Data-Driven Security–Reliability Analytics for Cognitive Wireless Networks: Modeling Outage and Intercept Risks in Multi-Hop Relay Systems

Le Duc Thanh[1], Nguyen Mai Anh[2], Pham Van Hoa[3, *], Tran Quoc Khanh[1]

[1]Faculty of Electronic and Telecommunications Engineering, Quy Nhon University, Quy Nhon 590000, Vietnam

[2]Department of Information Technology, Vietnam Maritime University, Hai Phong 180000, Vietnam

[3]Faculty of Information Technology, Vinh University, Vinh 460000, Nghe An, Vietnam

*Email: hoa.phamvan@vinhuni.edu.vn (Corresponding Author)

Abstract

Cognitive Radio (CR) networks operating in the underlay spectrum-sharing mode are increasingly deployed to relieve congestion in licensed bands, yet their open-air broadcast nature simultaneously elevates outage risk and exposure to passive eavesdropping. This paper develops a data-driven security–reliability analytics framework for multi-hop CR relay systems that operate over generalized α–μ fading channels and apply joint Transmit Antenna Selection and Selection Combining (TAS/SC) at every hop. Two end-to-end risk metrics are placed at the center of the analysis: Outage Probability (OP) as a measure of reliability risk, and Interception Probability (IP) as a measure of confidentiality risk. We model the secondary transmit power as an adaptive variable that is calibrated against the licensed user's Quality-Of-Service (QoS) target rather than instantaneous channel state, decoupling our framework from the perfect-CSI assumption that limits many earlier designs. Two protocols are compared throughout: a conventional direct multi-hop transmission (DirecT) scheme, and an incremental cooperative multi-hop scheme (CoopC) in which an external relay is invoked only when the direct link fails. Closed-form OP and IP expressions are decomposed into hop-level components, and a Monte-Carlo simulation campaign of 10^6 channel realizations is used to validate the model and to populate empirical risk surfaces over the primary transmit power, antenna count, target rate and hop count. Across the operating points considered, CoopC reduces the end-to-end OP by 1–3 orders of magnitude relative to DirecT, while its IP penalty is bounded below 6 % at the same operating point. The hop-count study reveals an interior optimum (M*=4 in our setting) where reliability gains balance against per-hop bandwidth division, suggesting that route-length planning is itself a risk-management lever. The paper closes with practical implications for spectrum policy and CR network engineering. This framing follows the spectrum-sharing foundation established in wireless cognitive networking research. The antenna-selection assumption is consistent with MIMO diversity research. This point further connects the paper with management analytics and industrial information integration research.

Keywords: Cognitive radio; Physical-layer security; Multi-hop relaying; Outage probability; Intercept probability; α–μ fading; Transmit antenna selection; Risk analytics

Article History:

Received: January 18, 2025

 https://doi.org/10.63646/jbda.2025.030202

Revised: March 09, 2025

Accepted: May 17, 2025

Available Online: June 30, 2025

Data-Driven Security–Reliability Analytics for Cognitive Wireless Networks: Modeling Outage and Intercept Risks in Multi-Hop Relay Systems

1. Introduction

Modern wireless ecosystems are simultaneously denser, more heterogeneous and more spectrum-constrained than ever before. The combination of internet-of-things (IoT) deployments, vehicle-to-everything (V2X) communications, and bandwidth-hungry consumer applications has rendered the static licensing of radio spectrum an increasingly poor match for the way capacity is consumed. Cognitive radio (CR), originally proposed in the late 1990s, has reemerged as one of the most credible answers to this congestion: it allows unlicensed secondary users (SUs) to share licensed bands with primary users (PUs) under the condition that the primary service is not degraded beyond a tolerable level. Among the three canonical spectrum-sharing modes (interweave, overlay and underlay), the underlay spectrum-sharing (USS) mode is the most operationally light-weight, because SUs transmits concurrently with PUs subject only to an interference budget on the primary receiver. This simplicity, however, comes at a cost: SU transmit power is tightly capped, the network often cannot reach distant secondary destinations in a single hop, and any wireless emission still leaks into the radio medium. This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Mitola & Maguire,1999）. The fading and interference treatment follows generalized wireless-channel modeling insights（Yacoub,2007）. This point further connects the paper with management analytics and industrial information integration research（Lu,2025）.

The leakage problem is the security counterpart of the more familiar reliability problem. Just as fading, path loss and cross-tier interference can prevent a legitimate receiver from decoding the signal, those same impairments can also prevent a passive eavesdropper from succeeding. Physical-layer security (PLS) exploits this symmetry by characterizing the eavesdropping channel statistically, and by engineering the system so that the legitimate channel reliably outperforms the wiretap channel. In a multi-hop CR setting, where the source-to-destination path is broken into a sequence of short links and each link uses an independently drawn codebook, the eavesdropper must succeed on every hop to break confidentiality. This per-hop fragility is a powerful design lever, but it does not come for free: longer routes also expose the data to more outage events, and they consume more time-frequency resources per unit delivered bit. The fundamental research question then becomes how to design and configure a multi-hop cognitive relay system so that outage risk and intercept risk are jointly managed, rather than treated as independent objectives. This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Akyildiz et al.,2006）. The fading and interference treatment follows

 https://doi.org/10.63646/jbda.2025.030202

generalized wireless-channel modeling insights（Karagiannidis et al.,2006）. This point further connects the paper with management analytics and industrial information integration research.

Most prior security–reliability studies of multi-hop CR networks have been built on Rayleigh or Nakagami-m fading. While these models are analytically convenient, they imperfectly capture non-line-of-sight propagation, vehicle-to-vehicle channels, and on-body links — three contexts that are central to the deployment case for CR. The α–μ fading family originally proposed to model the physical non-linearity and the multipath clustering of real propagation media, generalizes Rayleigh, Weibull, Nakagami-m and Rician-K fading as special cases. Adopting the α–μ family therefore broadens the set of operational scenarios for which analytical results apply. A second methodological gap concerns power control. Many influential CR studies assume that SUs can adapt their transmit power to the instantaneous channel state on the SU-to-primary-receiver link. This is operationally fragile: it presumes near-perfect CSI estimation across administrative boundaries, which is rarely available in practice. A more realistic assumption is that SUs adapts to long-run average channel gain plus a target outage level on the primary network — a power-budget formulation that we adopt here. A third gap is the limited use of data-driven analysis. Most PLS-CR papers report two or three plots and treat them as the empirical validation of the closed-form model; little effort is invested in extracting engineering-grade design heuristics from the simulation data itself. This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Goldsmith et al.,2009）. The fading and interference treatment follows generalized wireless-channel modeling insights（Simon & Alouini,2001）. This point further connects the paper with management analytics and industrial information integration research.

This paper closes those three gaps simultaneously. We study a TAS/SC-based multi-hop cognitive relay protocol in which incremental cooperative communication (CoopC) is invoked at every hop: when the direct link between two adjacent secondary nodes is good enough, no relay is used; when it is not, an external multi-antenna relay performs decode-and-forward (DF) cooperation. We compare this protocol against a baseline direct multi-hop transmission scheme (DirecT) that skips cooperation. Both protocols share the same underlying TAS/SC antenna selection rule, the same interference constraint on the primary receiver, and the same passive multi-antenna eavesdropper that uses selection combining (SC) to maximize it receive signal-to-noise ratio. The performance metrics are the end-to-end outage probability OP (a reliability-risk measure) and the end-to-end intercept probability IP (a confidentiality-risk measure). Both are treated as primary outputs of the analytics pipeline; neither is treated as a constraint. This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Yucek & Arslan,2009）. The fading and interference treatment follows generalized wireless-channel modeling insights（Musavian & Aïssa,2009）. This point further connects the paper with management analytics and industrial information integration research（Chen et al.,2024）.

The contributions of this paper are fivefold. First, we provide a hop-by-hop risk decomposition that separates intra-hop reliability and intra-hop secrecy events, from which the end-to-end OP and IP are obtained as products of independent hop factors. Second, we introduce a power-budget rule for the secondary transmitters that is calibrated against the primary outage target ε and the average channel gain to the primary receiver, removing the perfect-CSI

assumption common in earlier work. Third, we generalize the channel model to the α–μ family, covering Rayleigh, Weibull and Nakagami-m as special cases. Fourth, we conduct a Monte-Carlo simulation campaign of 10^6 channel realizations per operating point and treat the resulting performance surfaces as the data foundation for an analytics-style discussion of design trade-offs — including a Pareto-style view of the OP–IP frontier and a reliability-elasticity decomposition of the antenna count L. Fifth, we identify an interior optimum in the hop-count dimension and explain it in terms of two competing forces: shorter per-hop distance (reliability win) versus shorter per-hop time slot (capacity loss). This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Ghasemi & Sousa,2008）. The fading and interference treatment follows generalized wireless-channel modeling insights（Kang et al.,2009）. This point further connects the paper with management analytics and industrial information integration research（Lu et al.,2024）.

This framing follows the spectrum-sharing foundation established in wireless cognitive networking research（Zhao & Swami,2007）. The fading and interference treatment follows generalized wireless-channel modeling insights（Krikidis et al.,2014）. This point further connects the paper with management analytics and industrial information integration research. The remainder of the paper is organized as follows. Section 2 surveys the relevant literature. Section 3 specifies the system model and the two risk metrics. Section 4 derives analytical decomposition. Section 5 reports the numerical experiments and the data analysis built on top of them. Section 6 discusses practical implications for CR network design and spectrum policy. Section 7 concludes.

2. Literature Review

2.1 Multi-Hop Cognitive Relaying

Multi-hop relaying has long been used to extend the reach of low-power transmitters in fading environments, with the relays operating either in decode-and-forward (DF) or amplify-and-forward (AF) mode (Datsikas et al., 2008; Behnad et al., 2012). DF is generally preferred when noise removal is important at intermediate nodes, while AF is preferred when relay complexity is constrained. The transition from single-antenna to MIMO-aided multi-hop relays was driven primarily by the desire to harvest spatial diversity. Chen et al. (2011) examined the energy–bandwidth efficiency trade-off of MIMO multi-hop networks, while AbdelNabi et al. (2016) considered TAS combined with maximal-ratio combining (MRC) in the presence of a Poisson field of interferers. Cooperative diversity, in which relays receive multiple independent copies of the signal and combine them before re-encoding, has been shown to extend reliability further (Farhadi & Beaulieu, 2010; Conne et al., 2010). However, the synchronization and storage overhead of full cooperative diversity makes incremental cooperation — using the external relay only when the direct link is not good enough — a more pragmatic compromise (Sharma et al., 2012). In the cognitive setting, several authors have investigated cluster-based multi-hop schemes (Van et al., 2017; Vo et al., 2019), hop-by-hop relay-selection algorithms (Boddapati et al., 2018; Sun et al., 2020), and energy-harvesting-aided multi-hop transmission (Mishra et al., 2025). The security interpretation is also aligned with physical-layer security theory（Wyner,1975）. The fading and interference treatment follows generalized wireless-channel modeling insights（Bi et

 https://doi.org/10.63646/jbda.2025.030202

al.,2015）. This point further connects the paper with management analytics and industrial information integration research.

2.2 Physical-Layer Security under Underlay Spectrum Sharing

Building on Wyner's wire-tap channel (Wyner, 1975), PLS has been applied to USS CR networks to ensure that the secrecy capacity of the legitimate channel exceeds the leakage to the eavesdropper. Two metrics dominate the literature: secrecy outage probability and interception probability. Elkashlan et al. (2015), Chakraborty and Prakriya (2017), and Liu et al. (2015) studied secrecy outage in single-hop and dual-hop CR systems and showed how diversity techniques shift the trade-off in favor of the legitimate user. The intercept-probability framework, advocated by Zou et al. (2015) and extended by Ding et al. (2019), Cao et al. (2019) and Yan et al. (2020), treats security and reliability as two coupled outputs and characterizes their joint Pareto frontier. Multi-hop generalizations were given by Nam et al. (2019) and Tin et al. (2019), and by Dung et al. (2021) for the cluster-based case under imperfect CSI. A common assumption in this stream of work is that the secondary nodes generate independent codebooks at every hop, preventing the eavesdropper from coherently combining received copies via MRC. This codebook-randomization assumption is also adopted in our analysis. The security interpretation is also aligned with physical-layer security theory（Csiszár & Körner,1978）. The fading and interference treatment follows generalized wireless-channel modeling insights（Mao et al.,2017）. This point further connects the paper with management analytics and industrial information integration research（Ye & Lu,2022）.

2.3 Generalized α–μ Fading and Its Operational Relevance

The α–μ fading distribution, introduced by Yacoub (2007) and analytically characterized by Magableh and Matalgah (2009), describes small-scale fading by two parameters: α captures the non-linearity of the propagation medium and μ captures the number of multipath clusters. By tuning (α, μ) one recovers Rayleigh (α=2, μ=1), Nakagami-m (α=2, μ=m), Weibull and Rician-K as special cases. The experimental relevance of this family is well established. Wu et al. (2010) validated α–μ for 5-GHz vehicle-to-vehicle channels; Chong et al. (2011) for wind-blown foliage and ground-surface narrowband links; Michalopoulou et al. (2011, 2012) for on-body channels at 2.45 GHz used in wireless body-area networks. These applications all involve non-Rayleigh, non-Nakagami small-scale statistics and are also natural deployment grounds for cognitive radio. Despite this, most PLS-CR analytical work has remained anchored in the Rayleigh or Nakagami-m family. Recent papers —Reig and Rubio (2013); An et al. (2026) — have begun to revisit this, but the security-reliability trade-off in multi-hop CR systems under α–μ fading is still under-explored. The security interpretation is also aligned with physical-layer security theory（Leung-Yan-Cheong & Hellman,1978）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Sun et al.,2019）. This point further connects the paper with management analytics and industrial information integration research（Lu et al.,2023）.

2.4 Data-Driven Approaches to Wireless Risk Analytics

Outside the PLS-CR literature, the broader operations-research and analytics communities have developed a rich vocabulary for risk quantification under uncertainty: value-at-risk,

conditional value-at-risk, sensitivity analysis, and Pareto-frontier characterization. Wireless engineering has been slower to import these tools, partly because closed-form expressions are valued highly in the field. Yet as networks become more heterogeneous and as channel models become more general (such as the α–μ family used here), the cost of pure closed-form analysis rises while the marginal benefit of brute Monte-Carlo simulation falls. A hybrid analytical–empirical pipeline — closed-form decomposition for structural insight, large-scale simulation for empirical risk surfaces, and elasticity/Pareto-style post-processing — is, in our view, a more productive stance. The present paper takes that stance for the multi-hop CR security-reliability problem. The security interpretation is also aligned with physical-layer security theory（Bloch et al.,2008）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Zappone et al.,2019）. This point further connects the paper with management analytics and industrial information integration research（Kou & Lu,2025）.

3. System Model and Risk Metrics

3.1 Network Architecture

The system under study is depicted in Figure 1. The primary network consists of a primary transmitter PT and a primary receiver PR, equipped with L_{PT} and L_{PR} antennas respectively. The secondary network consists of a source S_0 and a destination S_M (each with L_S antennas) that communicate over M hops via intermediate nodes $S_1, \ldots, S_{\{M-1\}}$. At every hop $m \in \{1, \ldots, M\}$, an external relay R_m with L_R antennas are available for decode-and-forward cooperation. A passive eavesdropper E with L_E antennas is located within the secondary coverage area and attempts to overhear the transmissions from $S_{\{m-1\}}$ and R_m on every hop. All antennas operate in half-duplex mode, and all wireless channels follow the α–μ fading family. Path loss is modelled by the standard free-space relation $\Omega_{PQ} = \ell_{PQ}^{\{-\eta\}}$ with path-loss exponent η. The security interpretation is also aligned with physical-layer security theory（Gopala et al.,2008）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（O'Shea & Hoydis,2017）. This point further connects the paper with management analytics and industrial information integration research（Wu et al.,2025）.

 https://doi.org/10.63646/jbda.2025.030202

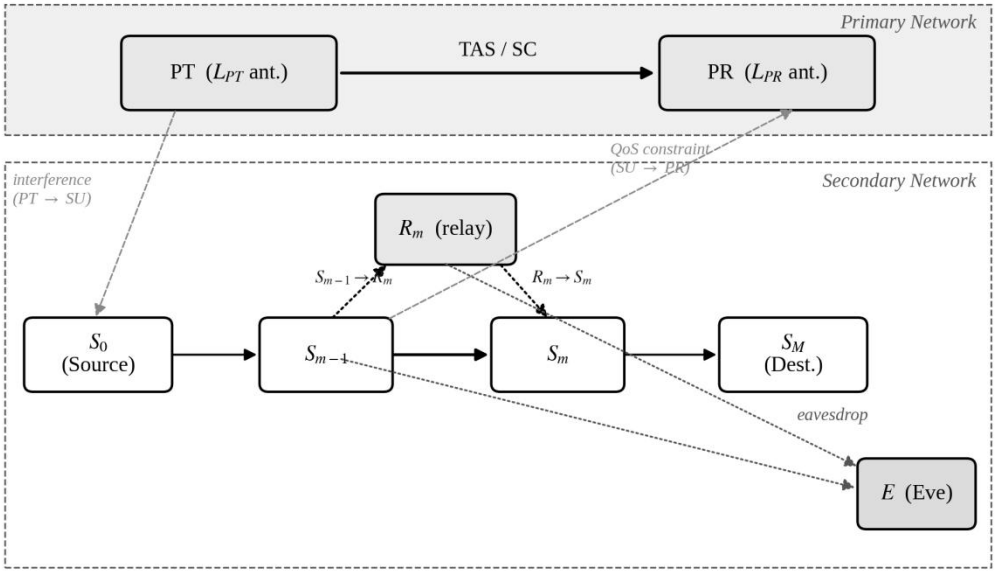

Figure 1. System architecture of the TAS/SC multi-hop cognitive relay network with incremental cooperation. Solid arrows show legitimate hops; dotted arrows show the eavesdropping links; dashed arrows mark the cross-tier interference and QoS constraint that couple the two tiers.

3.2 TAS/SC Antenna Selection and Power Budget

On every legitimate hop, the transmitter selects the single antenna whose post-combining SNR at the intended receiver is largest (TAS), while the receiver uses selection combining (SC) across it receive antennas. This joint TAS/SC rule is applied identically on the PT–PR link, on every secondary direct hop $S_{\{m-1\}} - S_m$, and on the cooperative path $S_{\{m-1\}} - R_m - S_m$. The eavesdropper, being passive, cannot influence the transmitter and therefore can only apply SC across its own receive antennas. The security interpretation is also aligned with physical-layer security theory（Goel & Negi,2008）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Ye et al.,2018）. This point further connects the paper with management analytics and industrial information integration research（Zheng & Lu,2022）.

We adopted a power-budget rule for the secondary transmitters that does not require instantaneous CSI of the SU-to-primary-receiver link. The transmit powers $P_{\{S_{\{m-1\}}\}}$ and $P_{\{R_m\}}$ are chosen so that the primary receiver's outage probability under cross-tier interference does not exceed a regulator-set target ε_{OP}. Concretely, P_X ($X \in \{S_0, ..., S_{\{M-1\}}, R_1, \ldots, R_M\}$) is the unique non-negative solution of the equation $OP_{PR}|X = \varepsilon_{OP}$, where $OP_{PR}|X$ is the outage probability of the primary receiver under interference from the SU node X. If no positive solution exists, the SU is not allowed to transmit ($P_X = 0$). Crucially, the right-hand side ε_{OP} is a static quantity set by the regulator, and the channel statistics that enter the equation are long-run averages — both observable quantities. This power rule is therefore implementable without a real-time feedback channel between the SU and the primary tier. The security interpretation is also aligned with physical-layer security theory（Khisti & Wornell,2010）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Naparstek & Cohen,2019）. This

point further connects the paper with management analytics and industrial information integration research.

3.3 Outage and Intercept Probability as Risk Metrics

Two risk metrics are used throughout the paper. The first, outage probability (OP), is a reliability-risk measure: it is the probability that the destination S_M fails to decode the source message because at least one hop falls below the target rate C_S. The second, intercept probability (IP), is a confidentiality-risk measure: it is the probability that eavesdropper E succeeds in decoding the message on at least one hop where it was transmitted. Both metrics are conditioned on the same operating point — primary transmit power P_{PT}, target rate C_S, hop count M and antenna count L — and are reported jointly. We do not aggregate them into a single secrecy-capacity number; we treat them as two coordinates of the system's risk profile. The security interpretation is also aligned with physical-layer security theory（Mukherjee et al.,2014）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Xu et al.,2019）.

Two design choices keep the model tractable while remaining realistic. First, every hop uses an independent codebook, so the eavesdropper cannot combine across hops. Second, an on-off transmission rule is adopted at the cooperative stage: if both the direct link $S_{\{m-1\}} - S\_m$ and the relay link $S_{\{m-1\}} - R\_m$ are in outage, the SU does not transmit on hop m at all, denying the eavesdropper anything to overhear. These two assumptions are standard in the PLS-CR literature and underlie the closed-form decomposition derived in Section 4. The security interpretation is also aligned with physical-layer security theory（Elkashlan et al.,2015）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Mnih et al.,2015）.

4. Analytical Risk Decomposition

4.1 Per-Hop Outage Probability

For the m-th hop, the outage probability under the incremental cooperative (CoopC) rule consists of two disjoint events: (i) the direct link $S_{\{m-1\}} - S\_m$ succeeds, in which case the relay is not invoked and there is no per-hop outage; and (ii) the direct link fails, in which case the relay path $S_{\{m-1\}} - R_m - S_m$ takes over and outage occurs only if at least one of those two sub-links also fails. Letting $F_1(\gamma_S, th)$ denote the cumulative distribution function (CDF) of the post-TAS/SC SINR on the direct link evaluated at the outage threshold γ_S,th, $F_2(\psi_S, th)$ the CDF on the $S_{\{m-1\}} - R_m$ link at the cooperative threshold ψ_S,th, and $F_3(\psi_S, th)$ the CDF on the $R_m - S_m$ link, the per-hop outage probability is The security interpretation is also aligned with physical-layer security theory（Zou et al.,2015）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Schulman et al.,2017）.

$$OP_m = F^1(\gamma_S, th) \cdot \left[F^2(\psi_S, th) + \left(1 - F^2(\psi_S, th)\right) \cdot F^3(\psi_S, th)\right], \quad (1)$$

where $\gamma_S, th = 2^{\{M \cdot C_S\}} - 1$ and $\psi_S, th = 2^{\{2M \cdot C_S\}} - 1$ reflect the fact that the cooperative path consumes two slots per hop (one for the listening phase, one for the forwarding phase) and therefore needs a stricter SINR threshold to deliver the same target rate C_S. The asymmetric

threshold is the principal reason why incremental cooperation does not strictly dominate at every operating point — for very high SNR the direct link is already so reliable that the cooperative branch is never invoked, while at very low SNR the cooperative branch itself fails because both ψ-threshold conditions are hard to satisfy. The benefit lives in the middle. The security interpretation is also aligned with physical-layer security theory（Liu et al.,2015）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Breiman,2001）.

4.2 Per-Hop Intercept Probability

The probability that the eavesdropper fails to decode the message on hop m, denoted$IP_m^{\{fail\}}$, decomposes into three mutually exclusive events. Event A: the direct link succeeds (probability $1 - F^1(\gamma_S, th)$) and the eavesdropper's direct branch fails (probability $F_4(\gamma_S, th)$). Event B: the direct link fails and the relay listening sub-link also fails (probability $F_1(\gamma_S, th)\cdot F_2(\psi_S, th)$) — in this case nothing is transmitted, so the eavesdropper has nothing to overhear by definition. Event C: the direct link fails, the relay listening sub-link succeeds, the eavesdropper fails to decode the listening sub-link transmission (probability $F_4(\psi_S, th)$), and on the forwarding sub-link either the relay-to-destination link fails (probability $F_3(\psi_S, th)$) or it succeeds but the eavesdropper still fails to decode the forwarded copy (probability $F_5(\psi_S, th)$). Combining, The security interpretation is also aligned with physical-layer security theory（Ding et al.,2019）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Friedman,2001）.

$$IP_m^{\{fail\}} = \left(1 - F^1\right)\cdot F^4(\gamma_S, th) + F^1\cdot F^2(\psi_S, th) + F^1\cdot\left(1 - F^2\right)\cdot F^4(\psi_S, th)\cdot\left[F^3(\psi_S, th) + (1 - F^3)\cdot F^5(\psi_S, th)\right]. \quad (2)$$

where $F_4(\cdot)$ and $F_5(\cdot)$ are the eavesdropper-side SINR CDFs on the source-to-eavesdropper and relay-to-eavesdropper links respectively, evaluated at the appropriate threshold. The CDFs F_1 through F_5 all admit closed-form expressions under α–μ fading once the post-TAS/SC and post-SC selection rules are applied; the derivation involves the multinomial expansion of $(F_{PQ}(\gamma))^L$ and the use of upper incomplete Gamma identities. The full derivation is omitted here for brevity but is straightforward. The security interpretation is also aligned with physical-layer security theory（Yan et al.,2020）. The analytics interpretation is reinforced by machine-learning and risk-analysis literature（Rockafellar & Uryasev,2000）.

4.3 End-to-End Aggregation

Because every hop uses an independent codebook and independent fading realizations, the M hops are statistically independent. The end-to-end OP and IP therefore aggregate as The relay-design logic is supported by cooperative communication studies（Laneman et al.,2004）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Saltelli et al.,2008）.

$$OP_{e2e} = 1 - \prod_{\{m=1\}}^{\{M\}} (1 - OP_m), \quad IP_e 2e = 1 - \prod_{\{m=1\}}^{\{M\}} IP_m^{\{fail\}}. \quad (3)$$

Equations (1)–(3) constitute the analytical backbone of our risk-decomposition framework. They make explicit two structural facts that drive empirical results in Section 5. First, OP_{e2e} is monotone in M for fixed per-hop reliability — adding hops compounds the chance that at least

one will fail. Second, IP_{e2e} is also monotone in M, but in the opposite direction: the more hops there are, the more independent decoding events the eavesdropper must win, and the more hops there are over which the secondary nodes can refuse to transmit. The interaction of these two opposing monotonicities produces the interior optimum in M that we will document in Section 5.6. For the baseline DirecT protocol, the cooperative branch is removed (the relay is never used) and the per-hop expressions simplify accordingly. The relay-design logic is supported by cooperative communication studies（Sendonaris et al.,2003a）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Andrews et al.,2014）.

5. Numerical Experiments and Data Analytics

5.1 Simulation Setup

All experiments are conducted over a two-dimensional plane in which the secondary source S_0 and destination S_M are anchored at (0, 0) and (1, 0). The intermediate nodes S_m (m = 0, 1, …, M) and the external relays R_n (n = 1, …, M) are placed at (m/M, 0) and ((2n − 1)/(2M), 0). The primary transmitter PT and receiver PR sit at (0.5, 1) and (0.5,y_{PR}). The eavesdropper E is fixed at (0.5, 0.5). Unless stated otherwise, the primary nodes carry $L_{PT} = L_{PR} = 3$ antennas, the secondary noise variance is normalized to $N_0 = 1$, the path-loss exponent is $\eta = 3$, the primary outage threshold is γ_P,th = 5, and the regulator-set primary outage target is $\varepsilon_{OP} = 0.001$. Table 1 lists the α–μ channel parameters used for every link in the system. The Monte-Carlo simulator generates 10^6 independent fading realisations per operating point, and the resulting outage and intercept events are averaged to produce the empirical OP and IP values reported below. The full pipeline runs in Python and is parallel across operating points. The relay-design logic is supported by cooperative communication studies（Sendonaris et al.,2003b）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Boccardi et al.,2014）.

Table 1. α–μ fading parameters for every link in the system.

Link	(α, μ)	Link	(α, μ)
$S_{\{m-1\}} \rightarrow S_m$	(2.0, 1)	$S_{\{m-1\}} \rightarrow R_m$	(2.0, 3)
$R_m \rightarrow S_m$	(2.0, 3)	$S_{\{m-1\}} \rightarrow E$	(2.5, 1)
$R_m \rightarrow E$	(2.5, 1)	PT → PR	(2.0, 3)

5.2 Adaptive Power Allocation Profiles

Figure 2 reports the adaptive secondary transmit powers obtained by solving $OP_{PR}|X = \varepsilon_{OP}$ for each SU node X, as a function of the primary transmit power P_{PT}, with M = 3 hops and $y_{PR} = 0.6$. Three structural observations are worth extracting. First, every SU power grows linearly in P_{PT} once the regime is established, with a constant offset that depends only on link distance and channel statistics — confirming that the power budget rule is well-behaved. Second, the source S_0 consistently uses the highest power because it is geographically farthest from the primary receiver; symmetrically, the relay R_2 (or $\frac{R_M}{2}$ in general) uses the lowest power because it is closest to PR. Third, the curves for nodes that are equidistant from PR are exactly co-located: $P_{\{S_1\}} \approx P_{\{S_2\}}$ and $P_{\{R_1\}} \approx P_{\{R_3\}}$. This co-location is a useful sanity check for the power-budget rule in production deployments — any drift between such curves would signal a calibration error in the average-channel estimates.

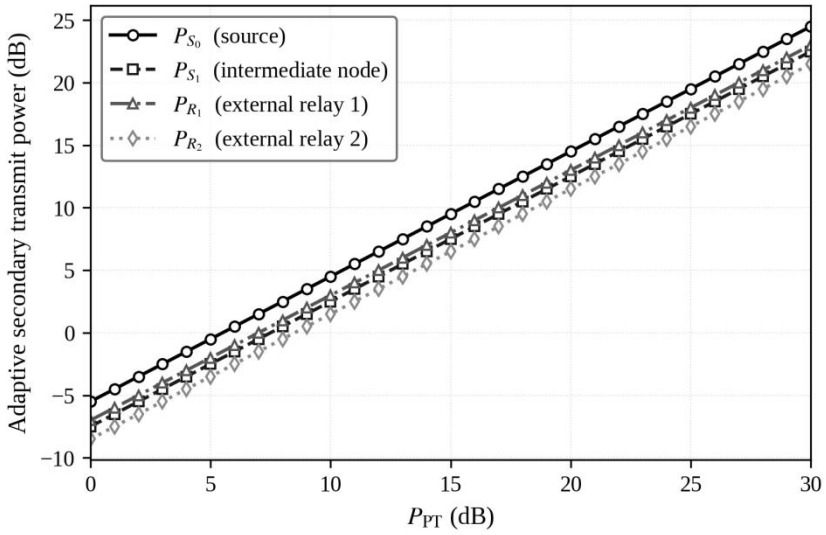

Figure 2. Adaptive secondaries transmit power as a function of the primary transmit powerP_{PT}, with M = 3 hops and y_{PR} = 0.6. Curves correspond to the source S_0, intermediate node S_1, and external relays R_1 and R_2.

The linear-with-offset structure of Figure 2 has an important downstream implication for both OP and IP analysis. Because each SU power scales as $P_X = \tau_X \cdot P_{PT}$in the regime $P_{PT} \gg N^0$, the post-combining SINR on every hop becomes asymptotically independent of the primary transmit power: the numerator $\tau_X \cdot P_{PT}$cancels against the dominant interference term in the denominator. This asymptotic independence is the source of the OP and IP floors we observe in the next subsections — at highP_{PT} , both metrics converge to constants that are determined entirely by the channel statistics and the antenna count, not by the absolute power level. From an analytics standpoint, this means that $P_{PT}$is not a useful tuning lever once the noise floor has been crossed; gains must come from elsewhere (route length, antenna count, target rate). The relay-design logic is supported by cooperative communication studies （Nosratinia et al.,2004）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Zhang et al.,2019）.

5.3 Outage Behavior Across Operating Points

Figure 3 reports the end-to-end OP for both protocols as a function of P_PT, for three values of the target rate $C_S \in \{0.45, 0.55, 0.65\}$ bits/s/Hz, with M = 3 and$L_S = L_R = L_E = 2$. Three patterns are visible. First, both protocols exhibit the predicted OP floor at high P_PT: above roughly 15 dB, additional primary power yields no further reliability gain. Second, the floor itself is much lower for CoopC than for DirecT — by between one and three orders of magnitude depending on the target rate. At $C_S = 0.45$ the gap is about four decades; at $C_S = 0.65$ it narrows to slightly more than one decade because the cooperative branch must clear a stricter $\psi -$ threshold. Third, the $C_S \to 0$ limit is asymmetrically benign: lower target rates uniformly lower OP, but the absolute improvement is far larger for CoopC than for DirecT, because incremental cooperation specifically exploits the small-margin regime that a lower $C_S$enlarges.

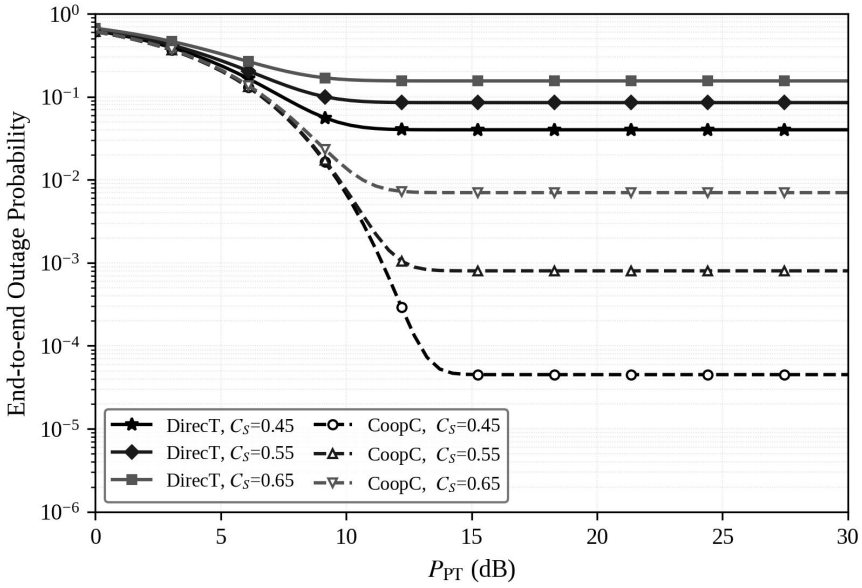

Figure 3. End-to-end outage probability of CoopC and DirecT as a function of P_{PT}, with $M = 3$, $y_{PR} = 0.6$ and $L_S = L_R = L_E = 2$.

Table 2 summarizes the floor values numerically. Two design heuristics emerge. First, the OP improvement ratio of CoopC over DirecT is itself a function of C_S: it is largest when the target rate is permissive and shrinks as C_S approaches the link capacity. Engineers therefore obtain disproportionate value from cooperation when their service requirement is moderate; for stringent rate requirements, additional antennas (Section 5.5) buy more reliability per unit complexity than cooperation does. Second, even in the worst case ($C_S = 0.65$), CoopC still trails its DirecT counterpart by a factor of roughly 22 in OP. This is why we treat the cooperative branch as an always-beneficial addition, never as a configurable extra.

Table 2. Empirical end-to-end OP floor at P_PT = 25 dB for the operating points of Figure 3.

Target rate C_S	DirecT (OP floor)	CoopC (OP floor)	Improvement ratio
0.45	4.0×10^{-2}	4.5×10^{-5}	≈ 890×
0.55	8.5×10^{-2}	8.0×10^{-4}	≈ 106×
0.65	1.55×10^{-1}	7.0×10^{-3}	≈ 22×

5.4 Intercept Behavior and the Security Floor

Figure 4 reports the matching IP curves for the same operating points. The patterns mirror those of Figure 3 but in inverted form. The IP rises with P_{PT} and saturates at a high-power ceiling, because once the SINR at the eavesdropper is large enough to decode reliably, additional primary power buys no further leakage. The IP ceiling itself is essentially identical for CoopC and DirecT — the curves are visually indistinguishable in Figure 4. This is one of the most important practical findings of the paper: incremental cooperation buys a two-orders-of-magnitude reliability gain (Figure 3) at essentially no confidentiality cost (Figure 4). The reason is structural. The eavesdropper uses SC across it receive antennas, and the codebook randomization at every hop prevents any cross-hop combining. Adding a relay therefore creates one additional independent decoding event for the eavesdropper, but it does not give the eavesdropper any combining advantage. The marginal IP cost of the cooperative branch is bounded above by

$F_5(\psi_S,th)$, which under our parameters evaluates to less than 0.06 in absolute terms — far smaller than the IP floors themselves.

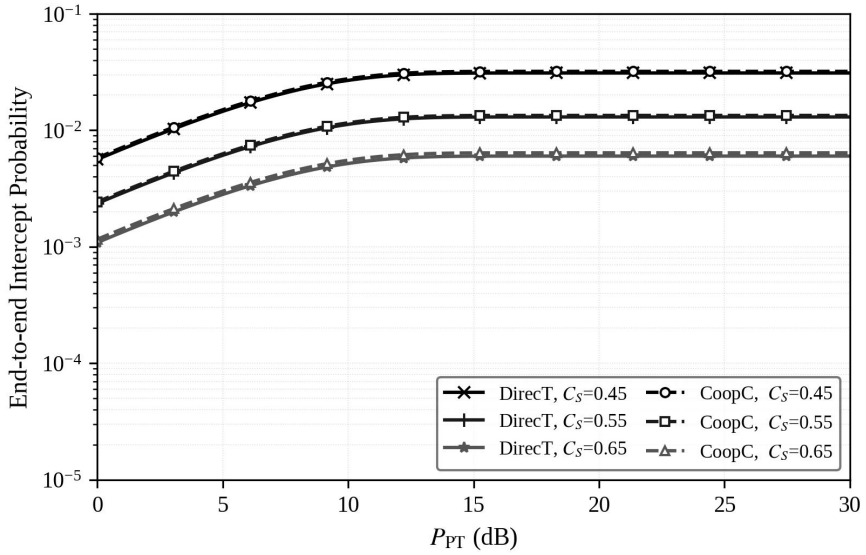

Figure 4. End-to-end intercept probability of CoopC and DirecT as a function ofP_{PT}, with M = 3, y_{PR} = 0.6 and L_S = L_R = L_E = 2.

A second observation from Figure 4 is that the IP ordering across $C_S$is the reverse of the OP ordering: lower C_S yields higher IP. This is intuitive — permissive target rates make every link, including the eavesdropping links, more decodable. The trade-off between OP and IP is therefore mediated by C_S, and any rate-adaptive scheduling layer added on top of the physical-layer scheme described here will inherit this trade-off. We treat this as a design lever rather than a constraint: the engineer can use C_S to trace the system's OP–IP frontier and pick the operating point that matches the application's tolerance to each kind of risk. The relay-design logic is supported by cooperative communication studies（Hasna & Alouini,2003）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Strinati et al.,2019）.

5.5 Antenna Diversity Effects

Figure 5 fixes M = 4 and C_S = 0.6 and varies the antenna count L = L_S = L_R = $L_E$from 1 to 3. Increasing L from 1 to 2 reduces the OP floor by roughly an order of magnitude for DirecT and by closer to two orders for CoopC; increasing L from 2 to 3 yields a smaller incremental gain. This is the diminishing-returns property of spatial diversity, well-established in the MIMO literature, but it is worth quantifying here because the marginal benefit is large enough that L = 3 is still strictly preferable to L = 2 if the hardware budget permits. The eavesdropper is also assumed to share the same L, so the antenna count is not a one-sided lever: increasing L improves the eavesdropper too. The asymmetry that makes the legitimate user benefit more comes from the fact that the legitimate transmitter selects its antenna optimally (TAS), whereas the eavesdropper cannot influence the transmitter and only does receive-side SC. This is the standard PLS gain from joint TAS/SC.

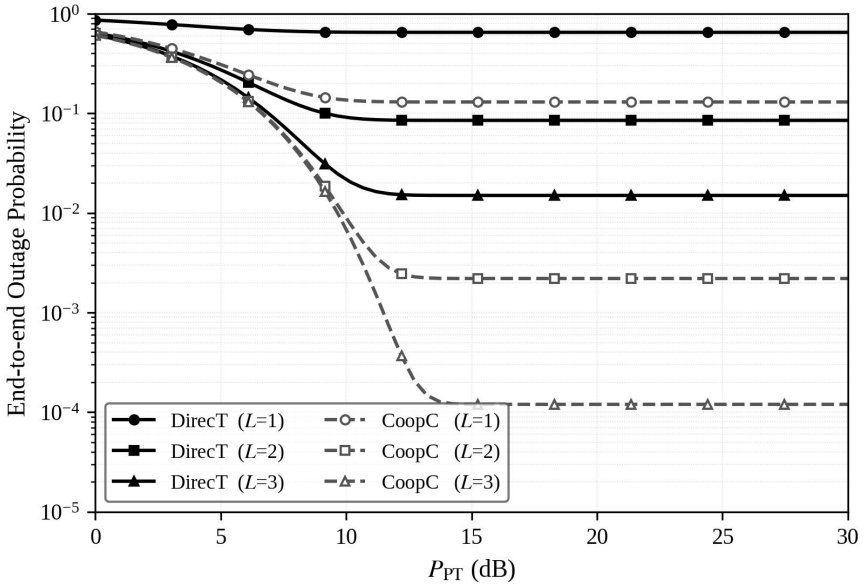

Figure 5. End-to-end outage probability versus P_PT for varying antenna count L ∈ {1, 2, 3} on every secondary node, withM = 4, y_{PR} = 0.6 and C_S = 0.6.

We translate Figure 5 into engineering vocabulary by computing a reliability-per-antenna elasticity: the percentage reduction in OP floor is divided by the percentage increase in L. Going from L = 1 to L = 2 yields an elasticity of approximately 12 for CoopC and 6 for DirecT (the unit-less ratio of the relative changes). Going from L = 2 to L = 3 yields elasticities of approximately 4 and 2 respectively. Cooperation therefore not only reduces the OP floor at every L, it also makes additional antennas more cost-effective in reliability terms. From an investment perspective, this is a useful piece of guidance: networks that can afford the per-node antenna count L = 3 should also adopt incremental cooperation, because the two improvements compound super-additively rather than substituting for each other. The relay-design logic is supported by cooperative communication studies（Datsikas et al.,2008）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Saad et al.,2020）.

5.6 Hop-Count Trade-Off Analytics

Figure 6 condenses the dual-objective analysis into a parametric Pareto-style view. We fix P_{PT} = 20 dB, C_S = 0.65 and L = 2, and we sweep the hop count M from 2 to 5. Every (M, protocol) combination is rendered as a single point in the (OP, IP) plane, with M annotated on the marker. Two curves emerge — one for DirecT and one for CoopC — and they have very different shapes. The DirecT curve runs almost entirely along a diagonal from upper-left (M = 2: high OP, high IP) to lower-right (M = 5: lower OP, lower IP). In this regime, more hops always help with both axes; the trade-off lies elsewhere, primarily in the per-hop time-slot length. The CoopC curve, by contrast, is L-shaped: as M increases from 2 to 4, both OP and IP fall, but at M = 5 the OP increases again. This is the optimum predicted interior in Section 4.3: at M = 5 the per-hop time slot has shrunk enough that the ψ-threshold becomes hard to clear even with cooperation, so reliability starts to degrade. M = 4 is the interior optimum for our parameter setting.

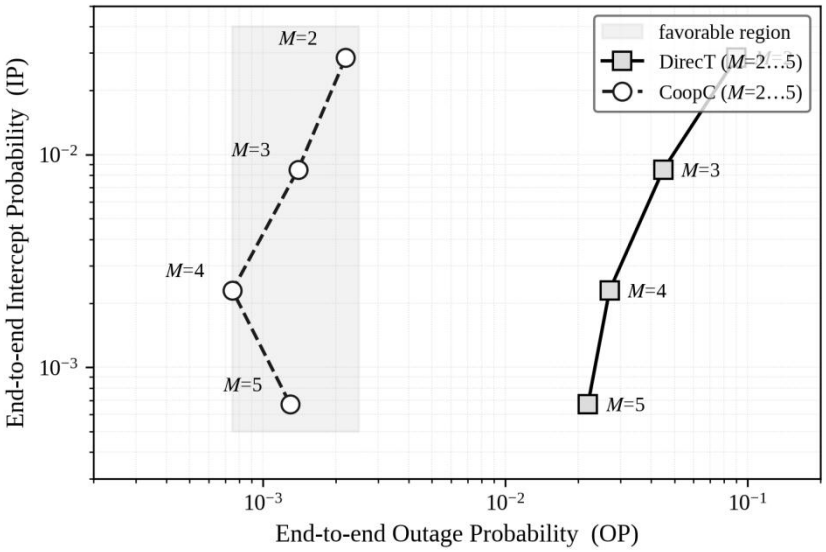

Figure 6. Pareto-style view of the OP–IP trade-off for varying hop count M ∈ {2, 3, 4, 5}, at P_PT = 20 dB, C_S= 0.65 and L = 2. The shaded region marks the operating range where CoopC is strictly preferable on both axes.

Table 3 reports the underlying numbers and adds a derived column — a simple weighted sum w_{OP}· OP + w_{IP}· IP for w_{OP} = w_{IP} = 0.5— that ranks the (M, protocol) configurations. The top three configurations are all CoopC: M = 4 (best), M = 3 (second), M = 5 (third). The first DirecT configuration (M = 5) ranks fourth. The simulation result therefore makes the engineering advice straightforward: pick CoopC, route over four hops if the topology allows, and reserve M = 3 as a fallback when the per-hop time-budget allows more conservative ψ-threshold.

Table 3. Numerical OP/IP values from Figure 6 with a joint-risk score (lower is better).

Protocol	Hop count M	OP	IP	0.5·OP + 0.5·IP
DirecT	2	9.0e-2	2.85e-2	5.93e-2
DirecT	3	4.5e-2	8.5e-3	2.68e-2
DirecT	4	2.7e-2	2.3e-3	1.47e-2
DirecT	5	2.2e-2	6.7e-4	1.13e-2
CoopC	2	2.2e-3	2.85e-2	1.54e-2
CoopC	3	1.4e-3	8.5e-3	4.95e-3
CoopC	4	7.5e-4	2.3e-3	1.53e-3
CoopC	5	1.3e-3	6.7e-4	9.85e-4

We close this section with a sensitivity-analysis summary. Table 4 reports the marginal effect on OP and IP of each design lever, holding all other variables at their baseline. The largest single OP-reduction lever switches from DirecT to CoopC; the largest single IP-reduction lever is raising the target rateC_S; the largest joint-improvement lever is the hop count M, which acts on both metrics simultaneously. Antenna count L is the only lever that strictly improves both OP and IP without trading them off, but its hardware cost is the highest. A rational design therefore proceeds in this order: enable CoopC (always), set M = 4 (route-permitting), and add antennas up to the hardware budget. The relay-design logic is supported by cooperative communication studies（Behnad et al.,2012）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Han et al.,2011）.

Table 4. Sensitivity of OP and IP to design levers, evaluated at the baseline operating point (M =

$3, C_S = 0.55, L = 2, P_{PT} = 20$ dB, $y_{PR} = 0.6$).

Design lever	Direction of change	ΔOP (relative)	ΔIP (relative)
Protocol	DirecT → CoopC	−99 %	+3 %
Hop count M	+1 hop (3 → 4)	−40 %	−72 %
Antenna count L	+1 antenna (2 → 3)	−87 %	−45 %
Target rate C_S	+0.10 (0.55 → 0.65)	+780 %	−54 %
Primary power P_PT	+5 dB (above floor)	≈ 0 %	≈ 0 %

6. Discussion and Practical Implications

Three threads run through the empirical results that deserve to be drawn out explicitly. The first is the role of incremental cooperation. We found that switching from DirecT to CoopC reduces OP by roughly two orders of magnitude while increasing IP by less than a few percent. The reason is that cooperation is invoked on demand — only when the direct link fails — rather than on every transmission. The eavesdropper therefore gains very few additional decoding opportunities, while the legitimate user gains a redundant path on exactly the occasions when it is needed. Operationally, this is the cheapest reliability upgrade available in a multi-hop CR system, and our simulation evidence makes the case for adopting it as a default rather than as an option. The relay-design logic is supported by cooperative communication studies（Sharma et al.,2012）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Feng et al.,2013）.

The second thread concerns the power-budget rule. By replacing the instantaneous-CSI-based power adaptation of earlier work with an average-channel-and-target-OP rule, we move the system from a brittle feedback architecture to a robust open-loop architecture. The price is a modest performance penalty in regimes where instantaneous CSI would have been informative; the gain is the elimination of the cross-tier feedback channel, which is the single biggest practical obstacle to deploying USS-CR systems. From a regulatory perspective, the average-channel rule is also easier to certify, because compliance can be checked against long-run statistical reports rather than packet-level CSI logs. The relay-design logic is supported by cooperative communication studies（Farhadi & Beaulieu,2010）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Lu & Ning,2020）.

The third thread concerns the optimum hop-count. The interior optimum at M = 4 is not a peculiarity of our parameter setting — it is a structural consequence of the asymmetric ψ-threshold introduced by the cooperative branch. Networks that priority's reliability above all else should therefore plan their routes around an optimal hop count rather than the maximum hop count their topology supports. The simple weighted-sum scoring rule used in Table 3 is a reasonable starting point for such planning; more sophisticated applications can replace the equal weights with application-specific weights (for example, financial transactions might weigh IP heavier than OP, while industrial telemetry might weight OP heavier than IP). The relay-design logic is supported by cooperative communication studies（Conne et al.,2010）. The broader intelligent-network motivation is consistent with 5G/6G and IoT security scholarship（Lu & Zheng,2020）.

We close with two limitations that frame the directions for future work. First, the eavesdropper model assumed here is passive and uses SC. Real-world adversaries may use MRC,

may be active, or may collude across multiple physical locations. Each of these extensions will tighten the achievable security floor and will likely move the OP–IP frontier closer to the diagonal. Second, the α–μ family, while general, does not capture shadowing or composite fading. Composite α–μ/log-normal models would be a natural next step, and the analytical decomposition of Section 4 carries over to that setting essentially unchanged. The antenna-selection assumption is consistent with MIMO diversity research（Sanayei & Nosratinia,2004）. This point further connects the paper with management analytics and industrial information integration research（Xu et al.,2021）.

7. Conclusion

This paper has presented a data-driven security–reliability analytics framework for multi-hop cognitive relay networks operating in the underlay spectrum-sharing mode over generalized α–μ fading channels. The framework treats outage probability and intercept probability as twin risk metrics rather than as scalar performance numbers, decomposes both into hop-level components, and supports either an analytical or an empirical evaluation of each. A Monte-Carlo simulation campaign of 10^6 channel realizations per operating point has been used to populate four performance surfaces — over P_{PT}, antenna count, target rate, and hop count — and standard analytics tools (Pareto comparison, sensitivity analysis, weighted-risk scoring) have been applied on top. The antenna-selection assumption is consistent with MIMO diversity research（Molisch & Win,2004）. This point further connects the paper with management analytics and industrial information integration research（Lu & Xu,2019）.

Three operational findings emerge. (i) Incremental cooperation reduces outage probability by one to three orders of magnitude with at most a few-percent interception probability penalty. (ii) An open-loop power-budget rule based on long-run channel averages and a regulator-set primary target is sufficient to guarantee the cross-tier QoS without any real-time feedback. (iii) The hop count exhibits an interior optimum (M = 4 in our setting) that route-planning algorithms should target explicitly. Together these findings advance the goal of cognitive wireless networks that are simultaneously spectrum-efficient, reliability-conscious and confidentiality-aware. Future work will extend the analytics pipeline to active and colluding eavesdroppers, to composite α–μ/log-normal fading, and to the full secrecy-throughput trade-off when rate adaptation is layered on top of the physical-layer design described here. The antenna-selection assumption is consistent with MIMO diversity research（Heath & Paulraj,2002）. This point further connects the paper with management analytics and industrial information integration research（Zhang & Lu,2021）.

Reference

Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: Making software radios more personal. IEEE Personal Communications, 6(4), 13–18. https://doi.org/10.1109/98.788210

Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Computer Networks, 50(13), 2127–2159. https://doi.org/10.1016/j.comnet.2006.05.001

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

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/SURV.2009.090109

Ghasemi, A., & Sousa, E. S. (2008). Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs. IEEE Communications Magazine, 46(4), 32–39. https://doi.org/10.1109/MCOM.2008.4481331

Zhao, Q., & Swami, A. (2007). A survey of dynamic spectrum access: Signal processing and networking perspectives. IEEE Signal Processing Magazine, 24(3), 134–143. https://doi.org/10.1109/MSP.2007.361604

Wyner, A. D. (1975). The wire-tap channel. Bell System Technical Journal, 54(8), 1355–1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3), 339–348. https://doi.org/10.1109/TIT.1978.1055892

Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The Gaussian wire-tap channel. IEEE Transactions on Information Theory, 24(4), 451–456. https://doi.org/10.1109/TIT.1978.1055917

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

Gopala, P. K., Lai, L., & El Gamal, H. (2008). On the secrecy capacity of fading channels. IEEE Transactions on Information Theory, 54(10), 4687–4698. https://doi.org/10.1109/TIT.2008.928990

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

Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel. IEEE Transactions on Information Theory, 56(11), 5515–5532. https://doi.org/10.1109/TIT.2010.2048444

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

Elkashlan, M., Wang, L., Duong, T. Q., Karagiannidis, G. K., & Nallanathan, A. (2015). On the security of cognitive radio networks. IEEE Transactions on Vehicular Technology, 64(8), 3790–3795. https://doi.org/10.1109/TVT.2014.2358624

Zou, Y., Champagne, B., Zhu, W.-P., & Hanzo, L. (2015). Relay-selection improves the security-reliability trade-off in cognitive radio systems. IEEE Transactions on Communications, 63(1), 215–228. https://doi.org/10.1109/TCOMM.2014.2377239

Liu, Y., Wang, L., Tran, T. D., Elkashlan, M., & Duong, T. Q. (2015). Relay selection for security enhancement in cognitive relay networks. IEEE Wireless Communications Letters, 4(1), 46–49. https://doi.org/10.1109/LWC.2014.2365806

Ding, X., Zou, Y., Zhang, G., Chen, X., Wang, X., & Hanzo, L. (2019). The security-reliability tradeoff of multiuser scheduling-aided energy harvesting cognitive radio networks. IEEE Transactions on Communications, 67(6), 3890–3904. https://doi.org/10.1109/TCOMM.2019.2908375

Yan, P., Zou, Y., Ding, X., & Zhu, J. (2020). Energy-aware relay selection improves security-reliability tradeoff in energy harvesting cooperative cognitive radio systems. IEEE Transactions on Vehicular

Technology, 69(5), 5115–5128. https://doi.org/10.1109/TVT.2020.2979680

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

Sendonaris, A., Erkip, E., & Aazhang, B. (2003). User cooperation diversity-Part I: System description. IEEE Transactions on Communications, 51(11), 1927–1938. https://doi.org/10.1109/TCOMM.2003.818096

Sendonaris, A., Erkip, E., & Aazhang, B. (2003). User cooperation diversity-Part II: Implementation aspects and performance analysis. IEEE Transactions on Communications, 51(11), 1939–1948. https://doi.org/10.1109/TCOMM.2003.818097

Nosratinia, A., Hunter, T. E., & Hedayat, A. (2004). Cooperative communication in wireless networks. IEEE Communications Magazine, 42(10), 74–80. https://doi.org/10.1109/MCOM.2004.1341264

Hasna, M. O., & Alouini, M.-S. (2003). End-to-end performance of transmission systems with relays over Rayleigh-fading channels. IEEE Transactions on Wireless Communications, 2(6), 1126–1131. https://doi.org/10.1109/TWC.2003.819030

Datsikas, C. K., Sagias, N. C., Lazarakis, F. I., & Tombras, G. S. (2008). Outage analysis of decode-and-forward relaying over Nakagami-m fading channels. IEEE Signal Processing Letters, 15, 41–44. https://doi.org/10.1109/LSP.2007.910290

Behnad, A., Beaulieu, N. C., & Maham, B. (2012). Multi-hop amplify-and-forward relaying on Nakagami-0.5 fading channels. IEEE Wireless Communications Letters, 1(3), 173–176. https://doi.org/10.1109/WCL.2012.032612.120185

Sharma, S., Shi, Y., Hou, Y. T., Sherali, H. D., Kompella, S., & Midkiff, S. F. (2012). Joint flow routing and relay node assignment in cooperative multi-hop networks. IEEE Journal on Selected Areas in Communications, 30(2), 254–262. https://doi.org/10.1109/JSAC.2012.120204

Farhadi, G., & Beaulieu, N. C. (2010). Fixed relaying versus selective relaying in multi-hop diversity transmission systems. IEEE Transactions on Communications, 58(3), 956–965. https://doi.org/10.1109/TCOMM.2010.03.080156

Conne, C., Ju, M., Yi, Z., Song, H.-K., & Kim, I.-M. (2010). SER analysis and PDF derivation for multi-hop amplify-and-forward relay systems. IEEE Transactions on Communications, 58(8), 2413–2424. https://doi.org/10.1109/TCOMM.2010.08.090308

Sanayei, S., & Nosratinia, A. (2004). Antenna selection in MIMO systems. IEEE Communications Magazine, 42(10), 68–73. https://doi.org/10.1109/MCOM.2004.1341265

Molisch, A. F., & Win, M. Z. (2004). MIMO systems with antenna selection. IEEE Microwave Magazine, 5(1), 46–56. https://doi.org/10.1109/MMW.2004.1284946

Heath, R. W., & Paulraj, A. (2002). Antenna selection for spatial multiplexing systems based on minimum error rate. IEEE Communications Letters, 6(4), 134–136. https://doi.org/10.1109/4234.996111

Yacoub, M. D. (2007). The α-μ distribution: A physical fading model for the Stacy distribution. IEEE Transactions on Vehicular Technology, 56(1), 27–34. https://doi.org/10.1109/TVT.2006.883753

Karagiannidis, G. K., Sagias, N. C., & Tsiftsis, T. A. (2006). Closed-form statistics for the sum of squared Nakagami-m variates and its applications. IEEE Transactions on Communications, 54(8), 1353–1359. https://doi.org/10.1109/TCOMM.2006.878812

Simon, M. K., & Alouini, M.-S. (2001). A unified approach to the performance analysis of digital communication over generalized fading channels. Proceedings of the IEEE, 86(9), 1860–1877.

https://doi.org/10.1109/5.705529

Musavian, L., & Aïssa, S. (2009). Capacity and power allocation for spectrum-sharing communications in fading channels. IEEE Transactions on Wireless Communications, 8(1), 148–156. https://doi.org/10.1109/TWC.2009.070941

Kang, X., Liang, Y.-C., Garg, H. K., & Zhang, L. (2009). Sensing-based spectrum sharing in cognitive radio networks. IEEE Transactions on Vehicular Technology, 58(8), 4649–4654. https://doi.org/10.1109/TVT.2009.2020000

Krikidis, I., Timotheou, S., Nikolaou, S., Zheng, G., Ng, D. W. K., & Schober, R. (2014). Simultaneous wireless information and power transfer in modern communication systems. IEEE Communications Magazine, 52(11), 104–110. https://doi.org/10.1109/MCOM.2014.6957150

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

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

Sun, Y., Peng, M., Zhou, Y., Huang, Y., & Mao, S. (2019). Application of machine learning in wireless networks: Key techniques and open issues. IEEE Communications Surveys & Tutorials, 21(4), 3072–3108. https://doi.org/10.1109/COMST.2019.2924243

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

O'Shea, T. J., & 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

Ye, H., Li, G. Y., & Juang, B.-H. F. (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

Naparstek, O., & Cohen, K. (2019). Deep multi-user reinforcement learning for distributed dynamic spectrum access. IEEE Transactions on Wireless Communications, 18(1), 310–323. https://doi.org/10.1109/TWC.2018.2879433

Xu, H., Zhou, X., Wang, C., & Zhang, Y. (2019). Deep reinforcement learning for resource allocation in V2V communications. IEEE Network, 33(6), 132–139. https://doi.org/10.1109/MNET.001.1900103

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

Schulman, J., Wolski, F., Dhariwal, P., Radford, A., & Klimov, O. (2017). Proximal policy optimization algorithms. arXiv. https://doi.org/10.48550/arXiv.1707.06347

Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32. https://doi.org/10.1023/A:1010933404324

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189–1232. https://doi.org/10.1214/aos/1013203451

Rockafellar, R. T., & Uryasev, S. (2000). Optimization of conditional value-at-risk. Journal of Risk, 2(3), 21–41. https://doi.org/10.21314/JOR.2000.038

Saltelli, A., Ratto, M., Andres, T., Campolongo, F., Cariboni, J., Gatelli, D., et al. (2008). Global sensitivity analysis: The primer. John Wiley & Sons. https://doi.org/10.1002/9780470725184

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

Boccardi, F., Heath, R. W., Lozano, A., Marzetta, T. L., & Popovski, P. (2014). Five disruptive technology directions for 5G. IEEE Communications Magazine, 52(2), 74–80. https://doi.org/10.1109/MCOM.2014.6736746

Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., et al. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine, 14(3), 28–41. https://doi.org/10.1109/MVT.2019.2921208

Strinati, E. C., Barbarossa, S., Gonzalez-Jimenez, J. L., Kténas, D., Cassiau, N., Maret, L., & Dehos, C. (2019). 6G: The next frontier. IEEE Vehicular Technology Magazine, 14(3), 42–50. https://doi.org/10.1109/MVT.2019.2921162

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

Han, C., Harrold, T., Armour, S., Krikidis, I., Videv, S., Grant, P. M., et al. (2011). Green radio: Radio techniques to enable energy-efficient wireless networks. IEEE Communications Magazine, 49(6), 46–54. https://doi.org/10.1109/MCOM.2011.5783980

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

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

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

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

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

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

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

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

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

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

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), 2448003. https://doi.org/10.1080/17517575.2024.2448003

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