applied sciences

MDPI

Article

Securing IoT Networks Against Wireless DoS Attacks via Energy Harvesting Relays

Mohammad Alkhawatrah [1] and Saleh Almahmoud [2,*]

[1] Department of Communications and Computer Engineering, Al-Ahliyya Amman University, Amman 19111, Jordan; m.alkhawatrah@ammanu.edu.jo
[2] Department of Electrical Engineering, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
* Correspondence: almahmooud@imamu.edu.sa

Abstract

This paper addresses the critical challenge of securing next-generation green wireless Internet of Things (IoT) networks against malicious physical-layer jamming attacks. Traditional opportunistic relay selection schemes, such as the conventional max-min, optimize routing paths based strictly on instantaneous channel conditions. However, this channel-only focus disregards the underlying energy states of candidate nodes, introducing an energy-starvation vulnerability, and severely degrades the network's overall secrecy and reliability. To counter this threat, we propose a robust two-stage selection mechanism engineered to provide resilient physical-layer security. In the first stage, the proposed protocol dynamically isolates energy-depleted relays, restricting the selection domain exclusively to a subset of verified, energy-sufficient candidates. In the second stage, the mechanism optimizes the final path selection by identifying the relay that maximizes the channel quality while explicitly accounting for the interference injected by the jammer. Analytical derivations and simulation results demonstrate that while traditional max-min schemes suffer from catastrophic outage floors and early throughput saturation in jamming environments, the proposed framework successfully eliminates these performance ceilings. The results confirm that the two-stage mechanism fully preserves the network's spatial diversity order, allowing the system to leverage the available relays to effectively neutralize aggressive jamming interference. Furthermore, the performance of the relay-assisted architecture is verified to be superior to that of the non-cooperative direct transmission across jamming environments.

Keywords: IoT security; jamming; physical layer security; relay selection; energy harvesting

Check for updates

Academic Editors: Mah-Rukh Fida and Giuseppe Caso

Received: 18 August 2026
Revised: 3 September 2026
Accepted: 17 September 2026
Published: 20 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Wired communication systems provide strong resilience against environmental noise and adversarial attacks, but their deployment is constrained by high maintenance costs and poor scalability. While wireless technologies like the Internet of Things (IoT) solve these infrastructure limits and have become ubiquitous, they remain significantly more vulnerable to reliability degradation and security weaknesses [1]. IoT has rapidly emerged as a dominant paradigm for achieving massive connectivity and realizing the vision of smart cities [2], driven by the extensive deployment of physical objects such as sensors, controllers, and actuators. However, securing these IoT architectures presents severe challenges due to the inherent broadcasting nature of the wireless medium and the strict energy constraints

of the deployed devices. Consequently, implementing robust security protocols within large-scale, resource-constrained IoT networks remains a critical bottleneck [3]. Despite significant advancements in wireless technologies over recent decades, the open nature of the wireless medium leaves modern networks inherently vulnerable to radio jamming attacks [4]. Jamming is defined as the intentional emission of electromagnetic energy directed toward a communication system to disrupt or completely prevent successful signal transmission. As a critical subset of Denial-of-Service (DoS) attacks, jamming aims to block communication between legitimate nodes [5] by flooding the shared spectrum with disruptive interference, such as white noise, to inhibit normal network management and data transfer [6].

The simplicity of launching these attacks underscores the urgency of securing wireless networks against intentional interference. With rapid advancements in software-defined radio (SDR) technology, an attacker can easily configure a low-cost, commercial-off-the-shelf USB SDR dongle to act as an effective jammer. Such a device can disrupt standard Wi-Fi services in home or office environments by covering a 20 MHz bandwidth below 6 GHz with up to 100 mW of transmission power, matching the maximum transmit power limit for typical 35-m indoor Wi-Fi hardware [7]. For instance, performance analysis of Wi-Fi networks operating on the 2.4 GHz band, which contains only three non-overlapping 20 MHz channels, demonstrated that a basic jammer could degrade aggregate network throughput by more than 65% [8].

Conventional security solutions relying on complex cryptographic techniques are often impractical for wireless IoT networks due to the stringent computational constraints of the deployed hardware [9]. Furthermore, traditional cryptographic schemes require rigorous key management frameworks to securely exchange secret keys between legitimate entities. Such key distribution architectures depend heavily on a centralized trusted entity, which cannot always be guaranteed in distributed, ad-hoc wireless deployments [10]. To address these limitations, Physical Layer Security (PLS) has emerged as a promising solution, exploiting the characteristics of the wireless channel to secure communications [11]. Consequently, PLS has been widely investigated both as a standalone alternative and as a complementary mechanism to upper-layer cryptographic methods [12]. For instance, while recent upper-layer frameworks such as the collaborative detection scheme in [13] focus on identifying reactive jamming threats by monitoring packet forwarding ratios, such approaches strictly perform threat detection rather than active transmission mitigation. Because jamming is inherently a physical (PHY) layer vulnerability, conventional defenses operating at the MAC layer or above are generally incapable of maintaining signal transmission during active interference, further highlighting the vital importance of physical-layer resilience.

A significant variety of PLS techniques have been developed to counteract radio jamming attacks. One fundamental approach is dynamic transmit power control; upon detecting a jamming attack, the source can scale up its transmit power to improve the legitimate links. However, this strategy accelerates energy depletion and is strictly constrained by the peak power capabilities of the hardware [6]. Another classic defense paradigm is spread spectrum technologies [14], primarily implemented via Frequency-Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS). While FHSS rapidly switches carrier frequencies to prevent tracking, it demands tight transceiver synchronization and remains vulnerable to wideband jammers. Conversely, DSSS suppresses interference by modulating data with a pseudo-random noise code across a wide bandwidth, yet its resilience degrades under high-power localized jamming [15]. Ultimately, the robustness of traditional spread spectrum architectures comes at the expense of spectral efficiency, making them not feasible for resource-constrained applications [16].

Spatial diversity techniques, particularly Multiple-Input Multiple-Output (MIMO) systems, offer an alternative path by exploiting independent spatial propagation paths. Through directional beamforming, MIMO transceivers can nullify interference or maximize array gain along legitimate paths [17]. For instance, experimental evaluations in [18] demonstrated that a MIMO network could successfully decode signals even when the jamming power was 20 dB stronger than the legitimate signal in a real-world implemented Wi-Fi network. Nevertheless, the sophisticated antenna arrays and precise channel estimation overhead required by MIMO systems introduce strict size, power and cost limitations, rendering them impractical for compact IoT nodes [19]. Extending the concept of spatial manipulation without the burden of multi-antenna arrays, recent literature has extensively explored Reconfigurable Intelligent Surfaces (RIS) to secure wireless communications against jamming attacks [19]. State-of-the-art RIS paradigms inherently formulate highly non-convex joint optimization problems [20]. Therefore, they involve complex mathematical formulations that are solved either by relaxing strict constraints as in [21,22] or via computationally heavy deep reinforcement learning approaches as [23]. High-dimensional channel matrix acquisition, coupled with the continuous computational burden of iterative phase-shift tuning, imposes severe operational challenges on resource-constrained IoT nodes. Furthermore, beyond the massive channel matrix acquisition overhead, Ref. [24] demonstrates that RIS architectures require large physical surface areas, which hinders device compactness in space-limited environments. Consequently, cooperative relaying has emerged as a well-established paradigm that allows single-antenna IoT devices to retain the spatial diversity benefits of MIMO and RIS architectures while bypassing their physical hardware, size constraints and signaling limitations [24–26]. Motivated by these cooperative capabilities, this paper proposes a relay selection mechanism designed to secure wireless links against malicious jamming. A comparison between the proposed framework and recent anti-jamming paradigms across key operational metrics is provided in Table 1.

Table 1. Comparison with recent anti-jamming paradigms.

Metric/Feature	Ashraf et al. [13]	Optimization-Based RIS Zhang et al. [21], and Chu, et al., [22]	DRL RIS Thanh et al. [23]	Cooperative Relaying (This Work)
Primary Objective	Threat Identification	Active Mitigation	Active Mitigation	Active Mitigation
Target Layer	Higher-layers	Physical (PHY)	Physical (PHY)	Physical (PHY)
Channel State Requirements	Not Applicable	High-Dimensional Matrix	High-Dimensional Matrix	Scalar
Processing Overhead	Low	High (Non-Convex)	High (DRL)	Low
Hardware Footprint	Compact	Large Surface	Large Surface	Single-Antenna/Compact

Furthermore, to ensure compatibility with green, energy-efficient IoT infrastructures, we incorporate energy-harvesting capability at the relay nodes. The key contributions of this work can be outlined as follows:

- A joint energy-harvesting and anti-jamming protocol is proposed. The two-stage relay selection mechanism incorporates node energy states to select the best anti-jamming relay.
- The mathematical analysis of the proposed framework over independent Rayleigh fading channels is presented. Specifically, we derive exact closed-form expressions for the ergodic system outage probability and effective throughput.
- We demonstrate both analytically and empirically that the proposed protocol completely eliminates the non-zero horizontal outage floors and early throughput plateaus that typically degrade the conventional max-min relay selection scheme.

- We validate that the proposed scheme achieves full diversity order. This confirms that the system's operational reliability scales monotonically with the number of relays, which overcomes the limitations of non-cooperative systems.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model. In Section 3, the analytical performance analysis is presented. Section 4 evaluates the performance of the proposed scheme. Finally, the paper conclusion is in Section 5.

2. System Model

In this paper, we propose an anti-jamming cooperative network with a source S, a destination D, a jammer J and K half-duplex (HF) decode-and-forward (DF) relay nodes denoted as R_k, $k = 1, \cdots, K$. Each relay is equipped with an energy buffer of capacity M, where e_k denotes the current state of charge (i.e., the number of charged energy slots available at relay R_k). The system model of the cooperative network under jamming attack is shown in Figure 1. The channel coefficients for the $S \to R_k$, $R_k \to D$, $J \to R_k$, and $J \to D$ links are denoted by h_{sr_k}, h_{r_kd}, h_{jr_k}, and h_{jd}, respectively. The Network is utilizing a Time Division Multiple Access (TDMA) structure. All channels are assumed to have flat Rayleigh fading coefficients that remain constant within the time-slot and change independently in different time slots. We assume that the source always has enough information for transmission in all time-slots. In each time-slot, a packet can be transmitted by the source via a relay, and information symbols intended for the destination are assembled into packets of equal size. Without losing generality, we assume that the transmit powers at all transmit nodes (source and relays) are P_t, and the noise variances at all receiving nodes are σ^2. The utilized relays do not employ data queues to avoid cumulative queuing delays entirely.

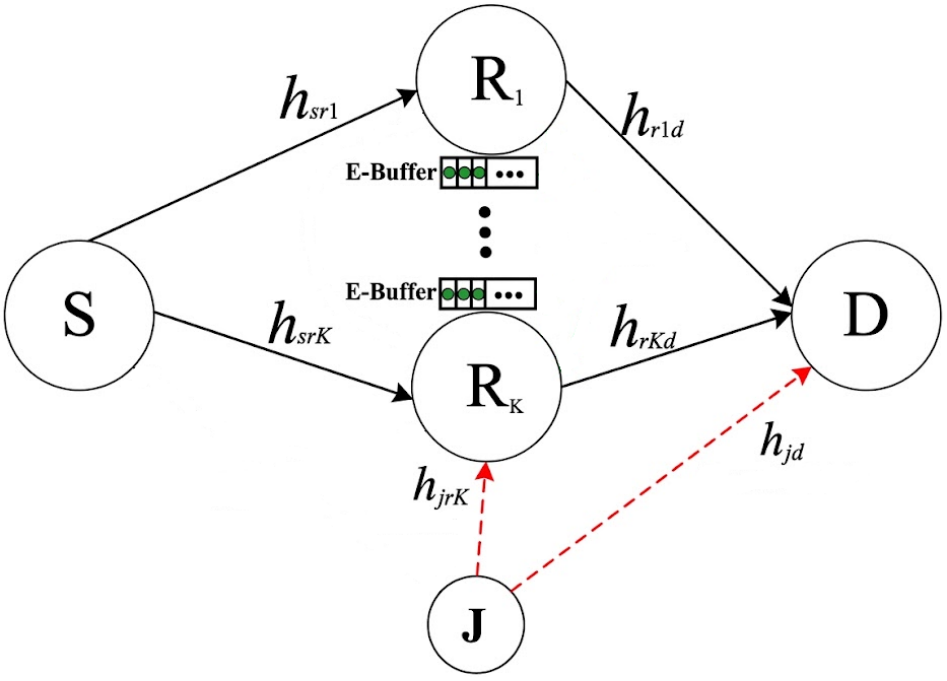


Figure 1. System model for anti-jamming cooperative network.

At time-slot t, the link capacity for channel $h_{sr_k}(t)$ is given by

$$C_{sr_k}(t) = \log_2\left(1 + \frac{\eta_{sr_k}(t)}{\eta_{jr_k}(t) + 1}\right), \quad k = 1, \cdots, K, \tag{1}$$

and the channel capacity for channel $h_{r_k d}(t)$ is

$$C_{r_k d}(t) = \log_2 (1 + \frac{\eta_{r_k d}(t)}{\eta_{jd}(t) + 1}), \quad k = 1, \cdots, K, \tag{2}$$

where

$$\eta_{sr_k}(t) = (P_t/\sigma^2)|h_{sr_k}(t)|^2,$$

and

$$\eta_{r_k d}(t) = (P_t/\sigma^2)|h_{r_k d}(t)|^2.$$

The jammer J causes interference at relays as well as at the destination, this is captured by

$$\eta_{jr_k}(t) = (P_j/\sigma^2)|h_{jr_k}(t)|^2,$$

and

$$\eta_{jd}(t) = (P_j/\sigma^2)|h_{jd}(t)|^2,$$

where P_j is the jammer transmitting power. Assuming $|h_{b_k}(t)|^2, b_k \in \{sr_k, r_k d, jr_k, jd\}$ is exponentially distributed with the average $\Theta_{b_k} = E[|h_{b_k}(t)|^2]$, where $E[.]$ is the expectation. $\eta_{b_k}(t)$ is also exponentially distributed with average calculated by replacing $|h_{b_k}(t)|^2$ with Θb_k. Thus, $\eta_{b_k}(t)$ and $\bar{\eta}_{b_k}$ are the instantaneous and average SNR for channel $h_{b_k}(t)$, respectively.

We assume that global CSI is available, which is a common assumption in the PHY security literature (see [27]). In practical energy-constrained IoT implementations, acquiring instantaneous global CSI introduces energy consumption as well as control signaling overhead. While perfect CSI is assumed in this study to establish theoretical performance and maintain benchmark parity with existing literature, real-world deployment can leverage statistical CSI models. As highlighted in recent embedded architecture studies [28], the design of distributed acquiring and processing systems must carefully balance acquisition accuracy with local hardware resource constraints. In our scheme, centralized CSI gathering requires $\mathcal{O}(K)$ control message exchanges per slot, whereas statistical CSI implementations can reduce messaging to a constant $\mathcal{O}(1)$ overhead, making the multi-relay framework scalable for larger node deployments.

Since $\eta_{sr_k}(t)$ and $\eta_{r_k d}(t)$ are exponentially distributed, the corresponding cumulative distribution functions, which represent the outage probability for each link, are expressed as $P(C_{sr_k}(t) < \epsilon)$ and $P(C_{r_k d}(t) < \epsilon)$ for $S \to R_k$ and $R_k \to D$, respectively; ϵ denotes the target data rate. Due to the presence of the jamming attack, the system performance is dictated by the signal-to-interference-plus-noise ratio (SINR). Consequently, the instantaneous outage event for an interference-limited link is defined as the condition where the received SINR falls below a predetermined transmission threshold $P\left(\frac{\eta_i}{1+\eta_j} < 2^\epsilon - 1\right)$, or thresholding on the SNR $P(\eta_i < (2^\epsilon - 1)(1 + \eta_j))$, where η_i represents the legitimate channels SNR ($S \to R_k$ and $R_k \to D$) and η_j denotes the corresponding jammer channels SNR ($J \to R_k$ and $J \to D$).

Towards realizing the energy efficiency requirements of 6G-IoT networks, energy harvesting relays are used in this study. As stated in [29], the contribution of noise to the harvested energy is considered negligible, given that the noise power typically falls below the sensitivity threshold of the energy harvesting circuitry. Energy harvesting and data decoding operate simultaneously across the network. The relay selected for data forwarding devotes its operation entirely to decoding and transmission, and thus, does not harvest energy during that slot. Concurrently, all unselected relays harvest energy. During the control phase, relays feed back a unified state vector comprising both their

energy buffer status and their CSI. The quantity of energy harvested by relay R_k from the source transmission during a single time-slot of duration t is expressed as [30]

$$E_k = \gamma P_t |h_{sr_k}|^2 t, \tag{3}$$

where $0 < \gamma < 1$ represents the efficiency of the energy conversion process. In practical green IoT systems, the continuous power captured by energy harvesting typically ranges from microwatts to nanowatts. To support milliwatt-level packet transmission, relays employ an accumulate-then-forward model [29]. This energy management aligns with practical green IoT architectures and real-world industrial control scenarios [31]. We exclude jammer-assisted energy harvesting in (3). This ensures a conservative performance lower bound, avoiding operational vulnerabilities against advanced reactive jammers that can intentionally cut its transmit power or remain completely silent during the energy harvesting phase, then turn on at maximum power exclusively during the information forwarding phase. Extending this framework to capture dynamic jammer-assisted harvesting is left for future work.

Relay Selection Scheme

In this work, we adopt the relay selection strategy proposed in [32], extending it to incorporate the effect of energy harvesting. The original max-min selects the optimal relay R^* via

$$R^* = \arg \max_{R_k} \min \left\{ |h_{srk}|^2, |h_{rkd}|^2 \right\}, \tag{4}$$

If R^* does not have enough energy to transmit the packet to the destination, an outage occurs. To avoid this, we use two-stage selection. In the first stage, we define the energy-sufficient relays (ESR) set, which contains the relays that can handle the transmission:

$$ESR = \{R_k | (e_k \geq 1)\}, \tag{5}$$

where at least one charged energy slot should be available at relay R_k to be considered for selection. In the second stage, the max-min in (4) is applied to the relays of ESR, accounting for the interference injected by the jammer:

$$R^* = \arg \max_{R_k \in ESR} \min \left\{ \frac{\eta_{srk}}{1 + \eta_{jrk}}, \frac{\eta_{rkd}}{1 + \eta_{jd}} \right\}. \tag{6}$$

This narrows the selection only to relays with sufficient energy. If two relays happen to have similar weak channels, i.e., more than one relay achieves R^*, we select one of them randomly. Throughout this paper, the terms relay selection scheme, selection strategy and relay selection protocol are used interchangeably to refer to the proposed physical-layer relay selection scheme.

3. Performance Analysis

3.1. Outage Probability

The end-to-end SINR for a given relay path in a DF network is constrained by its weakest link ($S \rightarrow R_k$ or $R_k \rightarrow D$). An outage occurs if the weakest link SNR of the selected relay R^* drops below the threshold ($(2^{\epsilon} - 1)(1 + \eta_j)$). Because the channels follow Rayleigh fading, the harvested energy profile inherits an exponential distribution (see (3)). The finite energy buffer is modeled as a one-dimensional, nearest-neighbor birth-death Markov chain. To apply general equilibrium (steady state) methodology in [33], we define the energy buffer's state space and flows, as any system is defined by its states and

the transition rates between them. The state space represents the discrete energy slots stored in the energy buffer. This formulation relies on the standard assumption that within any given time-slot, the buffer state can increment by at most one unit due to energy harvesting, or decrement by at most one unit due to packet transmission. The probability of harvesting an energy packet, denoted as p, represents the probability that the received energy at the relay during the harvesting phase is sufficient to fill one energy slot $p = \Pr(\gamma P_t |h_{srk}|^2 t \geq 1) = \Pr\left(|h_{sr}|^2 \geq \frac{1}{\gamma P_t t}\right)$. Under independent and identically distributed (i.i.d.) Rayleigh fading, the channel power gain $|h_{srk}|^2$ follows an exponential distribution with a mean of Θ_{srk}

$$p = \int_{\frac{1}{\gamma P_t t}}^{\infty} \frac{1}{\Theta_{srk}} e^{-\frac{x}{\Theta_{srk}}} \, dx = e^{-\frac{1}{\gamma P_t t \Theta_{srk}}}. \tag{7}$$

The probability of selecting a relay for transmission and losing one energy packet is $q = \frac{1}{n}$, where $n = |ESR|$. Due to the i.i.d. channel conditions, each of the n available candidate relays has an equal selection probability of $\frac{1}{n}$. Refstate spaceb32 shows that at steady state, the total probability flow leaving a state equals the total probability flow entering that state. For an intermediate state i: $\pi_i(p+q) = \pi_{i-1}p + \pi_{i+1}q$. Because energy transitions are restricted to nearest neighbors (a tridiagonal matrix structure), Ref. [33] proves that if local balance holds for every pair of adjacent states in a Markov chain, then global equilibrium is automatically achieved $\pi_i p = \pi_{i+1} q$, so $\pi_{i+1} = \lambda \pi_i$, where

$$\lambda = \frac{p}{q} = \frac{e^{-\frac{1}{\gamma P_t t \theta_{srk}}}}{1/n} = n e^{-\frac{1}{\gamma P_t t \theta_{srk}}}. \tag{8}$$

With this, we may express every single energy state as a geometric function of the empty buffer (starvation) state $\pi_i = \lambda^i \pi_0$, for $0 \leq i \leq M$. We focus on the starvation probability π_0 because it is the state that may cause an outage. The Markov chain must exist somewhere within its bounded state space: $\sum_{i=0}^{M} \pi_i = \lambda^i \pi_0 = 1$. Applying the algebraic identity for a finite geometric progression (where $\lambda \neq 1$), the series evaluates to:

$$\pi_0 = \frac{1-\lambda}{1-\lambda^{M+1}}. \tag{9}$$

By applying the law of total probability across all possible values of $|ESR|$, we get the total outage probability to be

$$\sum_{n=0}^{K} P(\text{Outage} \mid |ESR| = n) \cdot P(|ESR| = n). \tag{10}$$

Following established energy-harvesting relay literature, energy queue dynamics and instantaneous channel fading are treated as statistically independent to maintain tractability. The probability that exactly n out of K independent relays have sufficient energy follows a binomial distribution $P(|ESR| = n) = \binom{K}{n}(1-\pi_0)^n (\pi_0)^{K-n}$. For a single dual-hop path (Source $\rightarrow$ Relay $\rightarrow$ Destination), an outage happens if either the first hop fails or the second hop fails. The path experiences an outage if the instantaneous bottleneck SINR falls below the required threshold $2^{\epsilon} - 1$. The SNR threshold of the first hop is

$$Th_1 = (2^{\epsilon} - 1)(1 + \eta_{jr_k}),$$

and for the second hop

$$Th_2 = (2^{\epsilon} - 1)(1 + \eta_{jd}).$$

By evaluating the complementary cumulative distribution function of the links over Rayleigh fading channels, the conditional outage probability of the k-th dual-hop path, given a specific instantaneous jamming channel realization (η_{jr_k}, η_{jd}), is expressed as:

$$\mathcal{O}_k(\eta_{jr_k}, \eta_{jd}) = 1 - \exp\left(-\frac{Th1}{\Theta_{sr_k}} - \frac{Th2}{\Theta_{r_k d}}\right), \tag{11}$$

where $\mathcal{O}_k$ is the probability that the channels of relay R_k can not satisfy the threshold given that the relay has sufficient energy (i.e., $\mathcal{O}_k = P(\text{Outage} \mid R_k \in ESR)$). Based on the i.i.d channels assumption, the conditional dual-hop path outage probabilities across all relays: $\mathcal{O}_k(\eta_{jr_k}, \eta_{jd}) = \mathcal{O}(\eta_{jr_k}, \eta_{jd}), \forall k$. The system drops into a total channel outage if and only if all n energy-sufficient relays fail simultaneously. Thus, for a given realization $|ESR| = n$, the conditional system outage probability is $P(\text{Outage} \mid |ESR| = n) = \mathcal{O}^n$. Applying the law of total probability in (10) and then the binomial theorem, the conditional system outage probability for a given jamming realization is yielded as:

$$\left(\mathcal{O}(\eta_{jr_k}, \eta_{jd}) \cdot (1 - \pi_0) + \pi_0\right)^K. \tag{12}$$

Having a smaller K bounds spatial diversity, requiring a larger energy buffer M to suppress π_0 and maintain the target outage in (12). Conversely, a large K allows smaller buffers M to yield equivalent performance, as the joint probability of all K relays being simultaneously energy depleted decays rapidly. To capture the full ergodic performance across all channel dynamics, the final analytical expression can be obtained by numerically averaging (12) over the probability density functions of the independent Rayleigh fading jammer channels.

3.2. Diversity Order

The diversity order denoted as d reveals the average number of available links for selection at very high SNR, which shows the best potential performance of the network. The asymptotic behavior of p at high SNR $P_t \to \infty$:

$$\lim_{P_t \to \infty} p = \lim_{P_t \to \infty} e^{-\frac{1}{\gamma P_t \Theta_{srk}}} = e^0 = 1. \tag{13}$$

making $\lambda = K$. Because $K > 1$ for any multi-relay cooperative network, the denominator of π_0 grows exponentially, driving $\pi_0 \to 0$, which simplifies (12) to $\left[\mathcal{O}(\eta_{jr_k}, \eta_{jd})\right]^K$. Because the probability $\mathcal{O}(\eta_{jr_k}, \eta_{jd}) < 1$, raising it to the power of K suppresses the overall system outage probability by several orders of magnitude. For example, when $\lambda = K = 5$ and $M = 5$, according to (9), $\pi_0 = 2.6 \times 10^{-4}$. Consequently, as $P_t \to \infty$, $\mathcal{O}(\eta_{jr_k}, \eta_{jd}) \to 0$, which yields an overall system outage probability of zero and enables full spatial diversity $d = K$. In this study, the assumption is that the jammer behaves independently and is transmitting at constant power P_j. Hence, P_t completely dominates it asymptotically, preserving full diversity, which is going perfectly well with the findings in [34]. An adaptive jammer represents a more sophisticated threat, capable of counteracting an increase in transmit power P_t by proportionally scaling up its own jamming power P_j. This causes the system's diversity order to degrade to zero, resulting in a horizontal outage probability floor that prevents the network from achieving perfect reliability (0 outage probability). Nonetheless, cooperative networks can still offer valuable coding gains under such conditions. The analysis of adaptive jamming strategies falls outside the scope of this work and is deferred to future research.

3.3. Throughput Analysis

In the delay-limited transmission framework [35], the source transmits at a fixed, constant target data rate $\mathcal{R}$, and the system cannot adapt its rate to the channel. Therefore, the throughput is strictly binary: it is $\mathcal{R}$ if the channel is successful, and 0 if there is an outage. The average throughput is $E[\text{Throughput}] = \mathcal{R} \cdot (1 - P(\text{outage})) + 0 \cdot P(\text{outage}) = \mathcal{R}(1 - P(\text{outage}))$. Because a half-duplex two-hops relaying protocol is considered, two orthogonal time slots are required to complete a single end-to-end transmission. Similar to [36], the throughput can be written as $\text{Throughput} = \frac{\mathcal{R}}{2}(1 - P(\text{outage}))$ bps/Hz. As the transmit power scales up, the system outage probability vanishes ($P(\text{outage}) \to 0$), enabling the network throughput to asymptotically approach the half-duplex transmission upper bound of $\frac{\mathcal{R}}{2}$.

4. Performance Evaluation

This section introduces the performance investigation of the proposed anti-jamming cooperative network. All simulation results are averaged over 10^5 Monte Carlo trials. The target data rate $\epsilon = 2$ bps/Hz. The energy buffer size is $M = 5$. Conversion efficiency is set to $\gamma = 0.7$. Time is discretized into normalized transmission blocks of duration $t = 1$ s, and the energy required for a single packet transmission is normalized to one discrete energy unit e_k calculated via Equation (3). The energy buffer size is $M = 5$ units. The values of ϵ and M follow standard formulations widely adopted in the energy-harvesting relaying literature. A moderate number of relays $K \in [3, 5]$ is employed, reflecting a realistic localized cluster in smart factory assembly lines [10]. The average channel gain for all links is normalized to $\Theta_{b_k} = 1$. The noise variance at all receiving nodes σ^2 is set to unity. Consequently, the terms transmit power and transmit SNR are used interchangeably throughout this section.

In Figure 2, the outage probability of the traditional max-min scheme flattens out in the high-SNR region of the figure. For a fair comparison, both schemes are equipped with energy buffers of equal capacity. The proposed two-stage selection scheme successfully eliminates these outage floors entirely. The curves maintain a steep, downward slope as SNR increases. As k increases from 2 to 5, the slope of the two-stage scheme becomes significantly steeper. This visually confirms that the scheme achieves full spatial diversity order $d = K$, and the performance decays exponentially with K. To numerically validate the derived spatial diversity order, the empirical log-log slope of the outage probability curve at high SNR of 14 dB and 15 dB is evaluated using $d = -10 \times \frac{\Delta \log_{10}(P_{\text{out}})}{\Delta \text{SNR}_{\text{dB}}}$. For $K = 5$ candidate relays, the numerical slope yields $d \approx 4.95$, which closely matches the theoretical diversity order of $d = K = 5$ as the outage curve reaches its asymptotic high-SNR regime. The fundamental difference in diversity performance between the two schemes lies in their sensitivity to energy starvation. The traditional max-min repeatedly selects relays with strong channel conditions regardless of their energy queue. Under finite buffer capacity, this leads to selecting energy-depleted relays, which continues to induce an outage floor even as $P_t \to \infty$. Conversely, the proposed two-stage restricts the selection domain to the ESR set. Under this protocol, an energy-induced outage can only occur if the ESR set is entirely empty, which mathematically requires all K independent relays to be simultaneously depleted of energy. By forcing this joint dependency across the network, the proposed scheme successfully scales up operational reliability.

Figure 3 provides clear empirical proof of how the outage floors translate into a severe loss of system throughput for the traditional max-min scheme. A packet per time-slot represents the full delivery of the target data rate $\mathcal{R} = 2$ bps/Hz per transmission interval. Because the network operates in half-duplex mode over two orthogonal time-slots, the absolute maximum throughput upper bound is capped at half a packet per

time-slot [36]. Whereas the proposed two-stage selection scheme achieves the maximum half-duplex bound of 0.5 packets/slot, the traditional max-min baseline early-saturates at 0.34 packets/slot because it frequently selects energy-starved relays. This discrepancy represents a throughput loss of $\frac{0.5-0.34}{0.5} \times 100\% = 32\%$.

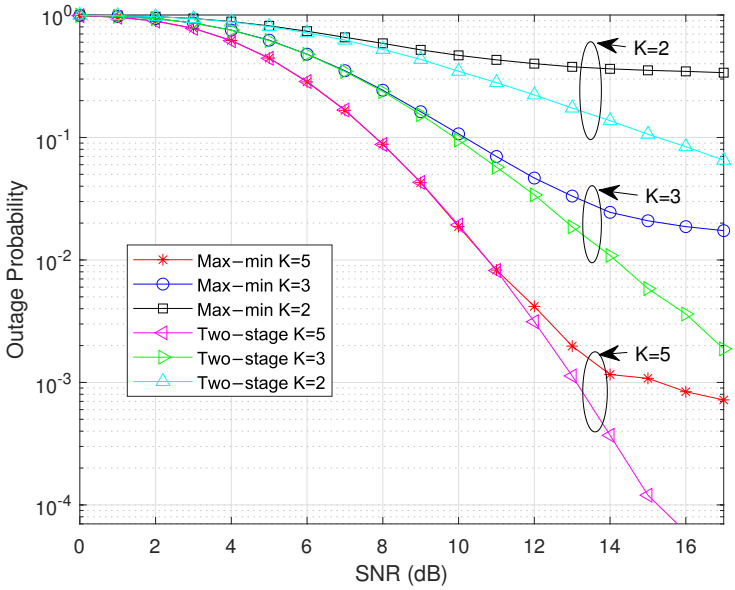


Figure 2. Outage probability comparison between max-min and the proposed two-stage selection schemes for 2, 3 and 5 relays.

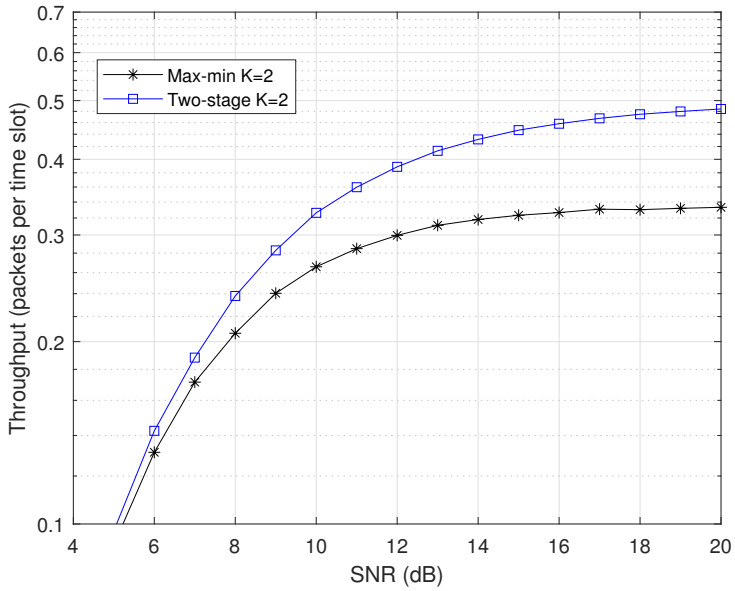


Figure 3. Throughput comparison between max-min and the proposed two-stage selection schemes, for 2 relays.

Figure 4 depicts the network outage probability under a jamming attack, evaluating the proposed two-stage selection policy across varying relay configurations ($K = 2, 3, 5$) against a baseline source-to-destination $S \rightarrow D$ direct link. While a significant body of existing literature assumes a blocked direct link $S \rightarrow D$ to simplify analysis, retaining the $S \rightarrow D$ link in our framework is considered to establish a baseline comparison between the relay-assisted and non-relaying scenarios. To ensure a fair comparison, the direct link transmits at the same $\mathcal{R}$ while benefiting from single-slot transmission, whereas the cooperative network incurs the half-duplex two-slot frame penalty. The jammer introduces a noticeable

degradation in the low-to-medium SNR regions for all configurations, as the injected 10 dB jamming power lowers the instantaneous signal-to-interference-plus-noise ratio across both of the two-hop channels. As the transmit SNR (P_t) increases, the structural limitations of the single-path direct link become apparent, maintaining a shallow slope corresponding to a single diversity order ($d = 1$). In contrast, the proposed two-stage selection mechanism leverages the available relay spatial dimensions to counter the malicious interference by providing unjammed paths. As the SNR scales up, the energy harvesting is enhanced, increasing the number of energy-sufficient relays. The significantly steeper asymptotic slopes for $K = 3$ and $K = 5$ confirm that the full spatial diversity order ($d = K$) is fully preserved even in jamming-prone environments, establishing the robust anti-jamming capabilities of the proposed routing framework.

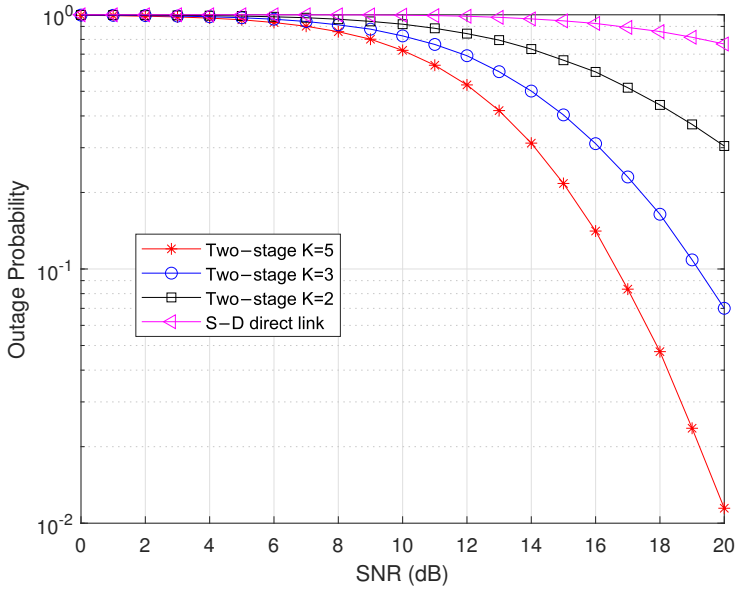


Figure 4. Outage probability in jamming environment comparison between the relay-assisted and non-relaying scenarios for 2, 3 and 5 relays. The SNR at the jammer is 10 dB.

In Figure 5, as the transmit SNR increases, the throughput of the two-stage scheme scales up rapidly, especially for a larger number of relays, $K = 5$. The $K = 5$ curve rushes toward the theoretical maximum ceiling of 0.5 packets per time slot, demonstrating strong resilience against the jammer due to its sufficient spatial degrees of freedom. Even the $K = 2$ curve remains above the direct link across the entire plotted range. This performance gap emphasizes a key design insight for physical-layer security: when operating in jamming environments, maintaining a sufficiently dense relay deployment is essential for the spatial diversity gains to successfully enhance the network performance significantly. It is worth mentioning that the direct link avoids the half-duplex penalty (allowing a theoretical throughput ceiling of 1.0 packet/slot versus 0.5 for two-hop relaying) and isolates the vulnerability to jamming exclusively at a single node (D) captured by η_{jd}, unlike the multi-hop cooperative paths where jamming can degrade both the transmission and forwarding phases captured by both η_{jr_k} and η_{jd}. However, the structural limitations of this single-path channel severely restrict high throughput performance. Even though the direct link's throughput curve does not exhibit a plateau, it requires an excessively high SNR to surpass the upper-bound throughput of the cooperative network, 0.5 packets per time-slot.

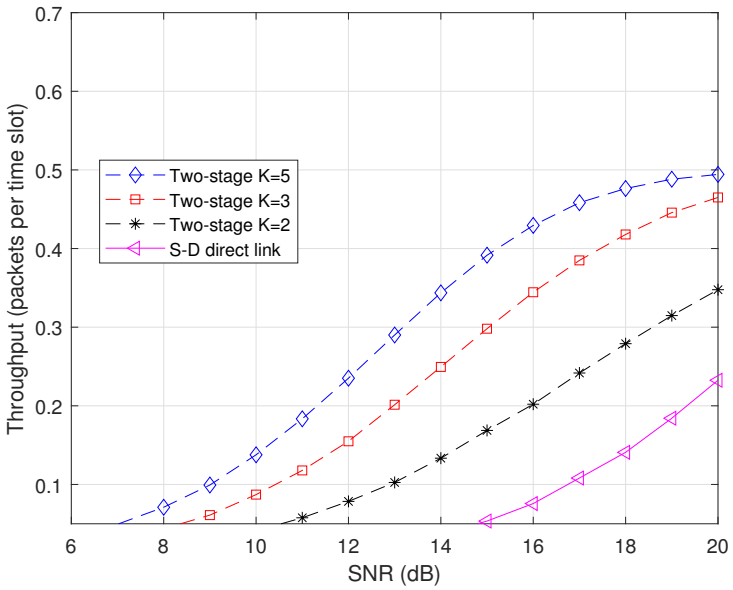


Figure 5. System throughput in jamming environment comparison between the relay-assisted and non-relaying scenarios for 2, 3 and 5 relay configurations. The SNR at the jammer is 10 dB.

Figure 6 illustrates the system throughput across varying jammer power P_j levels (0 dB, 10 dB, and 15 dB). As the jammer SNR (P_j) scales up, an acute rightward shift is observed across all throughput curves. This trend underscores the severe power penalty imposed on the network to overcome the elevated noise-plus-interference floor injected by the malicious jammer. A critical performance trade-off appears when analyzing the low-power jamming scenario (0 dB). At low-to-medium transmit SNRs, the proposed two-stage selection scheme consistently dominates the baseline. However, at high operating regions, specifically surpassing 18 dB, the direct link curve overtakes the cooperative framework. This behavior is directly attributable to the fact that the direct path completely bypasses the half-duplex penalty ($\frac{1}{2}$) inherent to conventional relaying architectures. Furthermore, the direct transmission isolates the network's vulnerability to jamming exclusively at a single node (D), whereas the cooperative network is susceptible to interference across both its routing hops. Consequently, the direct link avoids the early 0.5 packets per time-slot throughput ceiling, though achieving this requires a massive SNR investment. Furthermore, the robust anti-jamming efficacy of the proposed mechanism becomes evident under harsher interference regimes. As the jammer power P_j escalates to 10 dB and 15 dB, the direct link's throughput is severely degraded, failing to reach a meaningful throughput level until very high SNRs above 20 dB. In contrast, the proposed two-stage selection framework successfully leverages its available relay spatial dimensions to exploit alternative, unjammed propagation paths. Remarkably, the spatial diversity gain is powerful enough that the proposed two-stage scheme operating under a severe $P_j = 10$ dB jamming attack outperforms the uncooperative direct link operating under a much weaker $P_j = 0$ dB jamming baseline for a broad range of SNRs. This demonstrates that the proposed spatial selection framework effectively neutralizes high-power jamming threats where conventional single-path routing collapses. It is worth noting that assuming equal average channel gains across all links serves as a conservative benchmark to isolate and evaluate severe-jamming resilience, independently of favorable path-loss geometry. Finally, as demonstrated in [37], increasing the energy buffer size M initially reduces the outage probability by enhancing energy storage availability; however, beyond a certain threshold, its impact plateaus and the dominant factor is the link quality.

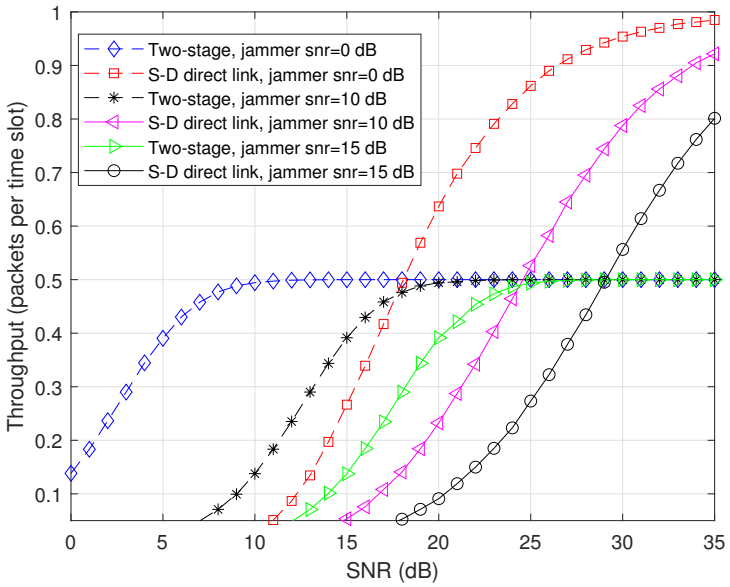


Figure 6. System throughput in jamming environment comparison between the relay-assisted and non-relaying at various jamming SNRs: 0 dB, 10 dB and 15 dB with fixing $K = 5$ relays.

5. Conclusions

In this paper, an anti-jamming solution is proposed. We investigated the performance of an energy-aware cooperative wireless network operating under active physical-layer jamming threats. To mitigate the systemic degradation characteristic of conventional opportunistic routing in next-generation green wireless networks, a robust two-stage selection mechanism was proposed. This framework prevents the selection of energy-depleted relays prior to optimizing for instantaneous channel and jamming conditions. Analytical and numerical results confirm that the proposed scheme successfully preserves the full spatial diversity order of the network, enabling both operational reliability and throughput to scale monotonically with the number of deployed relays. Furthermore, evaluations in harsh interference regimes revealed that the jammer introduces a substantial horizontal power penalty, which may grant the single-hop direct link a localized throughput advantage at excessively high SNRs by confining its attack to a single node. However, the spatial diversity gains of the two-stage protocol consistently dominate the baseline scenario. Ultimately, by effectively leveraging its inherent diversity to exploit unjammed alternative propagation paths, the proposed framework operating under a severe 10 dB jamming attack outperforms the non-cooperative direct link operating under a much weaker $P_j = 0$ dB jamming baseline across a broad range of jamming power levels.

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

Funding: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2604).

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

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

References

1. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
2. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
3. Hu, L.; Wen, H.; Wu, B.; Pan, F.; Liao, R.F.; Song, H.; Tang, J.; Wang, X. Cooperative jamming for physical layer security enhancement in Internet of Things. *IEEE Internet Things J.* **2017**, *5*, 219–228. [CrossRef]
4. Pirayesh, H.; Zeng, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 767–809. [CrossRef]
5. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tutor.* **2010**, *13*, 245–257. [CrossRef]
6. Mpitziopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A survey on jamming attacks and countermeasures in WSNs. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 42–56. [CrossRef]
7. Vanhoef, M.; Piessens, F. Advanced Wi-Fi attacks using commodity hardware. In *Proceedings of the 30th Annual Computer Security Applications Conference*; ACM Digital Library: New York, NY, USA, 2014.
8. Bandaru, S. Investigating the effect of jamming attacks on wireless LANS. *Int. J. Comput. Appl.* **2014**, *99*, 5–9. [CrossRef]
9. Hoseini, S.A.; Bouhafs, F.; Aboutorab, N.; Sadeghi, P.; den Hartog, F. Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning. In *2023 IEEE Globecom Workshops (GC Wkshps)*; IEEE: New York, NY, USA, 2023; pp. 1–6.
10. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 2734–2771. [CrossRef]
11. Mukherjee, A. Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
12. De Meulenaer, G.; Gosset, F.; Standaert , F.X.; Pereira, O. On the energy cost of communication and cryptography in wireless sensor networks. In *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*; IEEE: New York, NY, USA, 2008; pp. 580–585.
13. Alia, A.; Sagheer, M. Efficient Detection of Reactive Jamming Attacks in IoT Networks: A Collaborative Approach. *Int. J. Commun. Syst.* **2025**, *38*, e70098. [CrossRef]
14. Pickholtz, R.; Donald, S.; Laurence, M. Theory of spread-spectrum communications—A tutorial. *IEEE Trans. Commun.* **1982**, *30*, 855–884. [CrossRef]
15. Karhima, T.; Silvennoinen, A.; Hall, M.; Haggman, S.G. IEEE 802.11 b/g WLAN tolerance to jamming. In *IEEE MILCOM 2004. Military Communications Conference*; IEEE: New York, NY, USA, 2004; Volume 3.
16. Angueira, P.; Val, I.; Montalban, J.; Seijo, Ó.; Iradier, E.; Fontaneda, P.S.; Fanari, L.; Arriola, A. A survey of physical layer techniques for secure wireless communications in industry. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 810–838. [CrossRef]
17. Yan, Q.; Zeng, H.; Jiang, T.; Li, M.; Lou, W.; Hou, Y.T. MIMO-based jamming resilient communication in wireless networks. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*; IEEE: New York, NY, USA, 2014.
18. Zeng, H.; Cao, C.; Li, H.; Yan, Q. Enabling jamming-resistant communications in wireless MIMO networks. In *2017 IEEE Conference on Communications and Network Security (CNS)*; IEEE: New York, NY, USA, 2017.
19. Baccour, E.; Erbad, A.; Hamdi, M. RIS assisted Anti-Jamming in Next-Generation wireless communication networks: A survey of Threats, Solutions, and research challenges. *IEEE Open J. Commun. Soc.* **2025**, *6*, 8714–8744. [CrossRef]
20. Liu, J.; Yang, G.; Liang, Y.; Yuen, C. Max-min fairness in RIS-assisted anti-jamming communications: Optimization versus deep reinforcement learning approaches. *IEEE Trans. Commun.* **2024**, *72*, 4476–4492. [CrossRef]
21. Zhang, M.; Xu, X.; Chu, Z.; Huang, Y.; Zhu, Z.; Cumanan, K.; Wang, Y. Improving Anti-Jamming Throughput for Wireless Powered IoT Networks: Is RIS Beneficial or Not? *IEEE Internet Things J.* **2025**, *12*, 36730–36746. [CrossRef]
22. Chu, Z.; Chieng, D.; Kwong, C.F.; Jin, H.; Zhu, Z.; Huang, C.; Yuen, C. Throughput improvement for RIS-empowered wireless powered anti-jamming communication networks (WPAJCN). *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 4622–4637. [CrossRef]
23. Thanh, P.; Giang, H.; Hong, I. Anti-jamming RIS communications using DQN-based algorithm. *IEEE Access* **2022**, *10*, 28422–28433. [CrossRef]
24. Torres, A.; Sanguinetti, L.; Björnson, E. Intelligent reconfigurable surfaces vs. decode-and-forward: What is the impact of electromagnetic interference? In *2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC)*; IEEE: New York, NY, USA, 2022; pp. 1–5.
25. Alkhawatrah, M. Energy-Harvesting Cooperative NOMA in IOT Networks. *Model. Simul. Eng.* **2024**, *1*, 1043973. [CrossRef]
26. Alkhawatrah, M.; AlAyyad, M.; Korostynska, O. Balanced inter-relay charging buffer-aided IOT networks. *EURASIP J. Wirel. Commun. Netw.* **2025**, *2025*, 88. [CrossRef]

27. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2009**, *58*, 1875–1888. [CrossRef]
28. Laganà, F. Design and Simulation-Based Validation of an Embedded Acquisition Architecture for In Situ PCB Integrity Monitoring in Biomedical Devices. *Electronics* **2026**, *15*, 833. [CrossRef]
29. Gu, Y.; Chen, H.; Li, Y.; Liang, Y.-C.; Vucetic, B. Distributed multi-relay selection in accumulate-then-forward energy harvesting relay networks. *IEEE Trans. Green Commun. Netw.* **2018**, *2*, 74–86. [CrossRef]
30. Yan, P.; Zou, Y.; Ding, X.; Zhu, J. Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5115–5128. [CrossRef]
31. Zhang, Q.; Wang, H.; Cai, Y.; Xie, W.F.; Sun, X.; Chen, L. Stability-constrained coordinated control strategy for vehicle chassis integrated AFS and DYC via reinforcement learning. *Control Eng. Pract.* **2026**, *175*, 107122. [CrossRef]
32. Bletsas, A.; Shin, H.; Win, M. Cooperative communications with outage-optimal opportunistic relaying. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 3450–3460. [CrossRef]
33. Kleinrock, L. *Queueing Systems: Theory*; Wiley: Hoboken, NJ, USA, 1974; Volume 2.
34. Yang, L.; Hasna, M. Performance analysis of amplify-and-forward hybrid satellite-terrestrial networks with cochannel interference. *IEEE Trans. Commun.* **2015**, *63*, 5052–5061. [CrossRef]
35. Goldsmith, A.; Chua, S. Variable-rate variable-power MQAM for fading channels. *IEEE Trans. Commun.* **1997**, *45*, 1218–1230. [CrossRef]
36. Nasir, A.; Zhou, X.; Durrani, S.; Kennedy, R. Relaying protocols for wireless energy harvesting and information processing. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 3622–3636. [CrossRef]
37. Lin, C.H.; Liu, K.H. Relay selection for energy-harvesting relays with finite data buffer and energy storage. *IEEE Internet Things J.* **2021**, *8*, 11249–11259. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.