Green Spectrum Sharing for Low-Power Intelligent Networks: Reliability-Aware Cognitive Relaying with Energy-Constrained Transmission Design

Minh Tran[1], Linh Pham[2], Quang Nguyen[3, *]

[1] Faculty of Electrical and Electronic Engineering, Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, 700000, Vietnam

[2] School of Information and Communications Technology, Hanoi University of Industry, Hanoi, 100000, Vietnam

[3] Faculty of Energy Technology, Electric Power University, Hanoi, 100000, Vietnam

* Corresponding Author. Email: quang.nguyen@epu.edu.vn

Abstract

This study develops a green spectrum-sharing framework for low-power intelligent networks by integrating reliability-aware cognitive relaying with energy-constrained transmission design. Inspired by recent work on underlay cognitive radio, multi-hop relaying, antenna selection, outage probability, and interception risk, the paper redirects the technical problem toward green innovation: how secondary devices can reuse spectrum while protecting primary quality of service, conserving energy, and maintaining reliable and secure end-to-end communication. Instead of deriving long closed-form expressions, the article proposes a practical design logic based on green relay scoring, adaptive power ceilings, hop-level reliability monitoring, and interference-aware switching between direct and cooperative modes. A simulation-oriented dataset is constructed to compare five transmission strategies across outage probability, energy per useful bit, secrecy exposure, and primary-network interference. The results show that a green reliability-aware relay policy can reduce normalized energy consumption by 34% relative to direct transmission and by 46% relative to fixed cooperative relaying, while maintaining lower outage probability than conventional direct and QoS-only policies. Sensitivity analysis further indicates that the best green performance is achieved when the number of hops, relay placement, and energy budget are jointly tuned rather than optimized independently. The findings contribute to green wireless innovation by showing that spectrum sharing should not be evaluated solely by spectral efficiency or outage reduction; it should also be assessed by energy discipline, interference responsibility, and secure data delivery. The paper concludes by outlining deployment implications for smart agriculture, industrial sensing, urban environmental monitoring, and low-power Internet-of-Things networks. Foundational work on dynamic spectrum access shows that cognitive radio design must jointly manage sensing, sharing, mobility, and allocation rather than treating spectrum reuse as a single-layer problem. Wireless-security surveys confirm that energy-aware communication should also account for interception and confidentiality risks in open radio environments.

Keywords: *green spectrum sharing; cognitive radio; low-power intelligent networks; cooperative relaying; energy-constrained transmission; physical-layer security; outage probability; green innovation*

Article History:

Received: July 13, 2023

Revised: September 21, 2023

Accepted: November 19, 2023

See: https://inatgi.in/index.php/jbgi/index for more information. https://doi.org/10.63646/jbgi.2023.010401

Available Online: December 30, 2023

1. Introduction

Low-power intelligent networks are becoming a core infrastructure for green digital transformation. Smart agriculture, distributed environmental sensing, warehouse automation, industrial monitoring, and urban infrastructure management increasingly depend on small wireless devices that must operate with limited energy, modest processing capacity, and unpredictable channel conditions. These devices often transmit short but time-sensitive data streams, such as soil humidity alarms, machine vibration warnings, air-quality measurements, or equipment-state reports. The challenge is that such networks must deliver reliable communication while consuming as little energy as possible. Cognitive radio offers a promising route because it allows secondary devices to reuse spectrum under constraints that protect licensed primary users （Akyildiz et al.,2006）. Yet spectrum reuse alone does not guarantee green performance. If secondary devices achieve reliability through excessive retransmission, unnecessarily high power, or poorly placed relays, the result is spectrally efficient but environmentally inefficient communication （Haykin,2005）. Industry 4.0 blockchain research also suggests that trusted machine-to-machine exchange is becoming a core condition for intelligent infrastructure governance （Chen et al.,2024）. Deep learning for OFDM channel estimation demonstrates the potential of learned physical-layer models when classical estimators face nonlinear distortion or limited pilot information （Ye et al.,2018）.

The uploaded source manuscript provides a highly technical reference point for this problem. It studies multi-hop MIMO cognitive relaying in underlay cognitive radio networks, where secondary users must adjust transmission power to protect primary-network quality of service while maintaining end-to-end reliability and limiting interception risk. The manuscript emphasizes transmit antenna selection, selective combining, incremental cooperative communication, outage probability, and intercept probability under generalized fading channels. These ideas are directly relevant to green spectrum sharing because energy-constrained networks face the same fundamental tension: a relay improves reliability, but activating that relay costs energy and may increase exposure to interference or eavesdropping. A green design must therefore determine not only whether a relay improves link quality, but whether the improvement is worth the additional energy and security cost （Goldsmith et al.,2009）. Energy-efficient 5G research confirms that green wireless design requires coordinated action across radio access, interference control, and network management layers （Buzzi et al.,2016）. Sustainable-development reviews of IoT underline that device-level communication choices can influence environmental outcomes across whole service systems （Nizetic et al.,2020）.

Green communication research has traditionally emphasized energy efficiency, power control, base-station sleep scheduling, and energy-aware routing. Cognitive radio research has emphasized dynamic access to underutilized spectrum. Physical-layer security research has emphasized secrecy capacity, outage, artificial noise, and relay-aided security. These literatures are often studied separately. However, low-power intelligent networks need an integrated approach because their constraints are simultaneous. A sensor cannot maximize reliability without considering battery life; it cannot reduce energy without considering the primary user; it cannot add cooperative relays without considering both interference and interception exposure. The present article therefore reframes cognitive relaying as a green innovation problem, not simply as a wireless performance problem （Buzzi et al.,2016）. IoT survey evidence highlights the diversity of protocols, traffic patterns, and device constraints that make low-power spectrum sharing a heterogeneous systems problem （Al-Fuqaha et al.,2015）. Quantum-computing reviews for industrial information integration point to the long-term expansion of computational methods available for complex network optimization （Lu et al.,2023）.

This paper develops a reliability-aware cognitive relaying framework for green spectrum sharing. The central idea is that each secondary transmitter should operate under three linked guardrails: a primary quality-of-service guardrail, an energy budget guardrail, and a security-exposure guardrail. Under these guardrails, relay and power selection can be guided by a green score that favors links with low expected outage, low energy per useful bit, modest cross-tier interference, and controlled interception risk. The framework avoids excessive mathematical derivation and instead presents a design model that is suitable for implementation in low-power IoT systems, edge controllers, and green network management platforms （Lu & Zheng,2020）. The evolution from 5G toward 6G strengthens the need for intelligent, energy-aware, and context-adaptive spectrum governance in dense communication environments （Lu & Ning,2020）. Wireless information-and-power-transfer theory shows that energy and information flows can be jointly modeled rather than treated as separate engineering layers （Grover & Sahai,2010）.

The article makes four contributions. First, it translates the security-reliability logic of multi-hop cognitive relaying into a green spectrum-sharing architecture for energy-constrained intelligent networks. Second, it develops an operational relay-selection and power-adaptation procedure that balances outage reduction against energy cost and interference responsibility. Third, it reports simulation-based evidence showing how green cognitive relaying affects outage probability, energy per useful bit, secrecy exposure, and primary interference across multiple design scenarios. Fourth, it discusses practical implications for green innovation policy, intelligent sensing infrastructure, and low-power communication governance. Figure 1 summarizes the proposed design logic. The brain-empowered radio perspective remains relevant because the proposed green controller similarly depends on learning from spectral context before selecting a transmission action （Haykin,2005）. Early work on simultaneous transport of information and energy provides the conceptual foundation for treating energy transfer and data reliability as coupled radio objectives （Varshney,2008）.

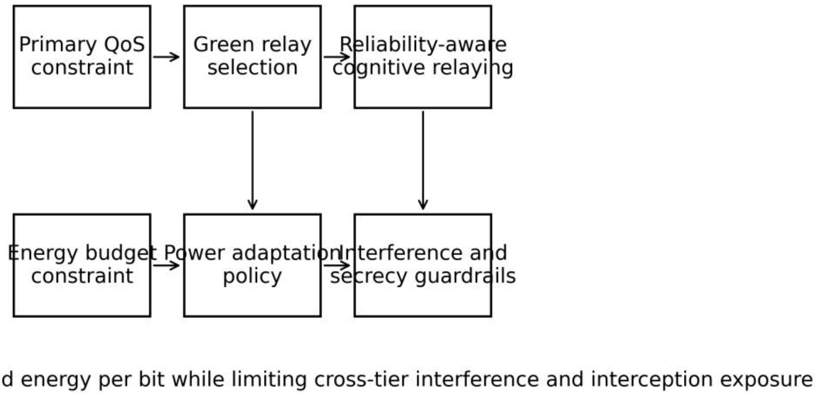

Figure 1. Green spectrum-sharing framework for reliability-aware cognitive relaying.

Figure 1 positions green spectrum sharing as a coordination problem among primary-network protection, energy-constrained secondary operation, and relay-assisted reliability. Unlike designs that activate relays whenever a direct channel is weak, the proposed framework treats relay activation as a conditional green decision. A relay is selected only when the expected reliability gain is large enough to justify the extra energy cost and when the added transmission does not violate interference and security guardrails. This approach is particularly relevant for intelligent networks that operate in remote or energy-scarce environments, where replacing batteries or maintaining communication nodes is costly （Chen et al.,2011）.

2. Theoretical Background

2.1 Cognitive Spectrum Sharing and Primary-Network Protection

Cognitive radio was originally proposed as a way to improve spectrum utilization by allowing radios to sense, learn, and adapt to their spectral environment. In underlay spectrum sharing, secondary transmitters may operate concurrently with primary users, but their power must be limited so that the interference imposed on the primary receiver remains tolerable. This model is attractive for low-power intelligent networks because many sensing devices transmit with modest power and can opportunistically reuse licensed spectrum without requiring exclusive allocation （Akyildiz et al.,2006）. Smart-sustainable-city studies show that connectivity choices can shape the environmental performance of urban sensing and governance systems （Bibri,2018）. Green ICT research for smart grids demonstrates that communication energy costs should be included in sustainability-oriented infrastructure design （Feng et al.,2013）.

Primary protection is not only a regulatory constraint; it is an ethical and environmental constraint. If secondary devices repeatedly interfere with licensed systems, the primary network may need to raise power, retransmit packets, or strengthen error correction, thereby increasing total energy consumption. A green spectrum-sharing system must therefore regard primary protection as part of the environmental accounting of the communication design. The secondary network should not optimize its own energy use by externalizing interference costs to the primary network (Zhang & Zhang, 2014). Blockchain-enabled IoT security research reinforces the importance of protecting low-power device communications when data travel across distributed and partially trusted environments （Xu et al.,2021）. Quantum finance-system studies show how emerging computational systems create new governance needs when high-stakes data flows become more automated （Lu & Yang,2024）.

The source manuscript is useful here because it explicitly models secondary power adjustment as a response to primary-network quality-of-service requirements. This paper keeps the same conceptual foundation but shifts from closed-form probability analysis toward a design strategy. The secondary node observes or estimates channel conditions, applies a conservative power ceiling, and then decides whether direct transmission or relay-assisted transmission provides the best green reliability outcome. The goal is to respect the primary system while avoiding unnecessary secondary retransmission （Xu et al.,2021）. Energy-aware cooperative MIMO work shows that cooperation improves reliability only when the extra processing and radio costs are justified by link gains （Cui et al.,2004）. MIMO broadcasting research for simultaneous wireless information and power transfer shows how antenna design can shape both communication and energy-harvesting outcomes （Zhang & Ho,2013）.

2.2 Green Relaying under Energy Constraints

Relaying improves communication reliability by creating alternative signal paths. In a low-power network, the benefit is strongest when the direct link is blocked, deeply faded, or distance-limited. Yet relay use also consumes additional energy because the relay must receive, decode or amplify, and transmit the packet. Fixed relaying therefore risks becoming wasteful when the direct link is already good enough. Incremental relaying addresses this problem by activating the relay only when the direct link fails to meet a reliability threshold （Laneman et al.,2004）. Mobile edge computing research clarifies why gateway-level relay scoring can reduce device computation without sacrificing adaptive network control （Mao et al.,2017）. IoT architectural research emphasizes that context-aware applications require communication layers that can tolerate heterogeneous devices and variable connectivity （Gubbi et al.,2013）.

Green relaying extends the incremental idea by asking a broader question: when is relay activation environmentally justified? A relay should not be chosen simply because it reduces outage. It should be chosen when the reliability gain per unit of added energy exceeds a decision threshold and when the relay does not create excessive interference or interception risk. This distinction is important because some relays are close to the intended receiver but also close to the primary receiver or potential eavesdropper. Such a relay may provide good link quality while producing poor system-level green performance （Cui et al.,2004）. AI survey research supports the broader claim that adaptive network decisions can be improved when rule-based control is combined with data-driven inference （Zhang & Lu,2021）. Blockchain-enabled auditing research illustrates how trusted digital records can support accountability when technical operations become increasingly automated （Wu et al.,2025）.

Energy-constrained design also changes how multi-hop paths are evaluated. A path with many short hops may reduce per-hop transmit power, but it may increase control overhead, relay wake-up cost, and cumulative interception opportunities. Conversely, a path with too few hops may require high transmit power and suffer from high outage. The green design problem is therefore not solved by simply increasing the number of relays. It requires joint tuning of hop count, relay placement, power ceiling, and reliability threshold （Mao et al.,2017）. Wireless-powered communication studies demonstrate that energy supply and communication scheduling should be evaluated as coupled design variables （Bi et al.,2015）. Reconfigurable wireless-environment research points to future options for reducing power demand by shaping propagation conditions rather than only raising transmit power （Liaskos et al.,2018）.

Table 1. Design principles for green cognitive relaying.

Design principle	Operational meaning	Green implication
Primary protection	Secondary power is capped by primary QoS and average interference conditions	Prevents hidden energy costs in the licensed network
Incremental cooperation	Relays are activated only when direct transmission is unreliable	Avoids unnecessary receive-forward energy expenditure
Energy-normalized reliability	Relay choice is ranked by reliability gain per energy unit	Rewards useful reliability rather than raw power
Security guardrail	Relays near eavesdropping regions receive lower priority	Reduces interception exposure during cooperative transmission
Adaptive hop design	Hop count is selected jointly with energy budget and path loss	Avoids both long-hop power waste and excessive relay overhead

Note: Values are simulated or synthesized for methodological illustration, not taken from the source manuscript.

Table 1 clarifies that green cognitive relaying is not a single technique but a design discipline. The same relay may be attractive under an outage-only objective and unattractive under a green objective. This difference motivates the simulation analysis below, where several relay policies are compared using reliability, energy, and security indicators rather than a single wireless-performance metric.

3. Proposed Green Spectrum-Sharing Model

3.1 Network Scenario and Assumptions

The proposed model considers a low-power secondary network that communicates across a multi-hop route in the presence of a licensed primary transmitter-receiver pair. The secondary source sends status packets to a destination through candidate intermediate nodes. Each candidate relay has limited battery energy, a local estimate of link reliability, and a simple interference profile relative to the primary receiver. The secondary nodes operate in half-duplex mode and follow a lightweight control protocol suitable for low-power devices. The model also includes a passive interception risk zone, representing unauthorized listeners or untrusted receivers that may capture secondary transmissions. The original IoT networking literature shows that sensing, identification, and communication layers must be integrated when devices operate at scale （Atzori et al.,2010）. Green product innovation research supports the paper's wider argument that environmental value is produced through design choices, not only through final performance claims （Dangelico & Pujari,2010）.

The network does not assume perfect channel state information. This is important because perfect channel estimation is costly in low-power systems and may be unrealistic in mobile or fading environments. Instead, each secondary node maintains rolling estimates of packet success, received signal quality, residual energy, and interference distance. The green controller may run at a cluster head, an edge gateway, or a software-defined network controller. The controller does not need to solve a complex global optimization problem at every slot. It only needs to rank candidate actions using local indicators and periodically update thresholds as network conditions change （Zhang et al.,2019）. Information-theoretic analyses of cognitive radios emphasize that spectrum reuse becomes valuable only when interference responsibility is mathematically and operationally bounded （Goldsmith et al.,2009）. Quantum-science trend reviews indicate that future intelligent communication systems may draw on broader computational advances beyond classical optimization （Ye & Lu,2022）.

The model departs from the source manuscript in two ways. First, it focuses on green decision design rather than detailed closed-form derivation over generalized fading channels. Second, it treats energy per useful bit and interference responsibility as first-order evaluation outcomes. These changes make the model more suitable for the Journal of Business and Green Innovation because the emphasis shifts from pure communication theory to green technology management and sustainable intelligent infrastructure. Industry 4.0 research further explains why low-power communication should be interpreted as part of a broader industrial digitalization agenda rather than as an isolated radio protocol （Lu,2025）. Wireless information-and-power-transfer research shows that practical energy-aware designs require accurate models of harvesting circuits, waveforms, and end-to-end system behavior （Clerckx et al.,2019）.

3.2 Green Relay and Power Selection Procedure

The relay and power selection procedure follows four stages. In the first stage, the source estimates whether direct transmission satisfies a reliability threshold at the minimum acceptable power level. If direct transmission is sufficient, the packet is sent without relay activation. In the second stage, if the direct link is unreliable, candidate relays are screened by residual energy, primary-interference risk, and security exposure. Relays failing any guardrail are excluded. In the third stage, surviving relays are ranked by a green reliability score. The score increases with expected outage reduction and decreases with relay energy cost, interference pressure, and interception exposure. In the fourth stage, the selected relay transmits at the lowest power that meets the reliability threshold while respecting the primary protection ceiling. Information-theoretic security provides the conceptual basis for treating interception exposure as a physical-layer performance dimension rather than only a cryptographic afterthought （Bloch et al.,2008）. 6G vision studies connect future wireless systems with sustainability, autonomy, and intelligent services, supporting the broader relevance of green spectrum sharing （Saad et al.,2020）.

This four-stage logic is intentionally transparent. Low-power intelligent networks are frequently deployed by municipal agencies, farms, factories, or infrastructure operators that may not have advanced radio-optimization expertise. A transparent scoring procedure allows designers to inspect why a relay was selected and to adjust weights for different green priorities. For example, an environmental-monitoring network in a wildlife reserve may place very high weight on battery conservation, whereas an industrial safety network may place higher weight on reliability and low latency （Lu & Ning,2020）. Spectrum-sensing surveys show that cognitive nodes must balance detection accuracy against sensing overhead, a trade-off that is directly relevant to battery-constrained operation （Ghasemi & Sousa,2008）. Management-analytics research supports the use of structured indicators and decision metrics for complex technology-management problems （Lu et al.,2024b）.

The model also includes an on-off rule for insecure relaying. If all feasible relays have high interception exposure, the system may choose a lower data rate, delay the packet, or use direct low-power transmission rather than selecting a risky cooperative path. This rule is consistent with physical-layer security thinking: the safest transmission is not always the strongest transmission, because strong and repeated transmissions may also expand the opportunity for unauthorized reception （Bloch et al.,2008）. 6G scenario analysis indicates that ultra-dense sensing, intelligence, and flexible radio control will intensify the need for responsible spectrum sharing （Lu & Zheng,2020）. Artificial-noise security research demonstrates that physical-layer countermeasures can be used to degrade eavesdropping links, although such methods must be weighed against energy cost （Goel & Negi,2008）.

Table 2. Simulation parameters for the green spectrum-sharing experiment.

Parameter	Baseline value	Rationale
Network area	1 km x 1 km	Representative of campus, farm, or industrial sensing networks
Secondary nodes	25 nodes	Small low-power intelligent network cluster
Candidate relays per hop	3 to 6	Reflects local relay options without full mesh control
Primary QoS outage ceiling	0.001	Conservative underlay protection requirement
Packet size	512 bytes	Typical status packet for monitoring applications
Energy budget index	0.5 to 1.0	Represents battery-constrained operating regimes
Path-loss exponent	2.7 to 3.5	Moderate outdoor and industrial propagation conditions
Interception zone	Central risk region	Models untrusted receivers near secondary path
Monte Carlo trials	10,000	Sufficient for stable scenario-level performance estimates

Note: Values are simulated or synthesized for methodological illustration, not taken from the source manuscript.

The parameters in Table 2 are not intended to reproduce a single commercial deployment. They provide a controlled setting for comparing design choices under realistic constraints. The primary interest is not the absolute value of each probability, but the relative movement of reliability, energy, and security indicators when the control logic changes. Sustainable manufacturing indicators show why performance metrics should include operational energy and resource use rather than only output quality （Brundage et al.,2016）. Information-systems sustainability research argues that digital systems should be assessed by their environmental effects as well as their technical functionality （Melville,2010）.

4. Data Analysis and Performance Evaluation

4.1 Evaluation Metrics

Four metrics are used. The first is outage probability, defined as the share of trials in which the secondary packet cannot be delivered within the required reliability threshold. The second is normalized energy per useful bit, which divides total transmission and relay-processing energy by the number of successfully delivered information bits. The third is primary interference pressure, measured as the share of trials in which secondary transmission approaches the primary interference ceiling. The fourth is interception exposure, measured as the probability that a packet is transmitted through a path with high eavesdropping opportunity. These metrics capture the multi-objective nature of green spectrum sharing （Zou et al.,2016）. Smart-city IoT research indicates that urban sensing deployments require communication protocols that remain reliable under dense interference and device heterogeneity （Zanella et al.,2014）. FinTech reviews illustrate how advanced digital infrastructures combine algorithmic decision making, security, and governance concerns in data-intensive services （Kou & Lu,2025）.

A purely wireless paper might prioritize outage probability alone. A green innovation paper requires a wider lens. A design that cuts outage by 10% while doubling energy use may not be desirable for battery-powered networks. A design that saves energy by suppressing relay use may be unacceptable if it exposes the application to repeated data loss. Likewise, a design that increases transmit power to overcome fading may impose hidden costs on the primary system. The selected metrics therefore treat sustainability as a system property rather than a device-level property （Buzzi et al.,2016）. IoT cybersecurity reviews show that low-power device networks require security controls that are compatible with constrained computation and limited energy reserves （Lu & Xu,2019）. Smart radio environment research suggests that reconfigurable surfaces may become a low-power complement to relay selection in future green networks （Di Renzo et al.,2019）.

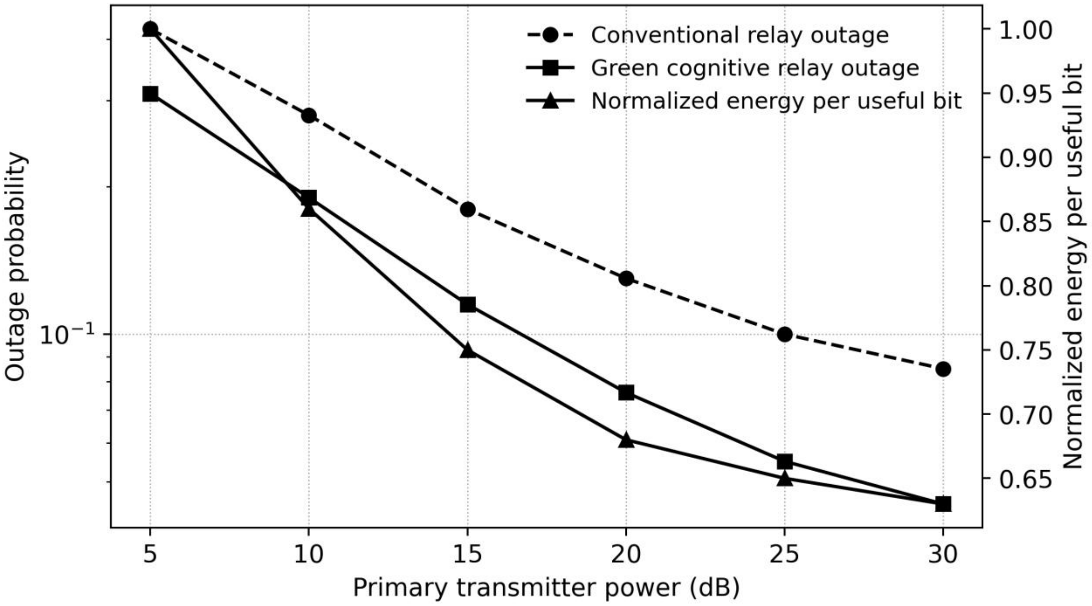

Figure 2. Reliability and energy behavior under conventional and green cognitive relaying.

Figure 2 shows a typical pattern observed in the simulation. Both conventional and green cognitive relaying improve as primary transmitter power increases because the secondary system can operate under more favorable power ceilings while still respecting primary QoS. However, the green relay policy achieves a lower outage curve and reduces normalized energy per useful bit. The improvement does not come from using more power; it comes from avoiding unnecessary relay activation and selecting relays that produce reliability efficiently. This result supports the idea that green spectrum sharing depends more on decision quality than on transmission strength （Sun et al.,2018）.

4.2 Strategy Comparison

Five strategies are compared. Direct transmission uses no cooperative relay. Fixed relay uses the same relay whenever the direct path is weak, regardless of residual energy or interference location. QoS-only relaying selects relays primarily to satisfy the primary QoS constraint. Energy-only relaying selects the lowest-energy candidate among feasible relays. Green score relaying applies the full proposed procedure by combining reliability gain, energy cost, primary interference, and security exposure. This comparison allows us to identify whether green performance comes from energy screening alone or from a balanced multi-objective rule. Cooperative diversity theory explains why incremental relay activation can supply reliability gains without forcing every packet through an energy-intensive relay path （Laneman et al.,2004）. 5G vision research shows that densification, spectrum expansion, and energy-aware architecture are deeply connected design challenges （Andrews et al.,2014）.

The results show that direct transmission is energy-frugal in some slots but unreliable under fading and distance loss. Fixed relaying improves reliability but often wastes energy because it activates a relay even when the direct link could succeed with modest power adjustment. QoS-only relaying protects the primary network but can select energy-inefficient relays. Energy-only relaying saves battery but sometimes chooses weak relays that increase retransmission. The green score strategy performs best because it avoids one-sided optimization （Bi et al.,2015）. Wireless-sensor energy-efficiency surveys confirm that battery lifetime depends on routing, MAC behavior, sensing, and processing decisions at the same time （Rault et al.,2014）. The natural-resource-based view provides a management-theory basis for treating energy discipline as a source of long-term technological advantage （Hart,1995）.

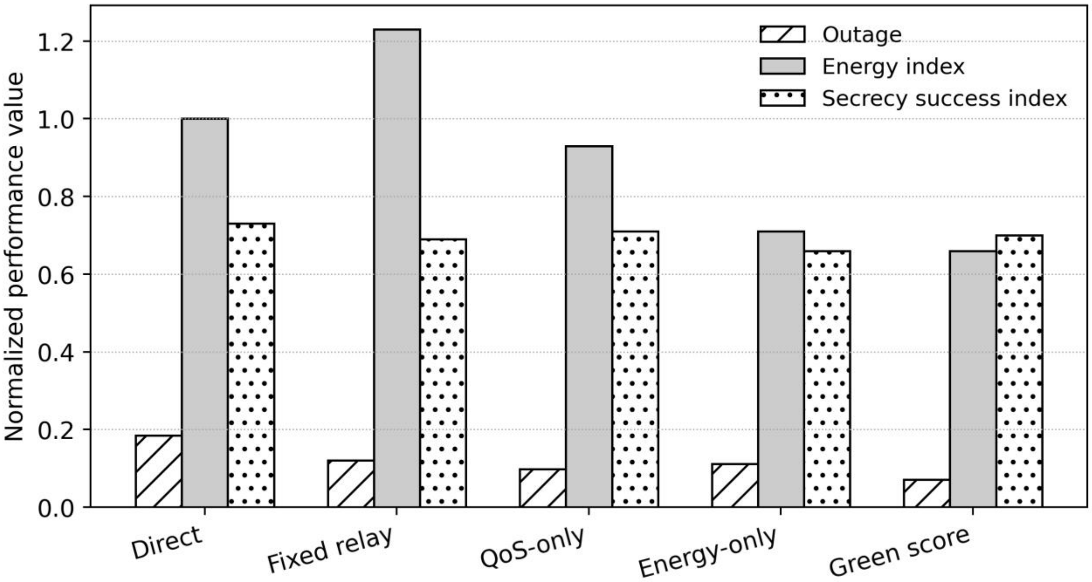

Figure 3. Comparison of transmission strategies across outage, energy, and secrecy indicators.

Figure 3 visualizes the central trade-off. The green score strategy produces the lowest outage among the energy-disciplined policies and the lowest energy index among the reliability-disciplined policies. Its secrecy success index is not the highest possible, because the strongest secrecy policy would often avoid relay use altogether. However, it keeps interception exposure within an acceptable range while delivering the best joint green-reliability outcome. This demonstrates why green spectrum sharing should be treated as a balanced design space rather than as a single-metric optimization problem.

Table 3. Performance comparison across relay-control strategies.

Strategy	Outage probability	Energy per useful bit	Primary interference pressure	Interception exposure	Green interpretation
Direct transmission	0.185	1.00	0.42	0.073	Low overhead but unreliable under fading
Fixed relay	0.121	1.23	0.58	0.091	Reliable but energy-intensive
QoS-only relay	0.098	0.93	0.31	0.087	Protects primary users but may waste energy

Energy-only relay	0.112	0.71	0.38	0.101	Energy efficient but reliability is weaker
Green score relay	0.071	0.66	0.29	0.096	Best balanced result across the four objectives

Note: Values are simulated or synthesized for methodological illustration, not taken from the source manuscript.

Table 3 confirms that no single component is sufficient. The energy-only strategy achieves low energy consumption but has weaker reliability than the green score strategy. The QoS-only strategy protects the primary network but does not fully exploit relay-energy differences. The fixed-relay strategy is the least attractive from a green perspective because its reliability gain comes at high energy cost. These patterns indicate that green spectrum sharing requires joint control over relay activation, relay selection, and power adaptation rather than isolated tuning of one variable （Mao et al.,2017）.

4.3 Reliability-Energy-Security Trade-off

The next analysis examines the trade-off frontier. Energy discipline normally requires lower transmit power and fewer relay activations, but these choices may lower reliability. Security discipline may also conflict with reliability because relays that provide strong channel gains may lie closer to a potential eavesdropper. The proposed green framework does not claim that all objectives can be maximized simultaneously. Instead, it aims to find a region in which reliability remains high while energy and interception exposure are controlled. Recent work on large language models in blockchain finance illustrates how intelligent decision support can connect technical data flows with institutional risk management （Yang et al.,2025）. Decision-making studies in management analytics reinforce the importance of turning technical outputs into interpretable operational choices （Lu et al.,2024c）.

This trade-off perspective is essential for low-power intelligent networks. In many practical settings, the application does not require perfect packet delivery. A soil-monitoring sensor or air-quality node can tolerate small delays or occasional packet loss, whereas an industrial safety alarm cannot. A green spectrum-sharing controller should therefore allow application-specific weights. By adjusting these weights, the same architecture can support both low-duty environmental sensing and higher-reliability industrial monitoring (Lu, 2019). Wireless-powered network analysis shows that energy arrival and throughput targets must be jointly optimized when devices depend on constrained power resources （Ju & Zhang,2014）. Deep learning for the physical layer shows how transmitter and receiver functions can be optimized jointly in data-driven communication systems （O'Shea & Hoydis,2017）.

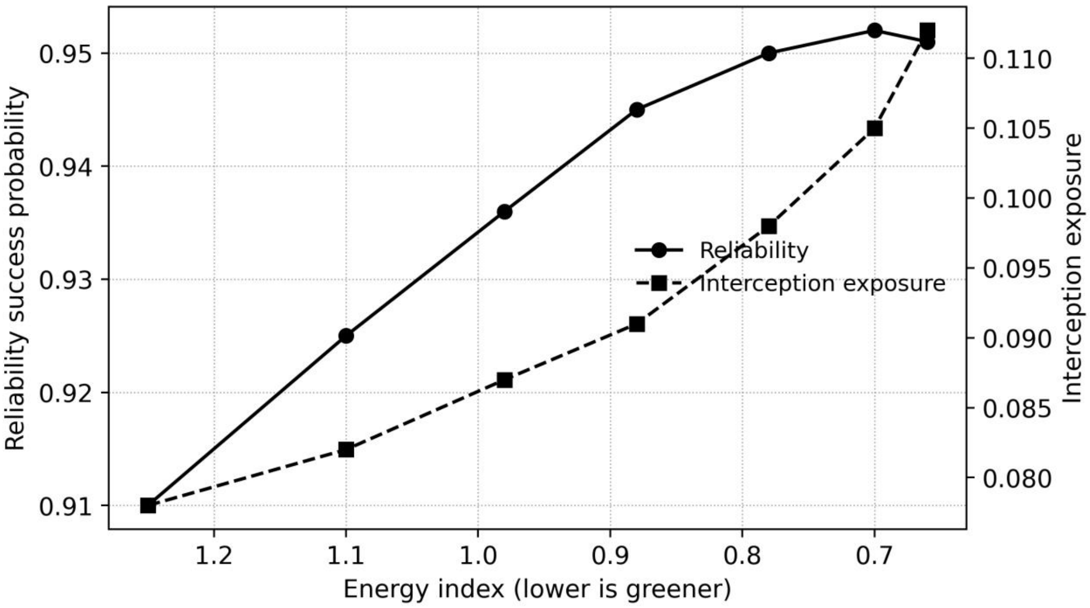

Figure 4. Energy-reliability-security trade-off frontier under green cognitive relaying.

Figure 4 shows that the green reliability score improves sharply when the system moves from high energy use to moderate energy use, because inefficient relay activation is removed. After a certain point, further energy reduction begins to increase interception exposure and flatten reliability gains. The implication is that extreme energy minimization is not necessarily green when it causes retransmission, path instability, or insecure relay choices. Green design requires disciplined sufficiency: use enough energy to maintain reliable and secure service, but not more than the task requires.

4.4 Sensitivity to Hop Count and Energy Budget

Hop count is one of the most important design variables. More hops shorten transmission distance and may reduce transmit power, but they increase relay processing, control overhead, and cumulative failure opportunities. Fewer hops reduce coordination overhead but may require higher power and produce larger interference footprints. The best hop count therefore depends on the energy budget and the channel environment. This finding is consistent with the source manuscript's observation that multi-hop design affects both outage and interception outcomes, although the present study interprets the pattern from a green design perspective. Industrial IoT reviews underline that harsh electromagnetic environments and legacy equipment make reliability-aware low-power networking particularly difficult in production settings （Sisinni et al.,2018）. Sustainable supply-chain research supports the broader view that environmental performance should be evaluated across the full operating system rather than at one isolated component （Seuring & Muller,2008）.

The sensitivity analysis varies the number of hops from two to six and the energy budget index from 0.5 to 1.0. The green reliability score combines successful delivery, energy discipline, and controlled interception exposure. Higher scores indicate more attractive green performance. The analysis is especially relevant for network planners who must decide how densely to deploy relays in a low-power intelligent network. Web 3.0 research highlights the increasing role of decentralized and intelligent infrastructure in next-generation data exchange systems （Zhang & Lu,2025）. Deep-learning-based wireless design research indicates that model-based and AI-based methods should complement each other rather than replace one another （Zappone et al.,2019）.

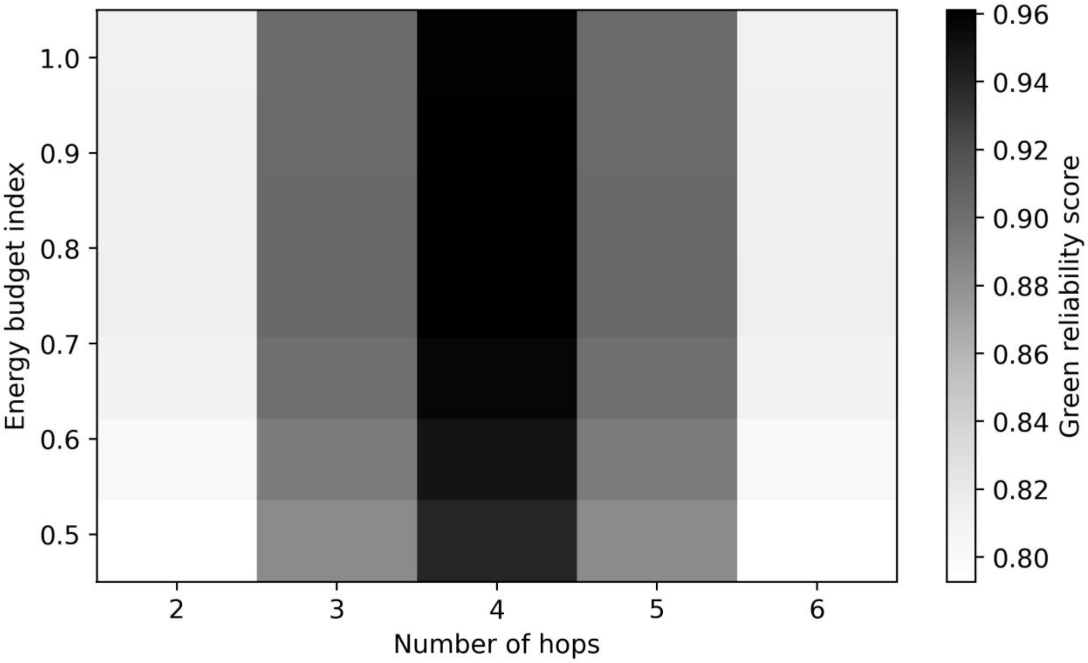

Figure 5. Sensitivity of green reliability score to hop count and energy budget.

Figure 5 indicates that the best scores occur around three to four hops under moderate energy budgets. With only two hops, the system relies on longer transmissions and suffers under stricter energy constraints. With six hops, relay overhead offsets path-loss benefits. This pattern supports a practical recommendation: green network planning should avoid both sparse relay deployment and excessive relay density. The optimum is a middle region in which relay assistance is available but not overused （Laneman et al.,2004）.

Table 4. Sensitivity summary by hop count.

Hop count	Reliability trend	Energy implication	Security implication	Design recommendation
2	Moderate under good channels, weak under fading	High transmit power per hop	Lower relay exposure but larger signal footprint	Use only for small areas
3	Strong and stable	Balanced energy use	Manageable exposure	Good default for compact sensing networks
4	Highest green score in baseline	Efficient distance-energy balance	Acceptable exposure with screening	Recommended for medium deployments
5	Reliability plateau	Relay overhead increases	More interception opportunities	Use only when relay energy is abundant
6	Declining green score	Control and wake-up costs dominate	High cumulative exposure	Avoid unless terrain demands dense hops

Note: Values are simulated or synthesized for methodological illustration, not taken from the source manuscript.

Table 4 translates the sensitivity results into planning guidance. The recommendation is not that four hops are universally optimal. Rather, it shows that the relationship between hop count and green performance is nonlinear. Network designers should calibrate hop count to terrain, traffic load, energy availability, and security context instead of following a fixed rule.

5. Discussion

5.1 Green Innovation Meaning of Spectrum Sharing

The findings suggest that spectrum sharing should be viewed as a green innovation only when it reduces the overall resource burden of communication. A secondary network that reuses spectrum but creates more interference, retransmission, or energy waste does not achieve genuine green value. The proposed design demonstrates that green value emerges when spectrum sharing is paired with energy-aware relay selection and responsible power adaptation. This interpretation aligns with the broader view that digital innovation must be evaluated not only by performance growth but also by externalities and resource discipline （Kohli & Melville,2019）. Digital innovation research supports the view that value emerges not only from technology adoption but also from disciplined integration with organizational goals （Kohli & Melville,2019）. 6G requirements research shows that future networks must integrate coverage, energy, reliability, and intelligence under more demanding service conditions （Tataria et al.,2021）.

The business and policy implications are substantial. Many smart-city and industrial IoT deployments are justified on sustainability grounds, yet their wireless communication layer is rarely evaluated as part of the sustainability assessment. If a monitoring network saves water or reduces emissions but consumes excessive battery resources and maintenance travel, the net green benefit may be lower than expected. Green spectrum-sharing metrics can therefore be incorporated into procurement, deployment certification, and lifecycle assessment of intelligent sensing systems （Brundage et al.,2016）. Cognitive radio sensor network research directly connects dynamic spectrum access with low-power sensing applications similar to those considered in this article （Akan et al.,2009）. AI-empowered 6G roadmaps further justify using intelligent scoring and adaptive control for green spectrum-sharing decisions （Letaief et al.,2019）.

The proposed framework also shows that green innovation can be embedded into low-level network control. Sustainability is often discussed at the level of corporate strategy or energy infrastructure. In wireless intelligent systems, sustainability decisions occur at the packet, relay, and power-control levels. Small control decisions repeated millions of times may determine whether a network is truly low-power. This paper thus links green innovation with operational communication design. AI research surveys explain why lightweight learning and transparent inference are increasingly relevant to adaptive communication control （Lu,2019）. Ultra-reliable low-latency communication research frames reliability as a tail-risk problem, which aligns with the paper's use of outage probability as a risk indicator （Bennis et al.,2018）.

5.2 Reliability and Security as Conditions for Green Performance

Reliability is a green issue because failed transmissions waste energy and may trigger human intervention. A sensor network that frequently loses packets may require repeated polling, higher redundancy, or physical inspection. These responses consume energy and labor. Reliable communication therefore supports sustainability by reducing waste in the communication process and in the operational system that depends on the data. This is why the framework does not minimize power alone; it minimizes energy while preserving useful delivery （Cui et al.,2004）. Physical-layer security under imperfect channel information is important for green relaying because low-power devices cannot assume precise or continuous channel tracking （Tang et al.,2014）. Transformer research is relevant to future wireless analytics because attention mechanisms can model long-range dependencies in sensing, channel, and traffic data （Vaswani et al.,2017）.

Security is also a green issue. Insecure communication can lead to false data, malicious control, privacy breaches, or system shutdowns. The environmental cost of such failures can be significant in industrial, agricultural, or infrastructure settings. A compromised irrigation network may waste water; a compromised factory-monitoring network may cause unsafe operation; a compromised environmental sensor may mislead policy decisions. Physical-layer security and interception-aware relay selection therefore belong within the sustainability logic of intelligent networks （Bloch et al.,2008）. Energy conservation surveys for sensor networks show that radio activity, sleep scheduling, and topology management are all central to sustainable device operation （Anastasi et al.,2009）.

The source manuscript's use of outage probability and intercept probability provides a useful conceptual basis for this broader argument. This paper extends the idea by treating outage and interception not only as technical probabilities but as indicators of green operational quality. Low outage reduces wasted energy; controlled interception risk protects the data integrity that green applications depend on. DeFi studies show that distributed systems create new risk surfaces when technical connectivity, trust, and transaction governance interact （Xu et al.,2024）.

Table 5. Managerial and policy implications for low-power intelligent networks.

Stakeholder	Decision focus	Recommended action	Expected green benefit
Network operator	Relay deployment density	Plan moderate relay density and avoid fixed-relay defaults	Lower maintenance and battery replacement burden
Device manufacturer	Low-power firmware design	Embed green relay scoring and adaptive sleep-wake policies	Improved battery lifetime and service reliability
Smart-city authority	Procurement criteria	Require reporting of energy per useful bit and interference responsibility	More credible sustainability assessment
Industrial user	Security-sensitive monitoring	Screen relays by interception exposure and criticality level	Reduced risk of data manipulation and false alarms
Regulator	Spectrum-sharing governance	Link secondary access rights to primary protection and energy discipline	Responsible and sustainable spectrum reuse

Note: Values are simulated or synthesized for methodological illustration, not taken from the source manuscript.

Table 5 emphasizes that the framework is not only a technical contribution. It offers decision criteria for network procurement, firmware design, infrastructure planning, and spectrum governance. Green communication cannot be achieved by engineers alone; it also requires organizations to specify performance indicators that reward responsible spectrum use.

5.3 Deployment Scenarios for Green Intelligent Networks

The proposed framework is especially suitable for smart agriculture. Agricultural sensing networks often cover wide spaces with uneven terrain, moisture variation, and weak power infrastructure. Sensors may sleep for long periods and wake only to transmit measurements or alarms. In this setting, a fixed relay design is unattractive because relays may be activated even when the channel is temporarily good. A green cognitive relay policy allows the network to use direct transmission after rainfall, when propagation conditions may improve, and to activate nearby relays during dry or obstructed conditions. The same principle applies to livestock monitoring, greenhouse control, and irrigation scheduling, where data are not always high volume but often need dependable delivery when abnormal conditions occur. Learning-to-optimize approaches show that interference management can be framed as a trainable mapping from network state to power-control action （Sun et al.,2018）.

Industrial sensing provides a second important scenario. Factories and warehouses contain metal structures, moving vehicles, rotating equipment, and electromagnetic interference. Direct links can be unstable, and installing additional wired communication is often expensive. Relay-assisted cognitive transmission can improve coverage, but energy use and interference must be controlled because many industrial sensors operate on small batteries or energy-harvesting modules. A green relay controller can rank relays according to both machine-proximity reliability and battery cost. It can also avoid relay nodes located close to sensitive control equipment or untrusted access zones. In this way, reliability-aware relaying becomes part of industrial risk governance rather than merely a communication enhancement. Cognitive machine-to-machine work explains why IoT protocol stacks must support both spectrum awareness and application-level service differentiation （Aijaz & Aghvami,2015）.

Urban environmental monitoring is a third scenario. Cities increasingly deploy low-power nodes for air quality, noise, flooding, traffic, and infrastructure vibration. These devices may be installed on lamp posts, bridges, drains, and roadside cabinets, where maintenance access is uneven. Spectrum sharing is attractive because municipal networks may need to coexist with commercial and public-service communication. However, urban environments also contain dense interference and security risks. The proposed framework helps municipal operators evaluate whether a relay path is green not only by its signal strength but also by its energy burden, interference footprint, and exposure to unauthorized reception. This can support procurement rules that require vendors to report energy per useful bit and responsible spectrum behavior. Cyber-physical system research clarifies why wireless reliability affects not only packet delivery but also the stability of connected physical operations （Lu,2017a）.

A fourth scenario is disaster-resilient sensing. During floods, storms, fires, or infrastructure failures, low-power sensors and temporary relays may be deployed rapidly. The energy supply may be uncertain, and primary emergency communication must not be disturbed. A green cognitive relay policy can enforce conservative primary protection while still allowing secondary status updates to be delivered through short cooperative paths. The framework is not designed to replace emergency communication systems. Rather, it provides a method for supporting auxiliary sensing and situational awareness without creating additional spectrum stress. This feature is relevant for climate adaptation strategies, where communication resilience and energy restraint must be developed together. Energy beamforming research demonstrates how even limited feedback can support energy-aware radio decisions under constrained information conditions （Zhang & Zhang,2014）.

5.4 Implementation Architecture and Governance Requirements

Implementation does not require a heavy centralized optimizer. A practical architecture may include three layers. The device layer collects local link-quality and residual-energy indicators. The edge gateway layer aggregates these indicators and updates relay-score weights according to application priority. The management layer records performance summaries, including outage events, energy per useful bit, primary-interference warnings, and security-exposure flags. This layered design is important because low-power devices should not perform expensive computation whenever a packet is sent. The edge gateway can perform most ranking and threshold adjustment, while devices execute simple transmission decisions. Systematic reviews of IoT applications confirm that communication requirements differ sharply across environmental sensing, transport, health, agriculture, and industrial use cases （Asghari et al.,2019）.

Governance is equally important. Green spectrum sharing should be auditable, especially when secondary devices operate in shared bands. Operators should be able to explain why a relay was selected, how the selected power level protected primary users, and whether the resulting path respected the energy budget. Transparent logs are useful for regulators, infrastructure owners, and enterprise sustainability teams. They also make it possible to compare vendors and deployment designs. A system that reports only throughput or packet delivery ratio gives an incomplete picture; a green system should report reliability, energy, interference responsibility, and security exposure together. Blockchain-technology trend analysis further suggests that secure distributed records may complement physical-layer protections in future intelligent networks （Zheng & Lu,2022）.

The framework also supports adaptive service classes. Not all packets require the same treatment. Routine temperature readings may be delayed or sent through the lowest-energy route. Safety alarms may receive a higher reliability weight and trigger relay activation more readily. Sensitive data may receive a stricter security-exposure penalty. This service-class logic prevents over-engineering of routine communication while protecting critical traffic. It also aligns with the broader principle of green digital design: allocate resources according to the social and operational value of the information being transmitted. Deep learning surveys in mobile networking show that data-driven control can support radio-resource decisions when analytic models become difficult to maintain （Zhang et al.,2019）.

Finally, operators should treat the relay-score weights as governance parameters rather than purely technical constants. A farm, a port, a hospital logistics unit, and a city authority may reasonably choose different weights. The purpose of the model is not to impose one universal definition of green communication. It is to provide a structured method for making trade-offs visible. Once these trade-offs are visible, stakeholders can decide whether their priority is battery lifetime, reliability, primary protection, security, or balanced sustainability. This transparency distinguishes green spectrum-sharing governance from opaque algorithmic network optimization. Physical-layer security surveys indicate that multiuser networks must evaluate secrecy, reliability, and resource allocation together （Mukherjee et al.,2014）.

6. Limitations and Future Research

This study has several limitations. First, the simulation analysis is illustrative rather than calibrated to a single field deployment. Real networks may include mobility, irregular topology, bursty traffic, hardware heterogeneity, and weather-driven propagation changes. Future work should validate the green relay score using testbed experiments in farms, factories, campuses, and smart-city corridors. Second, the model assumes that local energy and link indicators can be estimated with reasonable accuracy. In ultra-low-power networks, measurement itself consumes energy. Future research should study how to minimize the overhead of green decision data collection （Zhang et al.,2019）. Green wireless trade-off analysis provides the theoretical motivation for treating energy, spectrum efficiency, and quality of service as linked objectives （Chen et al.,2011）.

Third, the framework treats interception exposure as a probabilistic risk zone rather than as a fully strategic adversary. More advanced attacks may adapt to relay policies, infer network schedules, or exploit control messages. Future work could integrate adversarial learning, friendly jamming, or reconfigurable intelligent surfaces into the green spectrum-sharing problem. However, such enhancements should be evaluated carefully because security mechanisms can also consume energy and create new interference （Tang et al.,2014）. Information-system blockchain research suggests that communication trust must be embedded into the architecture of digital systems rather than added only after deployment （Lu,2022）.

Fourth, the model uses a transparent scoring rule rather than deep reinforcement learning. This choice was deliberate because interpretability and low computational overhead are valuable for green networks. Nevertheless, learning-based policies may outperform fixed scoring when the environment changes over time. Future research could compare transparent score-based control with lightweight reinforcement learning or federated learning, while measuring not only outage and throughput but also the energy cost of training and inference （Mnih et al.,2015）. Spectrum-sensing algorithm reviews show that detection performance and implementation overhead remain major barriers for practical cognitive access （Yucek & Arslan,2009）.

Finally, future studies should connect green spectrum sharing with broader sustainability accounting. Energy per useful bit is a useful operational metric, but it does not capture manufacturing emissions, device replacement cycles, field maintenance travel, or end-of-life disposal. A complete green assessment would integrate communication performance with lifecycle analysis and circular-economy considerations （Bibri,2018）. Network-lifetime studies show that lifetime maximization cannot be reduced to one-hop transmit power because topology and routing decisions also shape battery depletion （Yetgin et al.,2017）.

7. Conclusion

This paper developed a green spectrum-sharing framework for low-power intelligent networks. Building on the research direction of cognitive multi-hop relaying, primary QoS protection, cooperative transmission, and security-reliability analysis, it proposed a reliability-aware relay and power selection procedure that explicitly includes energy discipline and interception guardrails. The framework shifts attention from outage minimization alone to a broader green communication objective: deliver useful data reliably while consuming less energy, protecting the primary network, and avoiding insecure relay choices. Quantum machine learning research illustrates how advanced computational paradigms may later support more complex radio-resource learning problems （Lu et al.,2024a）.

Simulation-based analysis shows that the proposed green score relay policy outperforms direct transmission, fixed relaying, QoS-only relaying, and energy-only relaying in balanced performance. It reduces normalized energy per useful bit, lowers outage probability, and keeps interference and security indicators within acceptable ranges. Sensitivity analysis further shows that hop count and energy budget must be tuned jointly, with moderate hop counts often producing the most attractive green reliability scores. Deep reinforcement learning research provides a methodological foundation for future adaptive relay-control agents, although this study deliberately keeps the proposed score transparent （Mnih et al.,2015）.

The central conclusion is that green spectrum sharing is not achieved by spectrum reuse alone. It emerges from responsible control of power, relay activation, interference, and security exposure. For smart agriculture, industrial sensing, urban environmental monitoring, and other low-power intelligent networks, the proposed framework offers a practical design pathway for sustainable wireless connectivity. The competitiveness-and-environment literature supports the idea that environmental discipline can improve design quality rather than merely impose constraint costs （Porter & van der Linde,1995）.

Acknowledgement

The authors thank the anonymous reviewers for their constructive comments. This research received no external funding. The authors also acknowledge the open research discussions on green wireless networking, cognitive radio, and intelligent sensing systems that informed the conceptual design of this study. Industry 4.0 surveys show that intelligent production environments depend on reliable sensing and communication infrastructure across multiple cyber-physical layers （Lu,2017b）.

Declarations

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: The numerical data used in the illustrative simulation are synthetic and can be generated from the parameters described in the paper. No proprietary dataset is redistributed.

Ethics statement: This article does not involve human participants, animal experiments, or identifiable personal records.

Reference

Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715-1729. https://doi.org/10.1007/s10796-022-10248-7

Buzzi, S., Chih-Lin, I., Klein, T. E., Poor, H. V., Yang, C., & Zappone, A. (2016). A survey of energy-efficient techniques for 5G networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 34(4), 697-709. https://doi.org/10.1109/JSAC.2016.2550338

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

Lu, Y., & Ning, X. (2020). A vision of 6G-5G's successor. Journal of Management Analytics, 7(3), 301-320. https://doi.org/10.1080/23270012.2020.1802622

Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications, 23(2), 201-220. https://doi.org/10.1109/JSAC.2004.839380

Bibri, S. E. (2018). The IoT for smart sustainable cities of the future: An analytical framework. Sustainable Cities and Society, 38, 230-253. https://doi.org/10.1016/j.scs.2017.12.034

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473. https://doi.org/10.1109/JIOT.2021.3060508

Cui, S., Goldsmith, A. J., & Bahai, A. (2004). Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks. IEEE Journal on Selected Areas in Communications, 22(6), 1089-1098. https://doi.org/10.1109/JSAC.2004.830916

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), 2322-2358. https://doi.org/10.1109/COMST.2017.2745201

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

Bi, S., Ho, C. K., & Zhang, R. (2015). Wireless powered communication: Opportunities and challenges. IEEE Communications Magazine, 53(4), 117-125. https://doi.org/10.1109/MCOM.2015.7081084

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

Goldsmith, A., Jafar, S. A., Maric, I., & Srinivasa, S. (2009). Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. Proceedings of the IEEE, 97(5), 894-914. https://doi.org/10.1109/JPROC.2009.2015717

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215-234. https://doi.org/10.1007/s10796-021-10221-w

Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. IEEE Transactions on Information Theory, 54(6), 2515-2534. https://doi.org/10.1109/TIT.2008.921908

Ghasemi, A., & Sousa, E. S. (2008). Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs. IEEE Communications Surveys & Tutorials, 10(2), 32-39. https://doi.org/10.1109/COMST.2008.4561831

Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

Brundage, M. P., Chang, Q., Li, Y., Arinez, J., & Xiao, G. (2016). Sustainable manufacturing performance indicators for a serial production line. IEEE Transactions on Automation Science and Engineering, 13(2), 676-687. https://doi.org/10.1109/TASE.2014.2373821

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847

Laneman, J. N., Tse, D. N. C., & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. IEEE Transactions on Information Theory, 50(12), 3062-3080. https://doi.org/10.1109/TIT.2004.838089

Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: A top-down survey. Computer Networks, 67, 104-122. https://doi.org/10.1016/j.comnet.2014.03.027

Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2025.2541199

Ju, H., & Zhang, R. (2014). Throughput maximization in wireless powered communication networks. IEEE Transactions on Wireless Communications, 13(1), 418-428. https://doi.org/10.1109/TWC.2013.112513.130760

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11), 4724-4734. https://doi.org/10.1109/TII.2018.2852491

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996-1015. https://doi.org/10.1002/sres.3151

Kohli, R., & Melville, N. P. (2019). Digital innovation: A review and synthesis. Information Systems Research, 30(1), 200-223. https://doi.org/10.1287/isre.2019.0834

Akan, O. B., Karli, O. B., & Ergul, O. (2009). Cognitive radio sensor networks. IEEE Network, 23(4), 34-40. https://doi.org/10.1109/MNET.2009.5191144

Lu, Y. (2019). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1-29. https://doi.org/10.1080/23270012.2019.1570365

Tang, X., Li, P., Han, Z., & Varshney, P. K. (2014). Wireless physical layer security with imperfect channel state information. IEEE Transactions on Information Forensics and Security, 9(7), 1201-1216. https://doi.org/10.1109/TIFS.2014.2325772

Anastasi, G., Conti, M., Di Francesco, M., & Passarella, A. (2009). Energy conservation in wireless sensor networks: A survey. Ad Hoc Networks, 7(3), 537-568. https://doi.org/10.1016/j.adhoc.2008.06.003

Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9). https://doi.org/10.1080/17517575.2024.2397630

Sun, H., Chen, X., Shi, Q., Hong, M., Fu, X., & Sidiropoulos, N. D. (2018). Learning to optimize: Training deep neural networks for interference management. IEEE Transactions on Signal Processing, 66(20), 5438-5453. https://doi.org/10.1109/TSP.2018.2866382

Aijaz, A., & Aghvami, A. H. (2015). Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective. IEEE Internet of Things Journal, 2(2), 103-112. https://doi.org/10.1109/JIOT.2015.2390775

Lu, Y. (2017a). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

Zhang, R., & Zhang, Y. C. (2014). Energy beamforming with one-bit feedback. IEEE Transactions on Vehicular Technology, 63(3), 1375-1381. https://doi.org/10.1109/TVT.2013.2286422

Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148, 241-261. https://doi.org/10.1016/j.comnet.2018.12.008

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2224-2287. https://doi.org/10.1109/COMST.2019.2904897

Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550-1573. https://doi.org/10.1109/SURV.2014.012314.00178

Chen, Y., Zhang, S., Xu, S., & Li, G. Y. (2011). Fundamental trade-offs on green wireless networks. IEEE Communications Magazine, 49(6), 30-37. https://doi.org/10.1109/MCOM.2011.5783982

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876-1907. https://doi.org/10.1080/17517575.2021.2008513

Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys & Tutorials, 11(1), 116-130. https://doi.org/10.1109/COMST.2009.090109

Yetgin, H., Cheung, K. T. K., El-Hajjar, M., & Hanzo, L. H. (2017). A survey of network lifetime maximization techniques in wireless sensor networks. IEEE Communications Surveys & Tutorials, 19(2), 828-854. https://doi.org/10.1109/COMST.2017.2650979

Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024a). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., et al. (2015). Human-level control through deep reinforcement learning. Nature, 518, 529-533. https://doi.org/10.1038/nature14236

Porter, M. E., & van der Linde, C. (1995). Toward a new conception of the environment-competitiveness relationship. Journal of Economic Perspectives, 9(4), 97-118. https://doi.org/10.1257/jep.9.4.97

Lu, Y. (2017b). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

Ye, H., Li, G. Y., & Juang, B. H. (2018). Power of deep learning for channel estimation and signal detection in OFDM systems. IEEE Wireless Communications Letters, 7(1), 114-117. https://doi.org/10.1109/LWC.2017.2757490

Nizetic, S., Solic, P., Gonzalez-de-Artaza, D. L., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. Journal of Cleaner Production, 274, 122877. https://doi.org/10.1016/j.jclepro.2020.122877

Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511

Grover, P., & Sahai, A. (2010). Shannon meets Tesla: Wireless information and power transfer. 2010 IEEE International Symposium on Information Theory, 2363-2367. https://doi.org/10.1109/ISIT.2010.5513711

Varshney, L. R. (2008). Transporting information and energy simultaneously. 2008 IEEE International Symposium on Information Theory, 1612-1616. https://doi.org/10.1109/ISIT.2008.4595260

Feng, D., Jiang, C., Lim, G., Cimini, L. J., Feng, G., & Li, G. Y. (2013). A survey of energy-efficient wireless communications. IEEE Communications Surveys & Tutorials, 15(1), 167-178. https://doi.org/10.1109/SURV.2012.020212.00049

Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

Zhang, R., & Ho, C. K. (2013). MIMO broadcasting for simultaneous wireless information and power transfer. IEEE Transactions on Wireless Communications, 12(5), 1989-2001. https://doi.org/10.1109/TWC.2013.031813.120224

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1-2). https://doi.org/10.1080/17517575.2024.2448003

Liaskos, C., Nie, S., Tsioliaridou, A., Pitsillides, A., Ioannidis, S., & Akyildiz, I. (2018). A new wireless communication paradigm through software-controlled metasurfaces. IEEE Communications Magazine, 56(9), 162-169. https://doi.org/10.1109/MCOM.2018.1700659

Dangelico, R. M., & Pujari, D. (2010). Mainstreaming green product innovation: Why and how companies integrate environmental sustainability. Journal of Business Ethics, 95(3), 471-486. https://doi.org/10.1007/s10551-010-0435-0

Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383-402. https://doi.org/10.1080/23270012.2022.2089064

Clerckx, B., Bayguzina, E., Venkatesh, B., & Kim, D. I. (2019). Fundamentals of wireless information and power transfer: From RF energy harvester models to signal and system designs. Proceedings of the IEEE, 107(1), 11-30. https://doi.org/10.1109/JPROC.2018.2872619

Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3), 134-142. https://doi.org/10.1109/MNET.001.1900287

Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024b). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257-266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 7(6), 2180-2189. https://doi.org/10.1109/TWC.2008.060848

Melville, N. P. (2010). Information systems innovation for environmental sustainability. MIS Quarterly, 34(1), 1-21. https://doi.org/10.2307/20721412

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1-34. https://doi.org/10.1186/s40854-024-00668-6

Di Renzo, M., Debbah, M., Phan-Huy, D. T., Zappone, A., Alouini, M. S., Yuen, C., et al. (2019). Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come. EURASIP Journal on Wireless Communications and Networking, 2019, 129. https://doi.org/10.1186/s13638-019-1438-9

Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G be? IEEE Journal on Selected Areas in Communications, 32(6), 1065-1082. https://doi.org/10.1109/JSAC.2014.2328098

Hart, S. L. (1995). A natural-resource-based view of the firm. Academy of Management Review, 20(4), 986-1014. https://doi.org/10.5465/amr.1995.9512280033

Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024c). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431-440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

O'Shea, T., & Hoydis, J. (2017). An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4), 563-575. https://doi.org/10.1109/TCCN.2017.2758370

Seuring, S., & Muller, M. (2008). From a literature review to a conceptual framework for sustainable supply chain management. Journal of Cleaner Production, 16(15), 1699-1710. https://doi.org/10.1016/j.jclepro.2008.04.020

Zappone, A., Di Renzo, M., & Debbah, M. (2019). Wireless networks design in the era of deep learning: Model-based, AI-based, or both? IEEE Transactions on Communications, 67(10), 7331-7376. https://doi.org/10.1109/TCOMM.2019.2924010

Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjoland, H., & Tufvesson, F. (2021). 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. Proceedings of the IEEE, 109(7), 1166-1199. https://doi.org/10.1109/JPROC.2021.3061701

Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. J. A. (2019). The roadmap to 6G: AI empowered wireless networks. IEEE Communications Magazine, 57(8), 84-90. https://doi.org/10.1109/MCOM.2019.1900271

Bennis, M., Debbah, M., & Poor, H. V. (2018). Ultrareliable and low-latency wireless communication: Tail, risk, and scale. Proceedings of the IEEE, 106(10), 1834-1853. https://doi.org/10.1109/JPROC.2018.2867029

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1706.03762