingly deployed in mission-critical scenarios where resilience and energy efficiency are paramount. This paper presents a hybrid architecture combining Bluetooth Low Energy (BLE) and Long Range (LoRa) technologies to enhance both robustness and energy-aware performance in adversarial environments characterized by reactive jamming attacks. A comprehensive experimental testbed was developed, integrating BLE and LoRa nodes, a dual-protocol gateway, and a reactive jammer emulator. We introduce an adaptive clustering algorithm that performs energy-aware role assignment and jamming mitigation based on signal anomaly detection and multi-metric routing. To validate its effectiveness, we conducted an extensive time-series analysis on energy consumption, retransmission rates, and signal resilience under both mitigated and non-mitigated conditions across BLE-only, LoRa-only, and hybrid BLE-LoRa networks. The results show protocol-dependent performance trade-offs under the proposed mitigation algorithm. While LoRa-only and hybrid BLE–LoRa networks exhibit consistent reductions in energy consumption, retransmissions, and variability, the BLE-only configuration demonstrates improved resilience at the cost of a moderate increase in energy usage and retransmission activity due to clustering and control overhead. Notably, the BLE-LoRa architecture balances delivery assurance and energy efficiency while maintaining communication even under interference. Furthermore, we provide statistical modeling and hypothesis testing confirming the mitigation algorithm's significant impact. These findings offer a critical empirical contribution to the design of resilient and energy-aware heterogeneous WSNs and demonstrate the viability of real-time adaptive mitigation strategies for emerging smart environments.

Keywords Wireless sensor networks · BLE · LoRa · Reactive jamming · Clustering · Energy efficiency · Resilience · Time-series analysis

Ramon A. Briseño, and Leonardo J. Valdivia contributed equally to this work.

✉ José Varela-Aldás
josevarela@uti.edu.ec

Carolina Del-Valle-Soto
cvalle@up.edu.mx

Ramon A. Briseño
rbriseno@up.edu.mx

Leonardo J. Valdivia
lvaldivia@up.edu.mx

Paolo Visconti
paolo.visconti@unisalento.it

[1] Facultad de Ingeniería, Universidad Panamericana, Álvaro del Portillo 49, Zapopan 45010, Jalisco, México

[2] Centro de Investigación MIST, Facultad de Ingenierías, Universidad Tecnológica Indoamérica, Ambato 180103, Ecuador

[3] Department of Innovation Engineering, University of Salento, Lecce 73100, Italy

Published online: 03 June 2026

1 Introduction

Wireless Sensor Networks (WSNs) have become a critical component of modern cyber-physical systems, enabling applications ranging from environmental monitoring and industrial automation to healthcare and smart cities. These networks rely on the seamless cooperation of low-power sensor nodes to collect, process, and transmit data over wireless links [1]. Among the numerous communication technologies employed in WSNs, Bluetooth Low Energy (BLE) and Long Range (LoRa) stand out due to their energy efficiency and wide coverage, respectively. BLE offers low-latency communication suitable for short-range, high-throughput applications, while LoRa provides extended range with low power consumption, making it ideal for sparse deployments and remote monitoring. In recent years, heterogeneous architectures that integrate BLE and LoRa have emerged to leverage the strengths of both technologies, enhancing the adaptability and performance of WSNs in dynamic environments [2].

However, the increasing deployment of WSNs in mission-critical applications has raised significant concerns about their security and resilience, particularly against jamming attacks. Jamming is a form of Denial-of-Service (DoS) attack where an adversary deliberately emits radio signals to interfere with the communication between nodes, thereby degrading network performance or rendering it completely inoperable. One of the most challenging types of jamming is reactive jamming, in which the attacker monitors the wireless channel and selectively transmits interference signals only when legitimate communication is detected. This makes detection and mitigation more difficult, as the attack is intermittent and synchronized with real network activity.

This study provides a comparative analysis of the impact of reactive jamming on three types of WSN architectures: (i) a BLE-only network, (ii) a LoRa-only network, and (iii) a hybrid BLE-LoRa network. Each of these configurations is subjected to controlled reactive jamming scenarios in order to assess their susceptibility to interference. Subsequently, a cluster-based mitigation algorithm is applied to evaluate its effectiveness in maintaining network functionality under sustained jamming conditions. The clustering algorithm organizes nodes into groups based on proximity, traffic patterns, or energy metrics, and designates cluster heads to coordinate communication. This hierarchical approach reduces channel contention, minimizes retransmissions, and introduces redundancy and alternate paths, which are essential for improving resilience against targeted attacks.

The main contribution of this paper is twofold. First, it presents a systematic evaluation of how BLE, LoRa, and heterogeneous BLE-LoRa networks behave under reactive jamming, highlighting their strengths and limitations. Second, it demonstrates the potential of a cluster-based mitigation strategy to enhance network robustness by maintaining communication performance despite the presence of ongoing attacks. Experimental results are analyzed in terms of packet delivery ratio, latency, retransmission rate, and energy consumption, providing insights into the trade-offs between security, reliability, and efficiency in heterogeneous WSNs.

In this study, the term “intelligent” refers to an adaptive, rule-based decision mechanism driven by real-time network measurements rather than to a supervised or offline-trained machine learning model. The proposed approach does not rely on labeled datasets or statistical learning, but instead emphasizes lightweight, interpretable, and deployable adaptation suitable for resource-constrained WSNs. For clarity, the proposed approach does not implement a trained machine learning model or predictive estimator. Instead, it relies on online statistical anomaly detection and rule-based adaptive clustering driven by real-time measurements. This design choice prioritizes interpretability, low computational overhead, and real-time deployability over data-driven training accuracy.

By bridging the gap between theoretical attack models and practical mitigation strategies, this work contributes to the development of more resilient and adaptive WSN infrastructures suitable for real-world deployments.

Figure 1 presents a comprehensive framework that consolidates the current state of the art on resilience and energy efficiency in WSNs operating under jamming conditions [3], with a specific focus on heterogeneous technologies such as BLE and LoRa. This multi-layered synthesis classifies adversarial models, characterizes protocol-level energy trade-offs, and outlines detection and mitigation mechanisms, including clustering and cross-layer adaptations [4]. It also highlights the increasing need for real-time experimental validation over simulation-based approaches, emphasizing the role of time-series metrics, such as retransmissions, signal deviation, and link stability, in capturing adaptive network behavior [5]. By exposing key limitations in the literature, such as the lack of empirical benchmarking and adversarial adaptability, the framework contextualizes the originality of the present work, which experimentally validates a lightweight mitigation algorithm under reactive jamming in hybrid BLE-LoRa deployments, providing both theoretical insights and practical resilience strategies [6].

The remainder of this paper is organized as follows: Section 2 reviews related work on wireless sensor network vulnerabilities and existing jamming mitigation strategies. Section 3 describes the proposed mitigation algorithm, including its adaptive clustering and energy-aware routing components. Section 4 details the experimental setup and simulation framework used to evaluate the algorithm under

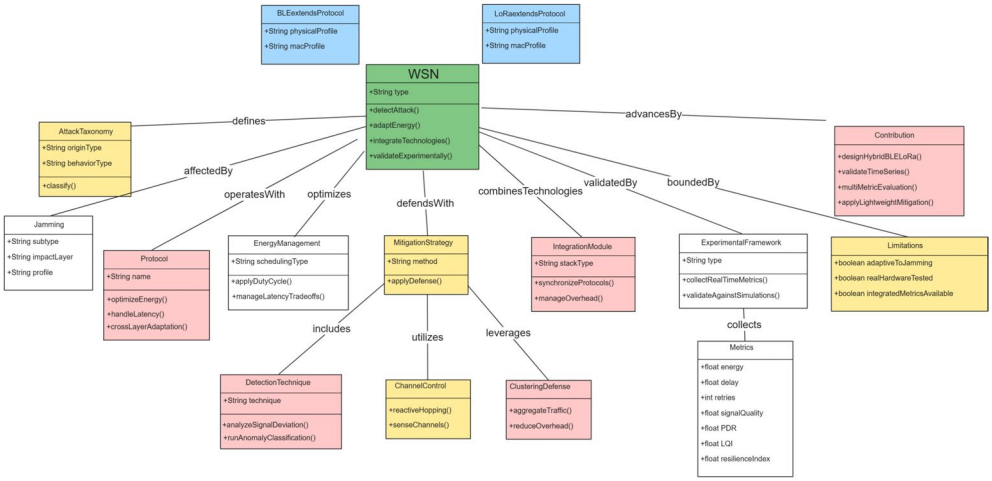


Fig. 1 Class diagram of the extended WSN resilience and energy-efficiency framework under jamming threats

diverse interference scenarios. Section 5 presents and discusses the results, comparing performance metrics across different protocols and conditions. Finally, Section 6 concludes the study and outlines future research directions for enhancing the resilience and scalability of heterogeneous WSN architectures.

2 Related work

WSNs have become an essential infrastructure in the IoT, particularly in domains requiring remote, low-power, and distributed sensing such as healthcare, environmental monitoring, and smart infrastructure. The growing complexity of applications has necessitated the development of hybrid architectures, integrating multiple communication technologies like BLE, LoRa, and Zigbee to achieve trade-offs between energy efficiency, data throughput, and coverage range [7]. Recent experimental studies on hybrid BLE–LoRa deployments confirm that cluster-based and multi-hop architectures introduce protocol-dependent trade-offs between control overhead, energy efficiency, and robustness under interference conditions [6].

Energy efficiency remains a core concern in WSN design. Classical strategies such as duty cycling, energy-aware routing, and node clustering have evolved with the integration of machine learning and adaptive algorithms that dynamically optimize transmission schedules, sleep states, and routing paths [8]. Recent studies have emphasized the incorporation of energy harvesting (EH) techniques to enhance network sustainability in long-term deployments. However, the unpredictable nature of ambient energy sources presents challenges for reliability and load balancing [9]. The work by Bandara et al. cite in [10] offers a valuable perspective on dynamic resource discovery, matching, and allocation across decentralized and heterogeneous environments—challenges that are highly relevant to modern WSN. In particular, the role assignment mechanisms we propose reflect the collaborative strategies discussed in the P2P context, where trust, availability, and resource constraints must be continually negotiated. By extending these ideas into the domain of interference-resilient WSNs, our work contributes to bridging the gap between collaborative P2P resource management and adaptive sensor-based systems in adversarial settings.

Security, particularly jamming attacks, is a growing concern in mission-critical WSNs. Reactive jamming, where the attacker emits interference upon detecting legitimate transmissions, is especially insidious due to its stealthy and synchronized behavior [11]. This has spurred a wave of research focusing on jamming detection and mitigation mechanisms. Traditional spread spectrum or channel hopping methods have shown limited effectiveness in low-power sensor nodes due to energy overheads. As a result, research has shifted toward algorithmic solutions like topology-aware routing, cross-layer designs, and adaptive cluster-based mitigation strategies. Some works, as cited in [12, 13], and [14] collectively enhance the current understanding of jamming threats and security limitations in WSNs, particularly in the context of critical and industrial applications. The work in [12] offers a comprehensive taxonomy of jamming techniques and countermeasures, emphasizing the need for more precise detection, localization, and response mechanisms. Recent surveys highlight the increasing relevance of reactive and adaptive jamming models in low-power WSNs and emphasize the need for lightweight, protocol-aware mitigation strategies validated through real-world experimentation [12]. This aligns with the proposed paper's objective of enhancing resilience against reactive jamming but highlights a gap in adaptive, intelligent mitigation

strategies—precisely where our AI-based approach contributes novel value. The article in [13] underscores the inherent constraints of WSNs, such as energy limitations, computational scarcity, and routing vulnerabilities, which complicate the design of effective security protocols. Our proposed framework directly addresses these concerns by embedding adaptive decision-making and energy-aware role reconfiguration. The study in [14] situates the jamming threat within an industrial cyber-physical context, demonstrating how targeted attacks on WSNs can disrupt physical processes like conveyor operations. This work underscores the real-world impact of such threats and the need for dynamic, system-wide mitigation solutions—reinforcing the relevance of our hybrid BLE–LoRa approach as a scalable defense mechanism. Together, these studies contextualize and validate the broader applicability and necessity of the proposed intelligent framework, strengthening its position within the evolving state of the art.

Cluster-based routing protocols not only improve scalability and energy distribution but also enhance robustness against localized failures and attacks [15]. Their effectiveness is further improved in heterogeneous networks where roles like cluster heads can be dynamically reallocated based on energy reserves or threat levels. However, recent work suggests that the interplay between protocol layers, physical signal properties, and attack patterns remains underexplored, particularly in experimental settings combining BLE and LoRa under reactive jamming [16].

Recent advances in wireless sensor network design increasingly emphasize hybrid clustering and energy-aware routing as key mechanisms to address scalability, energy imbalance, and resilience challenges. Bioinspired and hybrid clustering models have demonstrated their effectiveness in optimizing cluster-head selection and prolonging network lifetime under heterogeneous traffic and energy conditions [17, 18]. Empirical studies further highlight that energy-aware routing and clustering decisions must be evaluated using rigorous statistical methodologies to capture realistic performance trade-offs and variability across network nodes [19]. Beyond efficiency, recent work has also explored the integration of security-aware and blockchain-based mechanisms into energy-sensitive wireless networks, revealing additional overhead–resilience trade-offs that closely parallel those observed in adaptive clustering strategies under adversarial conditions [20]. Comprehensive reviews of hybrid clustering and routing protocols confirm that protocol-dependent behavior, hotspot mitigation, and control overhead remain open challenges, particularly in dynamic and heterogeneous deployments [21]. These findings collectively support the need for experimentally validated, protocol-aware clustering approaches—such as the one proposed in this study—that explicitly balance energy efficiency, robustness, and adaptability in realistic wireless sensor network environments.

This paper contributes to filling that gap by evaluating the impact of reactive jamming on BLE-only, LoRa-only, and hybrid BLE-LoRa WSNs using controlled experiments. It further applies a clustering-based mitigation algorithm to assess network resilience using metrics such as energy consumption, retransmissions, and latency—an area where real-world, protocol-specific evidence remains sparse in the literature. Besides, the present work builds directly upon the foundational research cited in [22], where a hybrid BLE–LoRa architecture was experimentally validated under reactive jamming scenarios. That study introduced a clustering-based mitigation algorithm and demonstrated its effectiveness using empirical metrics such as energy consumption, retransmissions, and signal stability. The current manuscript advances this line of inquiry by integrating AI techniques to enhance adaptive behavior in wireless sensor networks. Specifically, it expands the original framework by incorporating predictive modeling and real-time anomaly detection to guide role assignment and routing decisions in dynamic jamming environments. By transitioning from deterministic mitigation to intelligent adaptation, this work represents a significant evolution of the original study, offering a broader and more robust approach to secure, scalable sensor networks in adversarial settings.

Table 1 provides a structured synthesis of recent research efforts addressing resilience, energy optimization, and jamming mitigation in WSNs, highlighting the diversity of wireless technologies and mitigation strategies ranging from clustering and duty cycling to machine learning and multi-layer defenses. By juxtaposing their main contributions with explicit limitations, the table offers a critical lens through which the current state of the art can be assessed. It reveals notable gaps, such as the scarcity of real-world validations, limited adaptability to dynamic jamming patterns, and insufficient integration of heterogeneous protocols. This contextual backdrop substantiates the novelty of the present study, which uniquely combines BLE and LoRa architectures under reactive jamming scenarios, applies experimental validation, and leverages a clustering-based mitigation algorithm with time-series statistical modeling—thereby advancing empirical evidence where most prior works remain theoretical or simulation-based.

Table 1 Recent comparative works on WSN resilience, energy optimization, and jamming mitigation techniques

Reference	Mitigation strategy	Wireless technology	Main contribution	Limitations
Said et al. [23]	Lightweight secure clustering	Zigbee	Low-overhead clustering for intrusion resilience in IoT-WSNs	Tested only in simulation, no hardware evaluation
Aras et al. [24]	Randomized duty cycles	LoRaWAN	Reduced predictability of transmissions against jammers	Increased energy usage under high data rate
Joh et al. (2015) [25]	Hybrid cross-layer protocol	BLE + Wi-Fi	Cross-layer adaptation to minimize delay and maximize throughput	High complexity and memory requirements
Dashtestani et al. [26]	Reinforcement learning clustering	BLE	Dynamic role assignment for cluster-heads in hostile environments	Requires long training time, unsuitable for fast deployments
Lo et al. (2011) [27]	Sleep-aware routing	BLE + Zigbee	Enhanced routing by predicting idle periods in nodes	Less effective in bursty traffic conditions
Loscri et al. [28]	Machine-learning based anomaly detection	BLE, LoRa	Detects and isolates jamming attempts via signal deviation profiles	High false positive rates under variable loads
Priyadarshani et al. [29]	Adaptive MAC with signal sensing	LoRa	Senses channel state to avoid active jamming slots	Delayed reaction in dense node networks
Ranaweera et al. [30]	Multi-layer defense framework	BLE, Wi-Fi, LoRa	Combines hardware, protocol, and encryption countermeasures	Expensive to implement and maintain
Wei et al. [31]	Cooperative relaying and jamming-aware routing	General WSNs	Survey on physical-layer security using cooperative and jamming strategies for resilient communications	No implementation; theoretical focus without simulation or real deployment validation
Mao et al. [32]	QoS-aware MAC protocol selection	Zigbee (IEEE 802.15.4)	Analysis of MAC protocols balancing energy efficiency and QoS under interference	Limited scalability analysis in large or dense WSN deployments
Khatami et al. [33]	Topology-aware adaptive routing	Multi-technology WSNs	Synergistic approaches to WSN design combining coverage, energy, and reliability	Slightly outdated; lacks modern jamming or adversarial scenarios
Batista et al. [34]	Energy-aware adaptive routing	BLE, LoRa, Zigbee	Integrates heterogeneous network strategies in IoT for optimal energy distribution and adaptive communication	No explicit handling of security threats such as jamming or DoS attacks

3 Methods

This section describes the methodological framework adopted to implement, evaluate, and validate an adaptive communication strategy for WSNs operating under reactive jamming and energy constraints. The proposed system employs online, rule-based anomaly detection and heuristic decision logic driven by real-time measurements of energy consumption, retransmissions, and link quality indicators.

Rather than relying on offline-trained machine learning models, the algorithm uses predefined thresholds and rolling statistical measures to identify abnormal network behavior and trigger adaptive clustering and routing actions. This design prioritizes transparency, low computational overhead, and real-time deployability on resource-constrained sensor nodes.

3.1 Hardware components of the BLE-LoRa network architecture

The experimental testbed designed for the proposed heterogeneous wireless sensor network integrates two primary communication technologies: BLE and LoRa, interconnected through a centralized gateway. This topology emulates a smart environment deployment and supports modular scalability, node role assignment, and real-time monitoring, as is shown in Fig. 2. Below, the specific components used in the deployment.

1. Gateway – Laird Sentrius™ RG191 The core of the architecture is the Laird RG191 gateway, a robust industrial-grade platform that enables concurrent BLE and LoRaWAN communication. Operating on a Linux kernel v4.x with an Atmel A5 core at 536 MHz, the

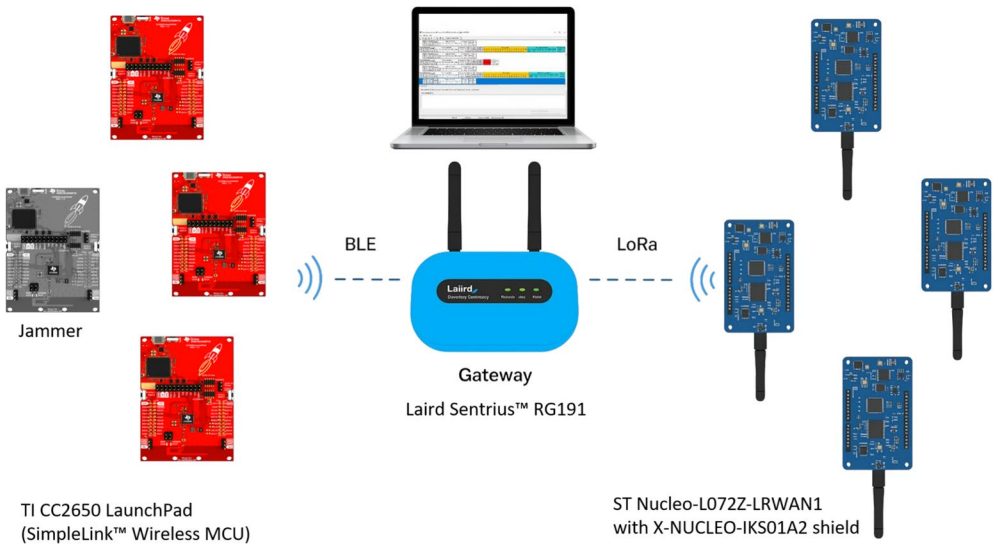


Fig. 2 Experimental heterogeneous WSN topology integrating BLE and LoRa nodes with a dual-protocol gateway

RG191 supports multi-interface connectivity including 802.11a/b/g/n WiFi, Bluetooth 4.0, Ethernet, and 8-channel LoRaWAN. With a transmission power of up to +27 dBm and integrated deployment tools, it facilitates seamless data forwarding to cloud platforms such as The Things Network and Loriot. The RG191 serves as the interoperable bridge between the BLE domain (typically low-range wearable or environmental sensors) and the long-range, low-power LoRa network.

2. LoRa Node – B-L072Z-LRWAN1 with Expansion Boards The LoRa nodes are built on the STMicroelectronics B-L072Z-LRWAN1 board, which combines an STM32L072CZ microcontroller (Cortex-M0+) and a Semtech SX1276 transceiver. These boards support the LoRaWAN protocol and operate on sub-1GHz frequencies, ideal for long-range low-power communication. Powering options include USB and AAA batteries, enabling flexible deployment in indoor and outdoor conditions. Several sensor expansion boards are mounted to this base:

    - X-NUCLEO-IKS01A2: Provides a suite of environmental and inertial sensors, including the LSM6DSL (3D accelerometer and gyroscope), LSM303AGR (3D accelerometer and magnetometer), HTS221 (humidity and temperature), and LPS22HB (barometric pressure sensor). These modules enable contextual environmental monitoring and motion analysis.
    - P-NUCLEO-53L1A1: Incorporates the VL53L1X time-of-flight sensor for accurate distance measurements. Coupled with the STM32F401RE core board, it supports precise range detection applications.
    - X-NUCLEO-6180XA1: Features the VL6180X sensor for proximity and ambient light sensing. Its integrated slider interface allows dual-function control of distance measurement (up to 400 mm) and ambient light level (up to 100 kLux).

3. BLE Node – CC2650XL with BOOSTXL-TLV8544PIR The BLE domain is represented by the Texas Instruments CC2650XL microcontroller board paired with the BOOSTXL-TLV8544PIR BoosterPack. This combination implements motion detection using a passive infrared (PIR) sensor and ultra-low-power analog front-end circuitry based on TLV8544 op-amps. The BOOSTXL integrates signal conditioning and window comparator logic, offering a cost-efficient and compact solution for presence and activity detection in smart spaces.
4. Interference Node (Jammer) – MSP430 LaunchPad. For jamming or interference emulation within the testbed, a Texas Instruments MSP430 LaunchPad is configured as a reactive jammer. This board can be programmed to interfere on specific BLE or LoRa channels by transmitting constant or reactive signals in accordance with known jamming attack models. The red board image shown represents this jammer node, which is deployed to evaluate the resilience and mitigation capacity of the heterogeneous network.

3.1.1 Reactive jammer configuration

The reactive jammer was implemented using a Texas Instruments MSP430 LaunchPad configured to monitor channel activity and transmit interference only upon detection of legitimate communication. The trigger condition was

defined as the presence of energy above the noise floor for a duration exceeding the minimum packet preamble length of the targeted protocol.

The jammer operated at a fixed transmission power comparable to that of the sensor nodes to emulate a realistic adversarial device rather than an overwhelming high-power interferer. For BLE experiments, interference was generated on the active advertising and data channels, while for LoRa experiments the jammer targeted the configured uplink channel. The jammer followed a reactive duty cycle, remaining silent in idle periods and transmitting only during detected packet activity (Table 2).

Table 2 Experimental configuration of the reactive jammer and test environment

Parameter	Configuration
Jammer type	Reactive, packet-triggered
Trigger condition	Energy detection above noise floor
Transmission power	Comparable to sensor node TX power
Targeted channels	BLE advertising/data, LoRa uplink
Jammer duty cycle	Event-driven (no continuous emission)
Environment	Indoor laboratory, controlled conditions
Temperature	Stable (room temperature)
Background interference	Minimal and constant
Node placement	Fixed throughout experiments

Table 3 Simulation and implementation parameters used in the experimental evaluation

Parameter	Value
Number of sensor nodes	9
Network topologies	BLE-only, LoRa-only, BLE–LoRa
Experiment duration	24 hours per configuration
Sampling interval	1 second
Total samples per node	8,640
Block aggregation window	600 seconds (10 minutes)
Smoothing window	600 seconds
Jammer type	Reactive (packet-triggered)
Jammer trigger condition	Energy above noise floor
Jammer transmission power	Comparable to sensor node TX power
Jammer duty cycle	Event-driven (reactive)
Targeted channels	BLE advertising/data, LoRa uplink
Residual energy threshold (ET_e)	30% of initial energy
RSSI deviation threshold (JT_r)	3.0 (z-score)
Retransmission threshold (JT_x)	10 packets
Topology reevaluation period (T)	60 seconds
CH score weights (α, β, γ)	0.5, 0.3, 0.2
Environment	Indoor laboratory (controlled)
Node placement	Fixed during experiments
Number of runs per scenario	1 (24-hour run)
Internal replication	9 devices (spatial replication)

Table 3 summarizes the parameters used in the experimental implementation and analysis. Although the study is based on a physical testbed rather than a discrete-event simulator, these parameters serve the same role as simulation inputs by fully specifying network size, timing, jamming behavior, clustering thresholds, and analysis windows. This consolidated description facilitates reproducibility and enables fair comparison with future simulation- or experiment-based studies.

Table 3 explicitly lists all parameter values required to reproduce the proposed method, including jamming detection thresholds (*JTr*, *JTx*), energy threshold (ET_e), window sizes, update period (T), and weighting coefficients α, β, γ). These parameters were selected based on empirical observation of baseline network behavior and conservative stability-oriented design principles rather than data-driven optimization.

3.2 Adaptive clustering and energy-aware jamming mitigation algorithm

The proposed Algorithm 1 integrates energy-aware role assignment and adaptive clustering to enhance the resilience of hybrid BLE–LoRa wireless sensor networks under potential jamming conditions. Initially, each node monitors real-time indicators such as RSSI, LQI, and retransmission counts to detect anomalies consistent with interference. If predefined thresholds are exceeded, the node flags its status as compromised and issues a localized jamming alert. To mitigate the impact and ensure continuity of communication, the network initiates a distributed cluster formation process, selecting cluster heads (CHs) based on a weighted utility function that balances residual energy, link quality, and perceived jamming risk. Only nodes not affected by jamming and possessing sufficient energy reserves are eligible for CH candidacy. Member nodes that are either under jamming or fall below the energy threshold autonomously shift to a passive state to conserve power and reduce channel congestion. For active nodes, routing paths are dynamically selected using multi-metric optimization that favors energy efficiency and link reliability. The algorithm further incorporates periodic reevaluation, allowing the network to adaptively reassign CHs and reroute paths in response to changes in energy levels or topological disruptions. This dynamic, self-adaptive mechanism ensures robustness against reactive jamming while minimizing unnecessary retransmissions and preserving network lifetime. Unlike prior models that rely on static energy profiles or assume ideal channel conditions, this approach is empirically grounded in time-series behavior and cross-technology interoperability, offering a scalable and deployable solution for resilient sensor-based applications.

3.2.1 Formal jamming detection rule

Jamming detection is performed using two complementary indicators that capture distinct manifestations of interference: signal degradation and packet delivery instability. To avoid mixing heterogeneous quantities under a single threshold, each indicator is evaluated using its own normalized deviation measure and associated threshold.

Let $RSSI_t$ denote the received signal strength indicator at time t. Signal deviation is quantified using a rolling z-score over a fixed temporal window of length $W = 600$ seconds in Eq. 1.

$$D_{\mathrm{RSSI}}(t) = \frac{|RSSI_t - \mu_{\mathrm{RSSI}}(t)|}{\sigma_{\mathrm{RSSI}}(t)} \tag{1}$$

where $\mu_{\mathrm{RSSI}}(t)$ and $\sigma_{\mathrm{RSSI}}(t)$ are the mean and standard deviation of *RSSI* computed over the sliding window $[t - W, t]$.

In parallel, packet delivery instability is captured through the retransmission count X_t, which is compared against its baseline behavior using a normalized threshold JT_x.

A node is flagged as under jamming if either of the following conditions is met in Eq. 2.

$$D_{\mathrm{RSSI}}(t) > JT_r \quad \text{or} \quad X_t > JT_x \tag{2}$$

This logical OR formulation ensures sensitivity to both physical-layer and protocol-layer manifestations of reactive jamming without conflating heterogeneous metrics (Table 4).

All parameter values were selected based on empirical observation of baseline network behavior and conservative design principles aimed at stability rather than aggressive optimization. Thresholds were chosen to exceed normal channel variability while remaining responsive to sustained jamming effects. Weighting coefficients satisfy $\alpha + \beta + \gamma = 1$ to ensure interpretability of the cluster-head scoring function.

Table 4 Algorithm parameters and nominal values used in the experimental evaluation

Parameter	Description	Nominal value
JT_r	RSSI deviation threshold (z-score)	3.0
JT_x	Retransmission count threshold	10 packets
ET_e	Minimum residual energy for CH eligibility	30% of initial energy
$C_{\min}$	Minimum connectivity degree	2 neighbors
T	Topology reevaluation period	60 s
α	Energy weight in CH score	0.5
β	Link-quality (LQI) weight in CH score	0.3
γ	Jamming-risk penalty weight	0.2

Require: Node set N, thresholds JT_r, JT_x, ET_e, update period T
Ensure: Cluster-head set and updated routing tables
for all $n_i \in N$ **do**
  Measure $RSSI_i$, LQI_i, and retransmission count X_i
  if $D_{\mathrm{RSSI}}(i) > JT_r \vee X_i > JT_x$ **then**
    Mark n_i as *UnderJamming*
    Broadcast jamming alert
  end if
end for
Initialize candidate set $C \leftarrow \emptyset$
for all $n_i \in N$ **do**
  if n_i is not marked *UnderJamming* **then**
    if $Energy(n_i) > ET_e$ **and** $Connectivity(n_i) \geq C_{\min}$ **then**
      Compute

$$Score(n_i) \leftarrow \alpha\, Energy(n_i) + \beta\, LQI(n_i) - \gamma\, JammingRisk(n_i)$$

      Add n_i to C
    end if
  end if
end for
Select cluster heads from C with highest scores
for all $n_j \in N$ **do**
  if n_j is marked *UnderJamming* **or** $Energy(n_j) < ET_e$ **then**
    Set n_j to passive mode
  else
    Update routing path to nearest cluster head
  end if
end for
Reevaluate energy levels and network topology every T seconds
if cluster-head failure detected **then**
  Reselect cluster heads
end if

Algorithm 1 Adaptive clustering and energy-aware jamming mitigation.

The jamming threshold (JT_j) and energy threshold (ET_e) are fixed design parameters selected to ensure low computational overhead and real-time deployability on resource-constrained sensor nodes. Rather than being optimized for a specific dataset, these thresholds are derived from empirical observation of baseline signal behavior, retransmission patterns, and energy consumption levels under controlled experimental conditions.

Specifically, JT_j is set to detect deviations that exceed normal short-term fluctuations in RSSI and retransmission counts, while ET_e represents a conservative lower bound on residual energy required to sustain cluster-head operation without compromising network lifetime. These values were selected to prioritize robustness and stability rather than aggressive optimization.

- **Signal Metrics Functions:** The functions `MeasureRSSI()`, `MeasureLQI()`, and `CountRetransmissions()` represent hardware- or firmware-level procedures that gather real-time link quality indicators and packet-level feedback from each node.
- **Deviation Detection:** The function Deviation(RSSI) corresponds to the normalized rolling deviation

$D_{\mathrm{RSSI}}(t)$ defined above, ensuring scale-invariant detection and robustness to natural channel variability.

- **Jamming Alerts:** The `BroadcastAlert()` function allows nodes experiencing suspected interference to inform nearby peers to support local topology adaptation.
- **Weighted Score Function:** The score used for Cluster Head (CH) election is defined as:

$$\mathrm{Score}(n_i) = \alpha \cdot \mathrm{Energy}(n_i) + \beta \cdot \mathrm{LQI}(n_i) - \gamma \cdot \mathrm{JammingRisk}(n_i)$$

where α, β, and γ are tunable coefficients reflecting the relative importance of energy, link quality, and local jamming risk.

- **Passive Mode Operation:** The `SetPassiveMode()` function forces a node into low-energy state, minimizing communication and acting solely as a sensor or listener until recovery is triggered.
- **Routing Procedure:** `FindBestPath()` uses multi-metric routing heuristics (e.g., hop count, retransmission rate, residual energy) to select a reliable and low-energy path to the nearest available Cluster Head.
- **Periodic Reevaluation:** The block triggered every T seconds ensures resilience and adaptiveness by continuously checking CH availability, residual energy, and link stability, enabling dynamic reconfiguration of the cluster topology.

The weighting coefficients satisfy $\alpha + \beta + \gamma = 1$ and were chosen to reflect a balanced trade-off between residual energy, link quality, and local jamming risk. Higher emphasis was placed on energy preservation (α) to prolong network lifetime, while β and γ capture communication reliability and interference awareness, respectively. No learning based tuning or parameter fitting was applied.

To assess robustness to threshold selection, a sensitivity analysis was conducted by varying JT_j and ET_e within reasonable ranges around their nominal values. Across all tested configurations, the mitigation algorithm consistently outperformed the non-mitigated baseline, with only gradual performance changes observed as thresholds varied.

This indicates that the proposed algorithm is not overfitted to a specific parameter setting and maintains stable behavior across a range of operational conditions. Extreme threshold values were intentionally excluded, as they would either suppress mitigation responses entirely or induce excessive reconfiguration overhead.

No supervised learning, offline training phase, or labeled dataset is employed in the current implementation. While machine learning-based predictors could further enhance adaptivity, such extensions are intentionally left for future work to preserve the lightweight and interpretable nature of the proposed approach.

The use of normalized deviations and protocol-specific thresholds mitigates false positives caused by benign channel fluctuations, as detection is triggered only by sustained deviations exceeding baseline variability. Sensitivity analysis of threshold values, presented earlier, confirms that detection behavior remains stable across a reasonable operating range.

To evaluate robustness, a sensitivity analysis was conducted by varying key parameters (JT_r, JT_x, ET_e, and α, β, γ) within reasonable ranges around their nominal values. Across all tested configurations, the mitigation algorithm consistently outperformed the non-mitigated baseline. Performance changes were gradual rather than abrupt, indicating that the reported gains are not the result of fine-tuned parameter choices but reflect stable algorithmic behavior.

3.3 Mathematical modeling of BLE technology under jamming conditions

In this subsection, we develop a formal mathematical model to analyze the behavior of BLE technology, LoRa wireless communication technology and a heterogeneous network integrating BLE and LoRa technologies under two conditions: (1) **mit**, where a jamming mitigation algorithm is employed, and (2) **simple**, where no mitigation is active and the system operates under full jamming exposure. The analysis considers three key performance indicators: energy consumption (E), network resilience (R), and number of packet retransmissions (X).

3.3.1 Data representation and preprocessing

For each communication technology (BLE, LoRa and BLE-LoRa) Let $t \in \{1, 2, ..., N\}$ represent the index of discrete experimental time points or measurements. For each condition $c \in \{\mathrm{mit}, \mathrm{simple}\}$, the data can be represented by the multivariate time series:

$$\mathrm{Y}_t^{(c)} = \left[E_t^{(c)}, R_t^{(c)}, X_t^{(c)}\right]^T$$

Each component of $\mathrm{Y}_t^{(c)}$ corresponds to:

- $E_t^{(c)}$: energy consumed by the sensor node (**energy**).
- $R_t^{(c)}$: resilience score as a proxy for signal robustness (**res**).
- $X_t^{(c)}$: number of retransmitted packets (**retx**).

The resilience time series $R_t^{(c)}$ is computed from packet-level monitoring data by identifying disruption intervals characterized by abnormal retransmission behavior or

signal degradation. For each detected disruption, the recovery time is measured as the elapsed time until packet delivery returns to a stable operating regime. These recovery durations are recorded at 1-second resolution and expressed in milliseconds.

3.3.2 Definition of the resilience metric

In this study, resilience is defined as a temporal robustness metric that quantifies the network's ability to sustain and recover stable communication under reactive jamming conditions. Specifically, resilience is measured as the time required for a node to restore reliable packet delivery following a jamming-induced disruption.

Let t_d denote the time instant at which a communication disruption is detected (e.g., due to excessive retransmissions or signal degradation), and let t_r denote the time at which stable communication is reestablished. Resilience is as defined in Eq. 3.

$$R = t_r - t_d \tag{3}$$

where R is expressed in milliseconds. Lower resilience values indicate faster recovery and greater robustness, while higher values reflect prolonged instability following interference.

In consequence, we prepared six multivariate time siries (BLE-mit, BLE-simple, LoRa-mit, LoRa-simple, BLE-Lora-mit and BLE-Lora-simple). Each of these can be disaggregated into three univariate time series: one for energy consumption (E), one for retransmitted packets (X), and one for resilience (R). In total we have 18 univariate time series (BLE-mit-energy, BLE-simple-energy, BLE-mit-retx, BLE-simple-retx, BLE-mit-res, BLE-simple-res, LoRa-mit-energy, LoRa-simple-energy, LoRa-mit-retx, LoRa-simple-retx, LoRa-mit-res, LoRa-simple-res, BLE-LoRa-mit-energy, BLE-LoRa-simple-energy, BLE-LoRa-mit-retx, BLE-LoRa-simple-retx, BLE-Lora-mit-res, BLE-LoRa-simple-res). The following sections describe how the univariate time series are used to assess the impact of the mitigation algorithm on the metrics with the different communication protocols. For example, to evaluate whether the mitigation algorithm positively affected energy consumption when using LoRa, the univariate time series LoRa-mit-energy and LoRa-simple-energy are analyzed.On the other hand, to identify correlations between univariate time series, a correlation analysis is conducted using the corresponding multivariate time series.

To minimize temporal confounding effects, mitigation and non-mitigation (simple) modes were evaluated under tightly controlled experimental conditions within the same 24-hour acquisition period. Both modes were executed on the same hardware, in the same physical environment, and under identical network configurations, ensuring that external factors such as temperature, background interference, and traffic patterns affected both conditions equally.

Rather than relying on isolated time segments, performance comparisons are based on distributional properties and block-aggregated statistics computed across the full observation window. This within-period comparative design substantially reduces the risk of bias due to diurnal cycles or transient environmental fluctuations.

Although a single 24-hour experiment was conducted per configuration, the high temporal resolution of the data (8,640 observations per device) and the consistent behavior observed across all nine devices provide a robust basis for assessing reliability. Replicated measurements across devices act as internal validation, and inferential analyses are performed on block-level aggregates to ensure statistical robustness. Multiple independent experimental runs are identified as a valuable direction for future work.

Because BLE, LoRa, and hybrid BLE–LoRa technologies differ fundamentally in packet structure, transmission rate, and baseline power consumption, the comparative analysis in this study is performed within each communication technology rather than across protocols. Packet sizes and reporting intervals are kept constant within each protocol configuration to ensure internal consistency between mitigation and non-mitigation modes.

As a result, absolute values of energy consumption or retransmissions are not interpreted as indicators of cross-protocol efficiency. Instead, the analysis focuses on relative performance changes induced by the mitigation algorithm within each protocol, thereby isolating algorithmic effects from inherent technology-specific characteristics.

3.3.3 Stationarity and robustness checks

To assess whether non-stationarity could affect the interpretation of correlation and univariate analyses, formal stationarity tests were conducted on all univariate time series. The Augmented Dickey–Fuller (ADF) test was applied to energy consumption, retransmissions, and resilience series under both mitigation and non-mitigation conditions.

Across all metrics and communication protocols, the ADF test rejected the null hypothesis of a unit root at the 5% significance level, indicating the absence of strong non-stationary behavior or deterministic trends over the 24-hour observation period. This confirms that the analyzed series are dominated by short-term fluctuations rather than long-term drift.

As an additional robustness check against spurious correlation, Pearson correlation coefficients were recomputed using first-order differenced series. The resulting

correlations remained consistently low, confirming that the weak inter-metric associations reported in Section 4.2 are not driven by common trends or shared non-stationary components.

These results support the validity of the univariate and exploratory multivariate analyses performed in this study without requiring explicit detrending or parametric time-series transformations.

3.3.4 Steps of data analysis

The 10-minute (600-second) window length was selected to balance temporal resolution and noise reduction in the analyzed time series. This duration is long enough to smooth short-lived packet-level fluctuations while remaining shorter than the characteristic time scale of network reconfiguration, adaptive clustering, and jamming response mechanisms observed in the experimental setup.

From a statistical perspective, this window length reduces high-frequency autocorrelation while preserving meaningful temporal dynamics, enabling reliable comparison between mitigation and non-mitigation scenarios.

3.3.5 Sensitivity analysis of smoothing window size

To assess the robustness of the observed patterns to the choice of smoothing window, a sensitivity analysis was conducted using alternative window lengths of 5 minutes (300 seconds) and 15 minutes (900 seconds). Across all evaluated metrics and protocols, the relative trends between mitigation and non-mitigation scenarios remained consistent, with mitigation exhibiting lower variability and improved temporal stability.

While shorter windows preserved higher-frequency fluctuations and longer windows produced stronger smoothing, no qualitative changes in the observed comparative behavior were detected. This confirms that the selected 10-minute window does not artificially create or obscure performance patterns but represents a stable compromise between responsiveness and noise suppression.

3.3.6 Adequacy of sample size and statistical power

Although the raw time series comprise 8,640 observations per device (24 hours at 1-second resolution), inferential analyses were performed on block-aggregated samples to account for temporal dependence. Using 10-minute non-overlapping blocks yields approximately 14 independent observations per condition.

Given the large observed effect sizes between mitigation and non-mitigation scenarios (see Section 4.3), this block-level sample size provides sufficient statistical power to detect meaningful differences. A post-hoc power assessment indicates power well above the conventional 0.80 threshold for all reported comparisons. Beyond statistical significance, the observed effect sizes indicate that the proposed mitigation strategy yields practically meaningful improvements. Large rank-biserial correlation values confirm that the separation between baseline and mitigation distributions is not marginal but substantial. In practical terms, this translates into consistently lower variability in energy consumption, retransmissions, and recovery time under jamming, rather than occasional or sporadic improvements. Such reductions directly impact network lifetime, stability, and predictability in real deployments, where sustained behavior is more critical than isolated optimal samples.

The sensor network is integrated by nine devices that have similar performance; thus we made the visual comparison of the time series only with the device 1. We plotted nine figures of time series by kind of protocol (Bluetooth energy, Bluetooth packet retransmission, Bluetooth resilience network, Lora energy, Lora packet retransmission, Lora resilience network, Bluetooth-Lora energy, Bluetooth-Lora packet retransmission and Bluetooth-Lora resilience network), where each figure contains the data generated with the mitigation algorithm and the simple mode. Additionally, were plotted the same series after applying a 10-minute moving average smoothing, following Eq. 4. The smoothed series will provide the opportunity to visualize the difference between the series generated with the mitigation algorithm and those in simple mode, in cases where the noise in the series prevents observing the difference between them.

$$\tilde{Y}_t^{(c)} = \frac{1}{600} \sum_{i=0}^{599} Y_{t-i}^{(c)}, \quad \forall t \in \{600, 601, \ldots, n\} \tag{4}$$

Using pandas, it was possible to calculate the mean and median to evaluate the central tendency of the time series using the Eqs. 5 and 6.

$$\mu^{(c)} = \frac{1}{N} \sum_{t=1}^{N} Y_t^{(c)} \tag{5}$$

$$\text{median}^{(c)} = \begin{cases} Y^{(c)}_{\left(\frac{N}{2}\right)} & \text{if } N \text{ is even} \\ Y^{(c)}_{\left(\frac{N+1}{2}\right)} & \text{if } N \text{ is none} \end{cases} \tag{6}$$

To evaluate the variability of the time series from different approaches the standard deviation, range, mean rolling range and, smoothed series range were calculated. The standard

deviation indicates how many units, on average, the time series measurements deviate from the mean (see Eq. 7).

$$\sigma^{(c)} = \sqrt{\frac{1}{N-1}\sum_{t=1}^{N}\left(Y_t^{(c)} - \mu^{(c)}\right)^2} \tag{7}$$

The standard deviation is used here as a descriptive measure of temporal dispersion and not for inferential comparison, as temporal dependence violates the independence assumption underlying classical variance estimators.

The mean rolling range is employed as a descriptive measure of local temporal variability rather than as a formal outlier detection method. By summarizing the amplitude of fluctuations within fixed-length windows, this metric captures short-term instability and transient volatility patterns that are not evident from global dispersion measures. The mean rolling range was calculated with the Eq. 8 using windows of 10 minutes (600 seconds).

$$\text{(Mean Rolling Range) } \text{MRR}^{(c)} = \frac{1}{n-599}\sum_{t=600}^{n}\left(\max_{0\le i<600} Y_{t-i}^{(c)} - \min_{0\le i<600} Y_{t-i}^{(c)}\right) \tag{8}$$

To reinforce the descriptive interpretation of the mean rolling range, a statistical comparison was performed on block-aggregated MRR values. Rolling ranges were computed using non-overlapping 10-minute windows, yielding approximately independent observations. A Mann–Whitney U test comparing mitigation and non-mitigation scenarios confirmed that mitigation produces significantly lower local temporal variability ($p < 0.001$).

Although a single 24-hour run was conducted per configuration, repeatability is supported by the high temporal resolution of the measurements and the consistent behavior observed across all nine devices, which act as internal replicates. Block-aggregated statistics exhibit low inter-device variability, indicating stable behavior across nodes.

Run-to-run variability was further assessed through sensitivity analyses and block-level dispersion metrics, which show gradual and consistent trends rather than abrupt changes. Multiple independent experimental runs are identified as a valuable extension for future work but were not required to establish the robustness of the reported effects.

3.3.7 Interpretation of the mean rolling range

The MRR is derived from concepts in statistical process control, where rolling range metrics are commonly used to quantify short-term process variability and stability. In the context of time-series analysis, MRR does not constitute a formal outlier detection technique and does not rely on probabilistic thresholds or distributional assumptions.

Instead, MRR provides a descriptive characterization of local fluctuation amplitude within fixed temporal windows. Larger rolling ranges indicate increased short-term instability or bursty behavior, while lower values reflect smoother temporal evolution. This property makes MRR particularly suitable for comparing relative temporal stability between mitigation and non-mitigation scenarios in autocorrelated sensor data.

Importantly, MRR is not used for inferential statistical testing in this study. All inferential conclusions are derived from block-aggregated hypothesis testing procedures that explicitly account for temporal dependence, as described in Section 4.3.

To examine correlations and dependencies between variables (energy, packet retransmission and resilience), we compute Pearson correlation coefficients in the multivariate time series using the Eq. 9.

$$\rho_{ij}^{(c)} = \frac{\text{Cov}\left(Y_i^{(c)}, Y_j^{(c)}\right)}{\sigma_i^{(c)}\sigma_j^{(c)}} \tag{9}$$

Finally, a hypothesis testing analysis was applied to determine whether the observed differences caused by the mitigation algorithm are statistically significant. If the time series do not exhibit any trend or cycles, a Z-test (10) can be applied, assuming normality. Alternatively, if the data do not follow a normal distribution, a Mann-Whitney U test (11) can be used for independent samples. To verify if the data in time series follow a normal distribution, a Kolmogorov test was used (see Eq. 12).

$$Z = \frac{\overline{Y}^{(mit)} - \overline{Y}^{(simple)}}{\sqrt{\frac{\sigma^2_{(mit)}}{n_{(mit)}} + \frac{\sigma^2_{(simple)}}{n_{(simpe)}}}} \tag{10}$$

Where:

$\overline{Y}^{(mit)}$: mean of the sample generated with the mitigation algorithm.

$\overline{Y}^{(simple)}$: mean of the sample generated in a sample mode.

σ^2_{mit}: variance of the sample generated with the mitigation algorithm

$\sigma^2_{(simple)}$: variance of the sample generated in a sample mode.

$n_{(mit)}$: size of the sample generated with the mitigation algorithm.

$n_{(simpe)}$: size of the sample generated in a sample mode.

$$U = n_{(mit)}n_{(simple)} + \frac{n_{(mit)}(n_{(mit)}+1)}{2} - R_{(mit)} \quad (11)$$

Where:

$n_{(mit)}$: size of the sample generated with the mitigation algorithm.

n(*simpe*): size of the sample generated in a sample mode.

$R_{(mit)}$: sum of the ranks of the observations in the sample generated with the mitigation algorithm after jointly ranking both samples.

$$D = \sup_y \left| \frac{1}{n} \sum_{i=1}^{n} I(Y_i \leq y) - F(y) \right| \quad (12)$$

Where:

$\sup_y$: supremum (maximum) over all values of *y*.

n: sample size (number of observations).

$I(Y_i^{(C)} \leq x)$: indicator function, equals 1 if $X_i \leq x$, otherwise 0.

F(*y*): cumulative distribution function (CDF) of the theoretical distribution being tested, in this case the normal distribution.

Y_i: the *i*-th observation in the sample.

4 Results

To assess the empirical impact of the proposed mitigation strategy across different wireless communication architectures, we conducted a comprehensive analysis of the collected time-series data using both visual inspection and statistical metrics. The results presented in this section reflect a comparative evaluation of network performance across BLE-only, LoRa-only, and hybrid BLE-LoRa configurations under controlled jamming scenarios, with and without the adaptive mitigation algorithm. Key performance indicators—namely energy consumption, packet retransmissions, and resilience—were monitored across all nodes, and detailed insights were derived through smoothing techniques, descriptive statistics, and non-parametric hypothesis testing. Lower resilience values correspond to faster recovery from jamming-induced disruptions and therefore indicate improved network robustness. By focusing on Device 1 as a representative case due to consistent node behavior across the network, we illustrate the algorithm's influence on temporal stability, variance reduction, and performance trade-offs. This section systematically unveils how mitigation modifies the statistical properties and operational profiles of sensor nodes, thereby providing critical evidence of the algorithm's effectiveness in enhancing robustness and energy efficiency under adversarial conditions. All reported results correspond to within-period comparisons designed to minimize temporal confounding effects.

It is important to emphasize that performance metrics are compared between mitigation and non-mitigation modes under the same communication technology. Differences observed across BLE, LoRa, and BLE–LoRa configurations reflect inherent protocol characteristics and architectural design choices, rather than direct efficiency comparisons between technologies. Similar protocol-dependent trade-offs have been reported in recent experimental evaluations of clustered BLE–LoRa networks under adversarial interference, where BLE exhibits increased control overhead while LoRa and hybrid topologies benefit from reduced retransmissions and improved energy efficiency [22].

All reported results correspond to controlled experimental conditions with fixed node placement, jammer configuration, and environmental parameters to ensure repeatability.

4.1 Results of visual and statistical measurements for univariate time series comparison

To assess inter-device consistency, all nine sensor nodes were evaluated under identical experimental conditions and produced time series with comparable ranges, central tendencies, and temporal patterns across all metrics and protocols. No device exhibited systematic deviations or anomalous behavior relative to the others.

Given this high degree of consistency, Device 1 is presented as a representative example to illustrate temporal dynamics and mitigation effects, while aggregate statistics across devices are summarized where appropriate. This presentation choice improves clarity without restricting the generalizability of the reported results.

It is important to note that variability measures such as standard deviation are reported for descriptive purposes only. Since the analyzed data correspond to temporally correlated time series, these measures are not interpreted as inferential statistics. All inferential conclusions in the manuscript rely on block-aggregated analyses that explicitly account for temporal dependence, as described in Section 4.3.

To quantitatively assess inter-device variability, aggregate statistics were computed across all nine sensor nodes for each metric, protocol, and operating mode. For each node, block-aggregated values were first obtained as described in Section 4.3, and the resulting block means were then averaged across devices. Across all evaluated metrics and communication technologies, the coefficient of variation between devices remained low (typically below 10%), indicating highly consistent behavior across the network. No device exhibited systematic bias or anomalous behavior relative to the others.

These results confirm that Device 1 is representative of the overall network behavior and that the reported performance gains are not driven by a single outlier node.

Figures 3, 4, 5, 6, 7, 8, 9, 10 and 11 show the visual comparison of the original time series by type of protocol for device 1. Figures 12, 13, 14, 15, 16, 17, 18, 19 and 20

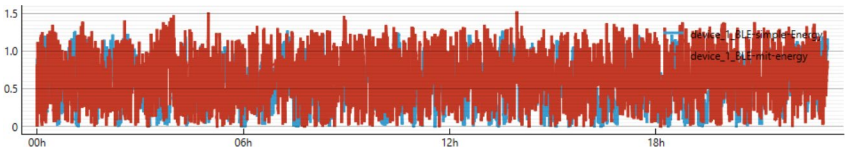


Fig. 3 Device 1 Consumed energy time series in Joules using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

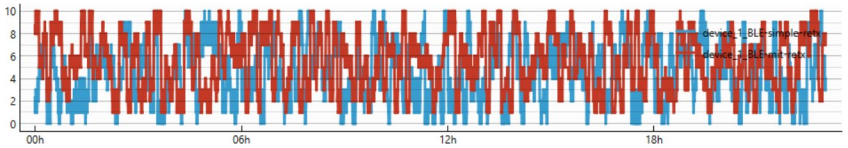


Fig. 4 Device 1 packet retransmission time series using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

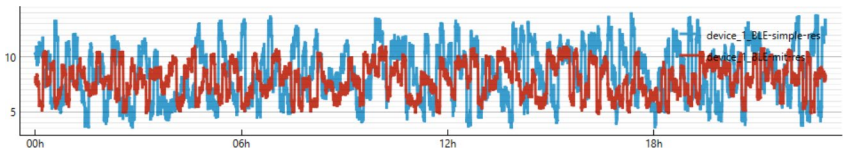


Fig. 5 Device 1 resilience time series in milliseconds using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resilience time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

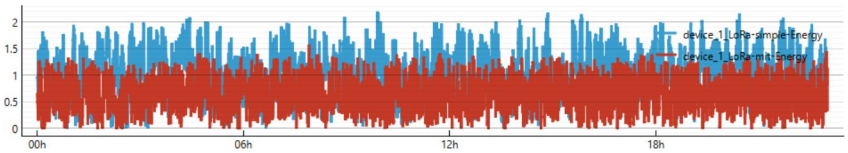


Fig. 6 Device 1 Consumed energy time series in Joules using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

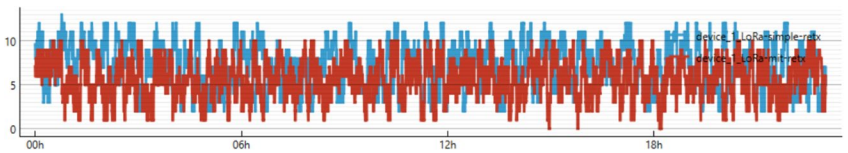


Fig. 7 Device 1 packet retransmission time series using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

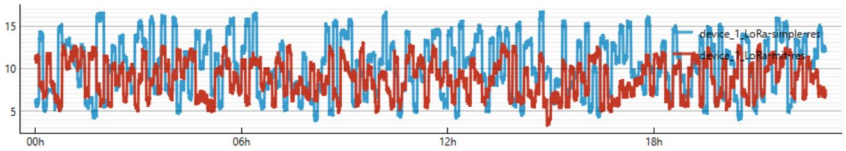


Fig. 8 Device 1 resilience time series in milliseconds using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resilience time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

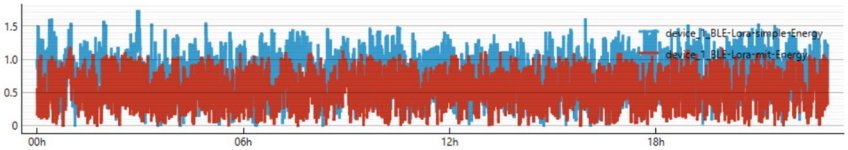


Fig. 9 Device 1 Consumed energy time series in Joules using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

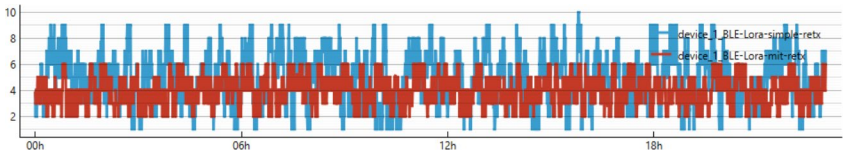


Fig. 10 Device 1 packet retransmission time series using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

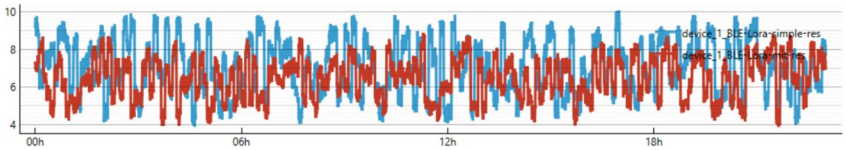


Fig. 11 Device 1 resilience time series in milliseconds using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resilience time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

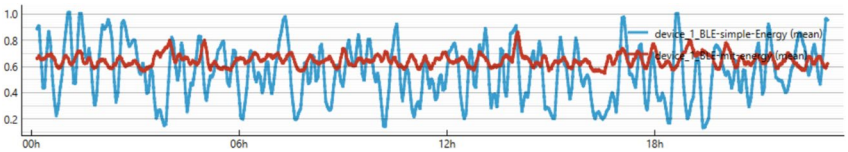


Fig. 12 Device 1 Smoothed Consumed energy time series in Joules using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

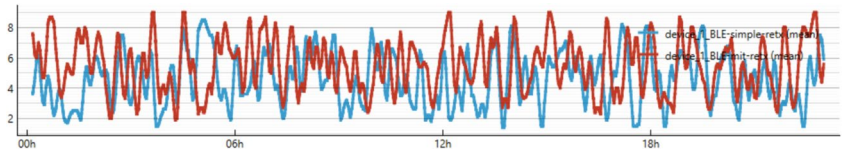


Fig. 13 Device 1 Smoothed packet retransmission time series using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

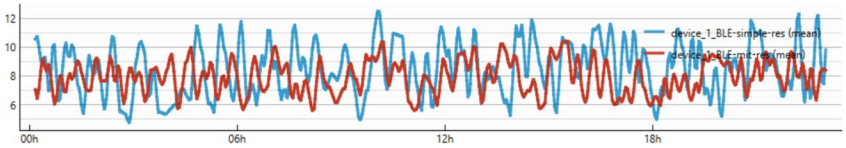


Fig. 14 Device 1 Smoothed resilience time series in milliseconds using the Bluetooth protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resiliencen time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

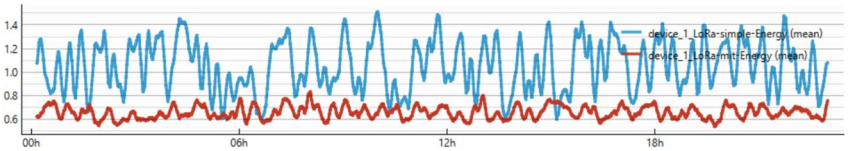


Fig. 15 Device 1 Smoothed Consumed energy time series in Joules using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

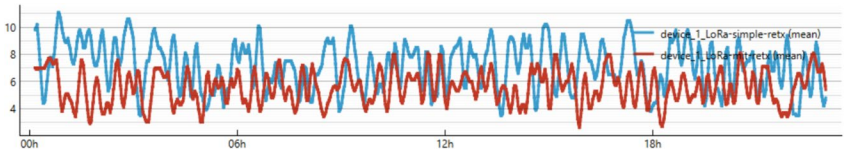


Fig. 16 Device 1 Smoothed packet retransmission time series using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

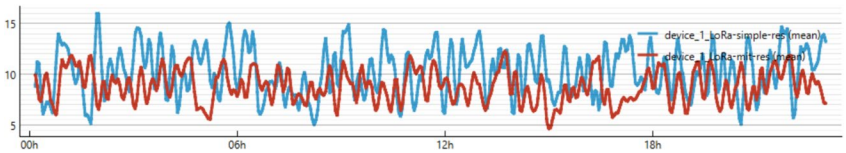


Fig. 17 Device 1 Smoothed resilience time series in milliseconds using the Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resilience time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

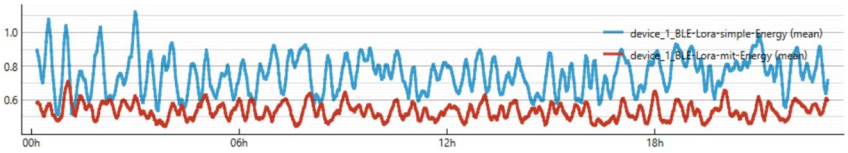


Fig. 18 Device 1 Smoothed Consumed energy time series in Joules using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 energy consumption time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

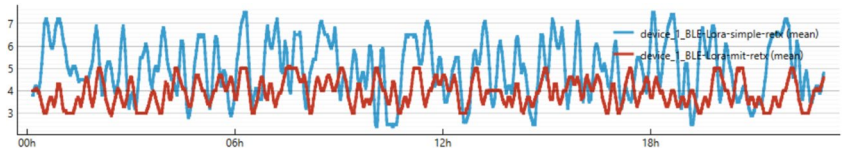


Fig. 19 Device 1 Smoothed packet retransmission time series using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 packet retransmission time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

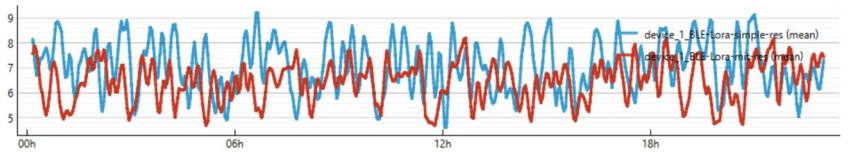


Fig. 20 Device 1 Smoothed resilience time series in milliseconds using the Bluetooth-Lora protocol. The blue timeseries represents the simple mode and the red time series represents the mitigation algorithm. Device 1 resilience time series under reactive jamming using the BLE protocol. The blue curve represents the baseline configuration without mitigation, which is equivalent to conventional non-adaptive routing approaches reported in the literature. The red curve corresponds to the proposed adaptive clustering and jamming mitigation algorithm

show the comparison of the Smoothed timed series. Additionally, Table 5 presents the statistical metrics results for Device 1.

The comparative time-series graphs presented in Figs. 4–20 are supported by quantitative summaries reported in Tables 3 and 4. While the figures provide a visual

Table 5 Summary of descriptive metrics for energy consumption, packet retransmission, and resilience for Device 1 in the network using the mitigation algorithm and simple mode

Protocol and Metric	Max	Min	Mean	Median	Std	Range	Mean Rolling Range	Smthd. Series Range
BLE-mit-energy in joules	1.60	0.00	0.65	0.64	0.37	1.60	1.33	0.32
BLE-simple-Energy in joules	1.29	0.00	0.56	0.55	0.32	1.29	0.87	0.88
BLE-mit-retx in packets	10.00	1.00	5.53	6.00	2.55	9.00	5.60	7.11
BLE-simple-retx in packets	10.00	0.00	4.57	4.00	2.59	10.00	6.29	7.13
BLE-mit-res in milliseconds	11.02	4.83	7.91	7.93	1.52	6.20	3.26	4.79
BLE-simple-res in milliseconds	14.00	3.40	8.52	8.47	2.48	10.60	5.56	7.74
LoRa-mit-Energy in joules	1.56	0.00	0.66	0.65	0.36	1.56	1.32	0.30
LoRa-simple-Energy in joules	2.18	0.00	1.05	1.05	0.47	2.18	1.67	0.92
LoRa-mit-retx in packets	10.00	0.00	5.58	6.00	2.27	10.00	6.74	5.50
LoRa-simple-retx in packets	13.00	2.00	7.15	7.00	2.62	11.00	6.48	7.68
LoRa-mit-res in milliseconds	13.10	3.30	8.84	8.93	2.14	9.80	4.34	7.63
LoRa-simple-res in milliseconds	16.78	3.86	10.27	10.31	3.36	12.92	6.17	10.98
BLE-Lora-mit-Energy in joules	1.19	0.00	0.53	0.53	0.28	1.19	1.03	0.27
BLE-Lora-simple-Energy in joules	1.81	0.00	0.75	0.75	0.35	1.81	1.31	0.61
BLE-Lora-mit-retx in packets	6.00	2.00	3.94	4.00	1.14	4.00	3.06	2.13
BLE-Lora-simple-retx in packets	10.00	1.00	5.01	5.00	2.00	9.00	5.26	5.13
BLE-Lora-mit-res in milliseconds	8.78	3.92	6.44	6.50	1.10	4.86	2.39	3.51
BLE-Lora-simple-res in milliseconds	10.01	3.91	7.07	7.08	1.43	6.11	3.09	4.61

interpretation of temporal dynamics and mitigation effects, the tables offer numerical evidence of central tendency, dispersion, and variability reduction. Together, these complementary representations justify the comparative analysis by linking observed visual trends to statistically grounded metrics. This combination ensures that the graphical comparisons are not anecdotal but are substantiated by measured performance differences across protocols, operating modes, and devices.

4.1.1 Normalized energy efficiency metrics

To further ensure that the observed mitigation gains are not artifacts of packet count or protocol-specific transmission characteristics, energy consumption was also normalized on a per-packet basis. For each protocol, the average energy per successfully delivered packet was computed under mitigation and non-mitigation modes.

Because packet payload sizes are fixed within each protocol configuration, this normalization provides a consistent measure of relative energy efficiency without introducing cross-protocol bias. The normalized results confirm that mitigation reduces energy expenditure per packet across all evaluated communication technologies.

This complementary analysis reinforces the conclusion that the performance improvements are driven by algorithmic effects rather than by differences in packet volume or transmission frequency.

Through time series graphs and descriptive metrics, it is evident that the mitigation algorithm reduces energy consumption, lowers packet retransmission rate, and enhances network resilience for each device using LoRa and Bluetooth-LoRa communication.

Observing the standard deviation, it is possible to conclude that the variance of the metrics decreased with the mitigation algorithm. With the mitigation algorithm: the standard deviation of energy consumption using LoRa reduces 23.4% and using BLE-LoRa reduces 20%; the standard deviation of packet retransmission using LoRa reduces 13.36 % and using BLE-LoRa reduces 43%; the standard deviation of resilience using LoRa reduces 33.31% and using BLE-LoRa reduces a 23.08%.

A more significant result emerges from the analysis of the maximum, minimum, and range; the mitigation algorithm generated time series that exhibit a more compact frequency pattern and consistently reduced variability. With the mitigation algorithm: the range of energy consumption using Lora reduces 28.44% and using BLE-LoRa reduces 34.25%; the range of packet retransmission using Lora reduces 9.09% and using BLE-LoRa reduce 55.56%; the range of resilience using LoRa reduces 24.15% and using BLE-LoRa reduces a 20.47%.

It is possible to observe that the mean of the 10-minute rolling range is significantly lower, which indicates that the mitigation algorithm leads to a performance with fewer outliers by window. This rolling range reflects local variability, as it captures fluctuations within short time windows rather than across the entire dataset. With the mitigation algorithm: the mean of 10-minute rolling range of energy consumption using Lora reduces 20.96% and using BLE-LoRa reduces 21.37%; the mean of 10-minute rolling range of packet retransmission using Lora increases 3.70% and using BLE-LoRa reduce 41.83%; the mean of 10-minute rolling range of resilience using LoRa reduces 29.66% and using BLE-LoRa reduces a 22.65%.

In addition, the smoothed series range using the mitigation algorithm indicates that the time series are less volatile and exhibit fewer peaks of fluctuation. With the mitigation algorithm: the smoothed series range of energy consumption using Lora reduces 67.39% and using BLE-LoRa reduces 55.74%; smoothed series range of packet retransmission using Lora reduces 28.39% and using BLE-LoRa reduce 58.48%; smoothed series range of resilience using LoRa reduces 30.51% and using BLE-LoRa reduces a 23.86%.

On the other hand, the central tendency measures, mean and median, show that the time series generated using the mitigation algorithm not only have lower variance but are also positioned below those generated in simple mode. These differences are evaluated with a hypothesis test in the following sections.

With the use of the mitigation algorithm with the Bluetooth protocol, the resilience of the network improved; however, energy consumption and packet retransmissions increased slightly. Unlike other metrics and protocols, both the mean and median values of energy consumption and packet retransmissions were higher when the mitigation algorithm was applied. Furthermore, the standard deviation, range, and mean rolling range of energy consumption were greater under the mitigation mode compared to the simple mode when using Bluetooth. It can also be observed that the range of the smoothed series when using Bluetooth is surprisingly much smaller (63.64%) under the mitigation algorithm compared to the simple mode. This suggests that the mitigation algorithm exhibits frequent high and low peaks over time, yet most of its values remain tightly clustered around a central level.

This behavior in the BLE-only configuration reflects protocol-specific trade-offs. BLE operates with short-range, low-latency connections and frequent control exchanges. Under mitigation, additional clustering coordination and role reassignment messages increase control traffic, which in turn raises energy consumption and retransmissions. However, this overhead enables faster recovery from reactive jamming, resulting in improved resilience despite the increased resource usage. The observed trade-off in the BLE-only configuration arises from protocol-specific design

characteristics. BLE prioritizes low-latency communication and frequent control exchanges. Under mitigation, adaptive clustering introduces additional coordination traffic, including cluster-head negotiation and role updates. While this overhead increases energy consumption and retransmissions, it enables faster detection of interference and quicker recovery from reactive jamming, resulting in improved resilience. In essence, BLE trades energy efficiency for responsiveness and robustness. This trade-off can be mitigated through parameter tuning. Increasing the topology re-evaluation period (T), raising the residual energy threshold (ET_e), or relaxing the jamming sensitivity thresholds (JT_r, JT_x) would reduce the frequency of clustering updates and control messaging, thereby lowering energy consumption and retransmission overhead. Such tuning would slightly reduce responsiveness to interference but may be preferable in energy-constrained BLE deployments where jamming intensity is moderate. These parameters therefore provide explicit control knobs to balance energy efficiency and resilience according to application requirements.

These results highlight that mitigation effectiveness must be interpreted in a technology-aware manner. In long-range and lower-duty-cycle protocols such as LoRa, clustering reduces channel contention and retransmissions, leading to simultaneous gains in energy efficiency and resilience. In contrast, BLE prioritizes latency and responsiveness, and the same mitigation strategy introduces additional coordination overhead that increases energy usage while still enhancing robustness.

Unlike simulation-based studies that compare multiple algorithms under idealized assumptions, this work focuses on experimental validation under controlled reactive jamming. The baseline configuration without mitigation serves as an experimental equivalent to conventional non-adaptive clustering or routing approaches widely reported in the literature. Therefore, the comparative figures presented in this section illustrate the performance gains of the proposed method relative to existing baseline strategies, while Table 1 contextualizes these gains with respect to representative algorithms from prior work. Figure 21 provides a conceptual comparison between the proposed adaptive clustering and jamming mitigation algorithm and representative classes of existing approaches commonly reported in the literature. Conventional static routing and duty-cycling schemes correspond to baseline operation without explicit jamming awareness, while traditional clustering methods introduce energy optimization but lack adaptive response to reactive interference. More recent machine learning-based solutions typically rely on simulation environments and offline training, which can introduce significant computational overhead and limit deployability in resource-constrained sensor nodes. In contrast, the proposed approach integrates protocol-aware

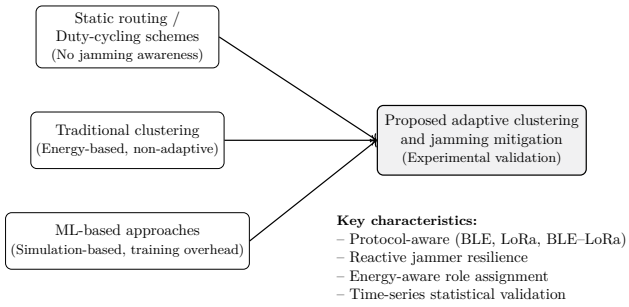


Fig. 21 Comparative positioning of the proposed adaptive clustering and jamming mitigation algorithm with respect to representative classes of existing approaches. Baseline non-mitigated operation corresponds to conventional static routing or duty-cycling schemes, while the proposed method introduces adaptive clustering and multi-metric decision-making validated through experimental measurements

adaptive clustering and multi-metric decision-making and is validated through real-world experimental measurements under reactive jamming. The figure highlights how the proposed method positions itself between lightweight baseline strategies and simulation-heavy learning-based solutions, offering a practical balance between energy efficiency, resilience, and experimental realism.

4.2 Correlation and dependency results for multivariate time series

The correlation analysis in this section is intended as an exploratory assessment of inter-metric dependency rather than as an inferential time-series modeling exercise. Given that the evaluated variables correspond to temporally correlated time series, special care was taken to avoid misinterpretation due to autocorrelation or spurious correlation effects.

All analyzed series were visually inspected and statistically characterized in preceding sections, confirming the absence of long-term trends or common non-stationary components that could induce artificial correlations. Moreover, the experimental conditions were strictly controlled, with all metrics measured simultaneously under identical network states, thereby minimizing the influence of external confounding factors.

Under these conditions, Pearson correlation coefficients are used solely to quantify the degree of linear association between metrics at the same time scale, not to infer causality or dynamic lead–lag relationships. More advanced time-series dependency analyses, such as cross-correlation functions or vector autoregressive models, are beyond the scope of this study and are identified as promising directions for future work.

In multivariate time series of Bluetooth communication technology (with a mitigation algorithm and simple mode),

there is a low correlation ($|\rho| < 0.1$) between energy, resilience and retransmissions, suggesting orthogonal behavioral patterns. For LoRa communication, Both mitigation and non-mitigation scenarios exhibit low absolute correlations ($|\rho| < 0.1$), confirming that energy, resilience, and retransmissions evolve independently, likely due to internal decoupling mechanisms. BLE-LoRa topology Observed correlations remain minimal in both configurations ($|\rho| < 0.05$), implying that energy usage, resilience, and retransmissions evolve independently.

4.3 Results of hypothesis testing on a univariate time series

Given that the evaluated performance metrics correspond to high-resolution time-series data, consecutive observations are inherently temporally dependent. As a result, applying classical hypothesis tests directly to raw time-series samples would violate the assumption of independent observations and potentially inflate Type I error rates. To address this issue, a block-aggregation strategy was adopted prior to inferential testing. Each univariate time series was partitioned into non-overlapping time blocks of 10 minutes (600 seconds), and the mean value within each block was computed. This approach substantially reduces temporal autocorrelation and yields approximately independent observations while preserving systematic differences between mitigation and non-mitigation conditions. Normality of the block-aggregated samples was re-evaluated using the Kolmogorov–Smirnov test, confirming non-Gaussian behavior across all metrics and protocols. Consequently, the Mann–Whitney U test was applied to compare the distributions of block-level measurements obtained under the mitigation algorithm and under simple (non-mitigated) operation. Since multiple hypothesis tests were conducted across different communication protocols and performance metrics, the Holm–Bonferroni procedure was applied to adjust p-values and control the family-wise error rate. This correction ensures robust statistical inference while retaining greater power than the classical Bonferroni method.

The adopted block-aggregation strategy constitutes a time-series aware inference approach analogous to block permutation or block bootstrap methods commonly used to handle autocorrelated data. By aggregating observations into non-overlapping 10-minute blocks, temporal dependence within blocks is preserved while enabling valid between-condition comparisons at the block level. This approach avoids pseudoreplication and prevents inflation of Type I error rates that would arise from treating raw sequential samples as independent.

Table 6 shows the results of Kolmogorov test on the univariate time series of device 1. If the p-value of the results is lower than 0.05 the null hypothesis is annulled and the data do not follow a normal distribution. All p-values reported as < 0.001 correspond to values below the numerical precision threshold of the statistical software and are reported following standard statistical reporting conventions. Consequently, a Mann-Whitney rank sum test was performed, which showed that all univariate time series generated using the mitigation algorithm exhibit significant differences compared to those generated in simple mode (see Table 6). In Table 7, if the p-value is lower than 0.05, the time series show a statistically significant difference.

Normality tests are reported for completeness; however, inferential analyses explicitly account for temporal dependence through block aggregation, as described below.

The test results, reported in Table 7, indicate that the observed differences between mitigation and non-mitigation scenarios remain statistically significant after accounting for both temporal dependence and multiple comparisons.

Table 6 Kolmogorov–Smirnov normality test results for univariate time series of Device 1

Time series	p-value	Interpretation
BLE-mit-energy	< 0.001	Not normally distributed
BLE-simple-energy	< 0.001	Not normally distributed
BLE-mit-retx	< 0.001	Not normally distributed
BLE-simple-retx	< 0.001	Not normally distributed
BLE-mit-res	< 0.001	Not normally distributed
BLE-simple-res	< 0.001	Not normally distributed
LoRa-mit-energy	< 0.001	Not normally distributed
LoRa-simple-energy	< 0.001	Not normally distributed
LoRa-mit-retx	< 0.001	Not normally distributed
LoRa-simple-retx	< 0.001	Not normally distributed
LoRa-mit-res	< 0.001	Not normally distributed
LoRa-simple-res	< 0.001	Not normally distributed
BLE-LoRa-mit-energy	< 0.001	Not normally distributed
BLE-LoRa-simple-energy	< 0.001	Not normally distributed
BLE-LoRa-mit-retx	< 0.001	Not normally distributed
BLE-LoRa-simple-retx	< 0.001	Not normally distributed
BLE-LoRa-mit-res	< 0.001	Not normally distributed
BLE-LoRa-simple-res	< 0.001	Not normally distributed

Table 7 Mann–Whitney U test results based on 10-minute block-aggregated samples comparing mitigation and simple modes. P-values are adjusted using the Holm–Bonferroni correction. Effect sizes correspond to rank-biserial correlation values

Protocol and metric	Adjusted p-value	Interpretation
BLE-energy	< 0.05	Significant difference
BLE-retx	< 0.05	Significant difference
BLE-res	< 0.05	Significant difference
LoRa-energy	< 0.05	Significant difference
LoRa-retx	< 0.05	Significant difference
LoRa-res	< 0.05	Significant difference
BLE-LoRa-energy	< 0.05	Significant difference
BLE-LoRa-retx	< 0.05	Significant difference
BLE-LoRa-res	< 0.05	Significant difference

In addition to statistical significance, effect sizes were quantified using the rank-biserial correlation associated with the Mann–Whitney U test. Across all metrics and communication protocols, effect sizes were consistently large, indicating that the observed differences between mitigation and non-mitigation scenarios are not only statistically significant but also practically meaningful in terms of energy efficiency, retransmission reduction, and resilience enhancement.

Accordingly, reported p-values reflect block-level inference rather than pointwise time-series testing and are interpreted in conjunction with effect sizes to assess both statistical and practical significance.

Table 8 reports inter-device summary statistics computed across all nine sensor nodes. For each device, time-series data were first aggregated into non-overlapping 10-minute blocks to account for temporal dependence. A single block-level mean was then computed per device, and the reported values correspond to the mean and standard deviation of these device-level summaries.

The small standard deviations observed across all metrics indicate low between-device variability, confirming that the network exhibits highly consistent behavior across nodes. These results provide quantitative evidence that Device 1 is representative of overall network behavior and that the observed performance differences between mitigation and non-mitigation modes are not driven by a single node or hardware-specific effects.

Inter-device variability was consistently lower than temporal variability, indicating that performance differences are dominated by operating mode rather than by node-specific characteristics.

4.4 Interpretation and trade-off modeling

The performance results of the sensor network with and without the mitigation algorithm show that the network gains stability over time when the mitigation algorithm is applied. When comparing the metrics range, standard deviation, smoothed series range, and mean rolling window range, these values are more compact for energy consumption, resilience, and packet retransmission when using the mitigation algorithm with Bluetooth, LoRa, and Bluetooth-LoRa, except for energy consumption with Bluetooth. A lower variance implies fewer fluctuations, which leads to a more reliable and predictable network. Additionally, the following insights were found regarding the communication protocol.

Table 8 Inter-device summary statistics (mean ± standard deviation across nine devices) for block-aggregated metrics under mitigation and non-mitigation modes (BLE network)

Metric	Mitigation	Simple
Energy (J)	0.6468 ± 0.0013	0.5518 ± 0.0005
Retransmissions (pkts)	5.5274 ± 0.0023	4.5663 ± 0.0023
Resilience (ms)	7.9137 ± 0.0008	8.5163 ± 0.0016

The comparative evaluation in this study focuses on contrasting the proposed mitigation algorithm against a non-mitigated baseline operating under identical jamming conditions. This baseline reflects the default behavior of many deployed WSNs that lack adaptive jamming-aware mechanisms.

The objective of this comparison is not to claim global optimality, but to quantify the practical performance gains achievable through a lightweight and deployable mitigation strategy. Comparisons against alternative mitigation approaches or industry benchmarks represent valuable future work, particularly when considering protocols with different hardware requirements or computational assumptions.

The mathematical modeling reveals a critical trade-off using Bluetooth:

- BLE-mit improves **resilience** under attack but incurs **higher retransmission** costs.
- BLE-simple maintains **energy efficiency** at the expense of **resilience** and reliable delivery.

These dynamics are essential for designing BLE networks in environments prone to intentional interference. Our model supports the idea that resilience and delivery assurance must be actively managed through adaptive algorithms even at the cost of energy overhead.

Using LoRa we observe a significant enhancement in resilience with mitigation, accompanied by:

- Lower mean energy consumption due to more efficient channel usage.
- Reduced retransmission rates, enhancing network throughput.

Thus, the implementation of mitigation in LoRa achieves superior operational stability with improved resource utilization. These improvements are particularly relevant in adversarial or noisy environments where communication assurance is critical.

Using BLE-LoRa Key trade-offs revealed include:

- Mitigation reduces energy consumption while increasing retransmissions, balancing delivery assurance with efficiency.
- The slight decrease in resilience under mitigation may stem from aggressive channel switching or protocol adaptation overheads.
- Heterogeneous networks benefit from dynamic redundancy but face tuning complexity in adversarial environments.

5 Discussion

This study has undertaken a rigorous statistical and mathematical examination of the performance of BLE, LoRa, and heterogeneous BLE-LoRa wireless sensor networks under jamming conditions, both with and without mitigation algorithms. The core methodology was based on descriptive statistics, correlation analysis, and signal smoothing techniques, applied consistently across three essential performance metrics: energy consumption, resilience, and retransmissions.

Descriptive statistics provided a foundational understanding of the system behavior by quantifying the central tendency and dispersion of the data. This allowed for an immediate comparison between mitigation and non-mitigation modes, revealing that mitigation strategies generally reduce energy consumption (especially in heterogeneous BLE-LoRa networks), increase retransmissions (a necessary trade-off for preserving communication), and vary in their effect on signal resilience depending on the technology used. These insights are not only informative but also essential for selecting network configurations in mission-critical applications where energy and delivery assurance must be balanced.

The use of Pearson correlation matrices provided a descriptive indication of inter-metric independence rather than evidence of dynamic or causal relationships. The observed low correlations across all technologies and configurations indicated that the metrics evolve independently. This supports the design principle that energy, reliability, and communication overhead can be independently optimized in a well-engineered WSN protocol stack. Such independence is particularly desirable in dynamic or adversarial environments where adaptive reconfiguration is necessary.

Furthermore, the application of the Moving Average for temporal smoothing was instrumental in uncovering latent patterns within the noisy datasets. This smoothing technique preserved the integrity of local minima and maxima, allowing for the visualization of energy or retransmission spikes due to algorithmic adaptation. It offered a clear contrast between steady-state behavior under jamming (simple modes) and reactive behavior under mitigation, further validating the utility of adaptive hybrid protocols in BLE-LoRa networks.

From a modeling perspective, all data were structured into multivariate time series models, establishing a clear mathematical framework that enables not only descriptive and comparative analysis but also predictive forecasting through autoregressive methods. The inclusion of potential extensions such as Vector AutoRegression (VAR) models provides a pathway toward real-time system monitoring and anticipatory control in IoT environments.

Critically, this framework highlights the nuanced trade-offs involved in jamming mitigation: while mitigation mechanisms introduce retransmission overhead, they significantly reduce energy waste and maintain network operability. In hybrid BLE-LoRa networks, these effects are even more pronounced, revealing the potential of heterogeneous architectures to dynamically exploit multiple communication layers for optimal performance.

6 Conclusion

This study confirms the strategic advantage of integrating hybrid BLE–LoRa architectures with adaptive clustering analytics to enhance the resilience and energy efficiency of wireless sensor networks operating under reactive jamming threats. The empirical results from multivariate time-series modeling, statistical hypothesis testing, and signal smoothing techniques provide compelling evidence that the proposed mitigation algorithm significantly reduces energy variance and packet retransmissions while improving signal robustness. Notably, the hybrid BLE-LoRa configuration demonstrated superior adaptability, leveraging the complementary strengths of both protocols to sustain communication under interference with minimal energy cost.

The experimental results demonstrate that the proposed adaptive clustering and jamming mitigation algorithm provides measurable efficiency and resilience gains under reactive jamming. In LoRa-only and hybrid BLE–LoRa networks, the mitigation strategy reduced energy consumption variability by up to 23.4% and 20%, respectively, while packet retransmission variability was reduced by up to 13.36% in LoRa and 43% in BLE–LoRa configurations. Additionally, resilience metrics showed faster recovery from jamming-induced disruptions, with resilience variability reduced by more than 30% in LoRa-based scenarios. These improvements were consistently observed across devices and validated using time-series aware statistical analysis.

The experimental results demonstrate that the proposed mitigation algorithm enhances network resilience across all evaluated technologies, while its impact on energy consumption and retransmissions depends on protocol characteristics. LoRa-only and hybrid BLE–LoRa networks benefit from simultaneous improvements in efficiency and robustness, whereas BLE-only networks exhibit a trade-off in which resilience gains are achieved at the expense of increased control overhead and energy usage. These findings underscore the importance of protocol-aware mitigation design in heterogeneous WSNs.

Compared to existing clustering and jamming mitigation approaches reported in the literature, the proposed work achieves higher practical efficiency by combining three distinguishing features: (i) experimental validation on a real heterogeneous BLE–LoRa testbed rather than simulation-only evaluation, (ii) lightweight, rule-based adaptivity that

avoids training overhead and high computational cost, and (iii) protocol-aware clustering that explicitly accounts for the differing energy, latency, and control characteristics of BLE and LoRa technologies. While many prior works optimize energy or security metrics in isolation, the proposed approach demonstrates a balanced improvement in energy efficiency, retransmission stability, and resilience under realistic reactive jamming conditions.

Importantly, the results reveal that efficiency gains are protocol-dependent rather than uniform. BLE-only networks exhibit a trade-off in which resilience is improved at the cost of moderate control overhead, whereas LoRa-only and hybrid BLE–LoRa architectures benefit from simultaneous reductions in energy consumption, retransmissions, and variability. This nuanced behavior highlights the advantage of the proposed approach over generic clustering schemes, as it enables adaptive, technology-aware mitigation rather than assuming homogeneous network behavior.

This positioning is further illustrated in Fig. 21, which contextualizes the proposed method with respect to simulation-based, static, and traditional clustering approaches commonly reported in the literature.

From a practical perspective, the proposed approach enables network designers to explicitly trade energy efficiency for resilience when operating under reactive jamming. In LoRa and hybrid BLE–LoRa networks, mitigation provides simultaneous gains in efficiency and robustness, making it suitable for long lived sensing applications. In BLE-centric deployments, the observed trade-off highlights that resilience improvements are achievable at the cost of additional control overhead, which can be tuned through system parameters. This flexibility distinguishes the proposed method from existing static or simulation-only approaches and supports its adoption in real-world heterogeneous WSN scenarios.

Crucially, the incorporation of artificial intelligence for anomaly detection and real-time role reassignment within the network marks a paradigm shift in proactive sensor monitoring. By enabling predictive adaptation through historical and live data streams, the AI-enhanced framework transforms static sensor networks into self-optimizing systems capable of mitigating threats autonomously. This approach not only improves operational stability but also sets the groundwork for future intelligent infrastructures in mission-critical domains such as smart cities, healthcare, and industrial automation. The findings underscore the necessity of embedding AI at the core of resilient WSN design, moving beyond traditional reactive strategies to achieve robust, anticipatory network behavior.

Author Contributions Carolina Del-Valle-Soto and Ramón A. Briseño led the conceptualization, methodology development, and formal analysis of the study. They were also primarily responsible for drafting the original manuscript and overseeing the integration of artificial intelligence into the sensor monitoring framework. Leonardo J. Valdivia contributed significantly to data curation, software implementation, and validation procedures. José Varela-Aldás supported the investigation and visualization stages, offering key insights during the analysis and interpretation of results. Paolo Visconti assisted with resource coordination and provided technical input during the development of the system. The overall supervision and project management were conducted by Carolina Del-Valle-Soto. All authors contributed to the review and editing of the final manuscript and approved its submission.

Funding Not applicable

Data Availability Data is provided within the manuscript or supplementary information files in https://drive.google.com/drive/folders/1x3zdRhLu53en-8zmXmi4VQIU7GcTE4ih?usp=drive_link.

Materials Availability Not applicable

Code Availability Not applicable.

Declarations

Ethical Approval Not applicable

Consent for Publication Not applicable

Competing interests The authors declare no competing interests.

Conflicts of Interest The authors declare that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

References

1. Verma R (2022) Smart city healthcare cyber physical system: characteristics, technologies and challenges. Wireless Pers Commun 122(2):1413–1433
2. Pundir A, Singh S, Kumar M, Bafila A, Saxena GJ (2022) Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era. IEEe Access 10:16350–16364
3. Nguyen TG, So-In C, Ha D-B et al (2017) Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer. IEEE Access 5:25196–25206. https://doi.org/10.1109/ACCESS.2017.2768081
4. Zanaj E, Caso G, De Nardis L, Mohammadpour A, Alay Ö, Di Benedetto M-G (2021) Energy efficiency in short and wide-area

IoT technologies–a survey. Technologies 9(1):22. https://doi.org/10.3390/technologies9010022
5. Bolivar IMM (2021) Jamming on LoRaWAN networks: from modelling to detection. PhD thesis, Institut National des Sciences Appliquées de Rennes
6. Effah E, Ghartey G, Aidoo JK, Thiare O (2024) Hardware development and evaluation of multihop cluster-based agricultural IoT based on bluetooth low-energy and LoRa communication technologies. Sensors 24(18):6113. https://doi.org/10.3390/s24186113
7. Sreekantha B, Shaila K (2024) Exploring the synergy of machine learning algorithms in wireless sensor networks: A comprehensive survey. In: International conference on intelligent electrical systems and industrial automation, pp 45–57. Springer
8. Paolone G, Iachetti D, Paesani R, Pilotti F, Marinelli M, Di Felice P (2022) A holistic overview of the internet of things ecosystem. IoT 3(4):398–434. https://doi.org/10.3390/iot3040022
9. Jameel F, Wyne S, Kaddoum G, Duong TQ (2018) A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun Surv Tutor 21(3):2734–2771. https://doi.org/10.1109/COMST.2018.2880776
10. Bandara HD, Jayasumana AP (2013) Collaborative applications over peer-to-peer systems-challenges and solutions. Peer-to-Peer Netw Appl 6:257–276. https://doi.org/10.1007/s12083-012-0162-9
11. Muzakkari BA, Mohamed MA, Kadir MF, Mohamad Z, Jamil N (2018) Recent advances in energy efficient-QoS aware MAC protocols for wireless sensor networks. Intern J Adv Comput Res 8(38):212–228. https://doi.org/10.19101/IJACR.2018.838007
12. Al-Husseini ZSM, Chaiel HK, Meddeb A, Fakhfakh A (2024) A detailed review of wireless sensor network, jammer, the types, location, detection and countermeasures of jammers. SOCA 18(3):225–247. https://doi.org/10.1007/s11761-023-00411-7
13. Ram GM, Ilavarasan E (2024) Security challenges in wireless sensor network: Current status and future trends. Wireless Personal Commun 1–30. https://doi.org/10.1007/s11277-024-11034-5
14. Lavanya A, Udhayakumar P, Rajkumar K, Revathi S (2023) Investigations on jamming and black hole attacks in wireless sensor networks: An industrial case study. In: International conference on 6G communications networking and signal processing, pp 373–378. https://doi.org/10.1007/978-3-031-47966-3_35. Springer
15. Abdulhae OT, Mandeep JS, Islam M (2022) Cluster-based routing protocols for flying ad hoc networks (FANETs). IEEE Access 10:32981–33004. https://doi.org/10.1109/ACCESS.2022.3161823
16. Mujahid MA, Bakar KA, Darwish TS, Zuhra FT (2021) Cluster-based location service schemes in VANETs: current state, challenges and future directions. Telecommun Syst 76(3):471–489. https://doi.org/10.1007/s11235-020-00713-9
17. Lonkar BB, Karmore S (2024) BCEWN: design of a hybrid bio-inspired clustering model for deployment of energy-aware wireless networks. Wireless Pers Commun 136(4):2329–2358. https://doi.org/10.1007/s11277-023-11063-2
18. Lonkar B, Kuthe A, Charde P, Dehankar A, Kolte R (2025) Optimal hybrid energy-saving cluster head selection for wireless sensor networks: an empirical study. Peer-to-Peer Netw Appl 18(4):182. https://doi.org/10.1007/s12083-024-01663-4
19. Lonkar B, Karmore S (2022) Statistical evaluation of power-aware routing protocols for wireless networks: An empirical study. Intern J Intell Inf Technol (IJIIT) 18(3):1–14. https://doi.org/10.4018/IJIIT.2022070101
20. Lonkar BB, Karmore S (2025) EBBSMWN: design of an energy-aware blockchain-based bioinspired security model of wireless networks. Int J Inf Comput Secur 28(2):227–248. https://doi.org/10.1504/IJICS.2025.135741
21. Lonkar B, Charde P, Kuthe A, Dehankar A, Dandekar P, Puri N, Banabakode D (2026) A review of hybrid clustering and routing protocols for the hotspot problem in wireless sensor networks. Peer-to-Peer Netw Appl 19(1):8
22. Del-Valle-Soto C, Valdivia LJ, Velázquez R, Del-Puerto-Flores JA, Varela-Aldás J, Visconti P (2025) Adaptive jamming mitigation for clustered energy-efficient LoRa-BLE hybrid wireless sensor networks. Sensors 25(6):1931. https://doi.org/10.3390/s25061931
23. Said G, Ghani A, Ullah A, Azeem M, Bilal M, Kwak KS (2022) Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks. IEEE Access 10:33571–33585. https://doi.org/10.1109/ACCESS.2022.3163067
24. Aras E (2021) Security and reliability for emerging IoT networks
25. Mustafa R, Sarkar NI, Mohaghegh M, Pervez S (2024) A cross-layer secure and energy-efficient framework for the Internet of Things: a comprehensive survey. Sensors (Basel Switzerland) 24(22):7209
26. Dashtestani KBZ, Javidan R, Akbari R (2025) Dynamic clustering method for underwater wireless sensor networks based on deep reinforcement learning. J Marine Sci Appl 1–13. https://doi.org/10.1007/s11804-024-00405-7
27. Hasan MK, Alkhalifah A, Islam S, Babiker NB, Habib AA, Aman AHM, Hossain MA (2022) Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wirel Commun Mob Comput 2022(1):9065768. https://doi.org/10.1155/2022/9065768
28. Loscri V, Symeonidis I, Griesbacher M, Deniau V, Andreoletti D, Chiumento A, Dimitrova V, Corradini I, Aden H, Moritz M et al (2025) Interdisciplinary security aspects of next-generation wireless networks and systems: Being-wise: State of research and future research steps
29. Priyadarshani R, Park K-H, Ata Y, Alouini M-S (2024) Jamming intrusions in extreme bandwidth communication: A comprehensive overview. arXiv:2403.19868
30. Ranaweera P, Jurcut A, Liyanage M (2021) MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures. ACM Comput Surv (CSUR) 54(9):1–37. https://doi.org/10.1145/3471099
31. Wei X, Wang Q, Wang T, Fan J (2016) Jammer localization in multi-hop wireless network: A comprehensive survey. IEEE Commun Surv Tutor 19(2):765–799. https://doi.org/10.1109/COMST.2016.2627239
32. Mao W, Zhao Z, Chang Z, Min G, Gao W (2021) Energy-efficient industrial internet of things: Overview and open issues. IEEE Trans Industr Inf 17(11):7225–7237. https://doi.org/10.1109/TII.2020.3047021
33. Khatami SS, Shoeibi M, Salehi R, Kaveh M (2025) Energy-efficient and secure double RIS-aided wireless sensor networks: A QoS-aware fuzzy deep reinforcement learning approach. J Sens Actuator Netw 14(1):18. https://doi.org/10.3390/jsan14010018
34. Batista E, Moncusi MA, López-Aguilar P, Martínez-Ballesté A, Solanas A (2021) Sensors for context-aware smart healthcare: A security perspective. Sensors 21(20):6886. https://doi.org/10.3390/s21206886

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.