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

Hongmei Su[1], Duo Zhang[1], Baoyang Zhao[1,*]

[1] Faculty of Business, Information & Human Sciences, Kuala Lumpur University of Science & Technology, Kuala Lumpur, Malaysia 43000

* Email: 175336404@qq.com (Corresponding Author)

Received 20 March 2025 · Revised 4 May 2025 · Accepted 18 June 2025 · Published 30 September 2025

Abstract

Cognitive radio (CR) networks operating in underlay spectrum-sharing mode can relieve congestion in licensed bands, but wireless transmission also exposes information to outage and passive eavesdropping. This paper develops a security–reliability analytics framework for multi-hop CR relay systems over generalized α–μ fading channels, with joint transmit antenna selection and selection combining at each hop. It examines end-to-end outage probability (OP) as a measure of reliability risk and intercept probability (IP) as a measure of confidentiality risk. Secondary transmit powers are calibrated against the primary user's quality-of-service target and long-run channel statistics. A conventional direct multi-hop transmission scheme is compared with an incremental cooperative scheme in which an external relay is invoked when the direct link fails. Hop-level analytical expressions and Monte Carlo results are used to examine the effects of primary transmit power, antenna count, target rate and hop count. For the tested configurations in Table 3, four-hop cooperation has the lowest OP, whereas five-hop cooperation has the lowest equally weighted OP–IP score. The results illustrate how the preferred route length depends on the risk measure, the weights assigned and the operating parameters. The paper discusses implications for cognitive network engineering and spectrum management.

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

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 before. Internet-of-things deployments, vehicle-to-everything communications and bandwidth-intensive applications put pressure on licensed spectrum. Cognitive radio enables unlicensed secondary users to share spectrum while protecting primary users [1–3]. Spectrum-sensing and dynamic-access research explores several ways of identifying and using available frequencies [4–6]. Among the spectrum-sharing modes, underlay permits secondary and primary users to transmit concurrently subject to an interference constraint at the primary receiver. Secondary transmit power is therefore limited, long links may require relaying, and the broadcast nature of wireless transmission still exposes the signal to unintended receivers.

The leakage problem is the security counterpart of reliability risk. Fading, path loss and cross-tier interference affect both legitimate reception and passive eavesdropping. Physical-layer security uses properties of the communication channel to study confidentiality [7–9], including in cognitive radio and fading channels [10, 11]; related work surveys techniques for multiuser wireless systems [12]. In the model considered here, intercept probability measures the chance that an eavesdropper decodes a transmission on at least one hop, consistent with the aggregation in Section 4.3. Longer routes may also expose a message to more outage events and consume more time-frequency resources. The research question is how to configure a multi-hop cognitive relay network so that reliability and confidentiality risks can be examined jointly.

The choice of fading model affects predictions of reliability and security. The α–μ family generalizes several common distributions, including Rayleigh, Weibull and Nakagami-m [13]; other analyses address generalized fading channels and diversity reception [14, 15]. A second design issue is power control. Spectrum-sharing studies have investigated the allocation of secondary transmit power under primary-user constraints [16, 17]. Here, the secondary power budget is calibrated using long-run channel statistics and a primary outage target, rather than relying on instantaneous cross-tier channel-state information. A third issue is how best to interpret multiple performance measures. This paper combines hop-level analysis with simulation-based risk surfaces to examine how system parameters affect the two risks.

ISSN: 3068-3661 | © 2025 INATGI (Institute of Advanced Technology and Green Innovation)

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.

The contributions of this paper are fivefold. First, it decomposes reliability and interception risks into hop-level events and aggregates them across independent hops. Second, it considers a secondary power-budget rule based on average channel gain and a primary outage target. Third, it uses the α–μ fading family, including Rayleigh, Weibull and Nakagami-m as special cases. Fourth, it uses Monte Carlo simulations to examine risk surfaces over transmit power, antenna count, target rate and hop count, including a Pareto-style comparison of OP and IP. Fifth, it discusses how the choice of hop count depends on the reliability measure, the confidentiality measure and their relative weights.

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 extends the reach of low-power transmitters in fading environments. Decode-and-forward (DF) and amplify-and-forward (AF) relaying have both been studied under Nakagami fading [18, 19]. In DF, a relay decodes a message before forwarding it; AF instead forwards an amplified received signal. The choice influences the accumulation of noise and the complexity of the relay. Relay-selection strategies and cooperative diversity provide further means of improving wireless transmission reliability [20, 21].

Cooperative-diversity research has considered the implementation and performance of user cooperation [22, 23], while related work examines end-to-end performance over fading links and joint routing and relay assignment [24, 25]. In incremental cooperation, a relay is invoked when the direct link is insufficient. Its usefulness depends on channel conditions, the route and the resources required for relaying. In a cognitive network, secondary relaying must also protect the licensed primary receiver from excessive interference.

2.2 Physical-Layer Security under Underlay Spectrum Sharing

Building on Wyner's wire-tap channel [7], physical-layer security has been studied in cognitive radio networks with passive eavesdroppers [10]. Liu et al. [26] examined relay selection for security enhancement, and subsequent studies considered the trade-off between security and reliability in cognitive radio systems [27–29]. Other research investigates secure transmission using multiple antennas and artificial noise [30, 31]. This paper evaluates outage and intercept probabilities together for its specified multi-hop model. It adopts independent codebooks across hops and reports the two risks at common operating points.

2.3 Generalized α–μ Fading and Its Operational Relevance

Yacoub introduced the α–μ distribution as a physical fading model [13], and Magableh and Matalgah studied its moment-generating function [32]. The parameters α and μ characterize propagation nonlinearity and multipath clustering. The family includes Rayleigh, Weibull and Nakagami-m cases, making it useful when different small-scale fading behaviours need to be studied within one model. Here the α–μ family provides the channel model for the security–reliability analysis of the specified multi-hop network.

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.

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, …,$S_{|M-1|}$. At every hop m∈{1, …, 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 $\Omega_{PQ} = l_{PQ}^{|-\eta|}$ with path-loss exponent η.

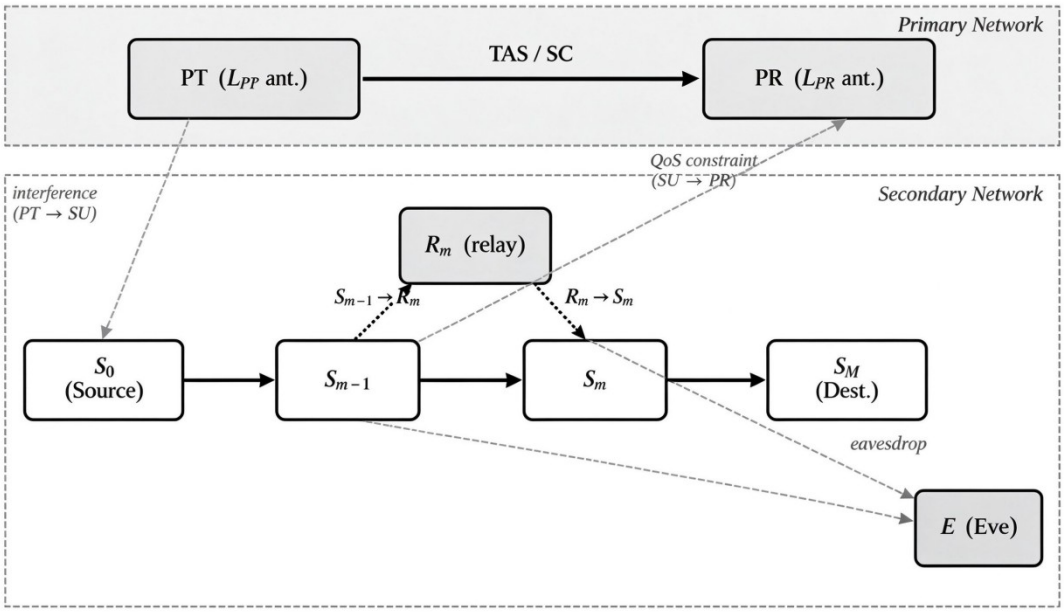


Figure 1. TAS/SC Multi-Hop Cognitive Relay Network with Incremental Cooperation

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.

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 $(X \in \{S_0, \ldots, S_{|M-1|}, R_1, \ldots, R_M\})$ 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.

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.

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.

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 $F_1(\gamma_S, \text{th})$ denote the cumulative distribution function [CDF] of the post-TAS/SC SINR on the direct link evaluated at the outage threshold

γ_S,th, $F_2(\psi_S,\text{th})$ the CDF on the $S_{|m-1|} - R_m$ link at the cooperative threshold ψ_S,th, and $F_3(\psi_S,\text{th})$ the CDF on the $R_m - S_m$ link, the per-hop outage probability is

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

where $\gamma_S, th = 2^{|M \cdot C_S|} - 1 \wedge \psi_S, th = 2^{|2M \cdot C_S|} - 1$ 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.

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 $F_4(\gamma_S,\text{th})$). Event B: the direct link fails and the relay listening sub-link also fails (probability $F_1(\gamma_S,\text{th}) \cdot F_2(\psi_S,\text{th})$) — 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 $F_4(\psi_S,\text{th})$), and on the forwarding sub-link either the relay-to-destination link fails (probability $F_3(\psi_S,\text{th})$) or it succeeds but the eavesdropper still fails to decode the forwarded copy (probability $F_5(\psi_S,\text{th})$). Combining,

$$IP_m^{|fail|} = \left(1 - F^1\right) \cdot F^4(\gamma_S, th) + F^1 \cdot F^2(\psi_S, th) + F^1 \cdot \left(1 - F^2\right) \cdot F^4(\psi_S, th) \cdot \left[F^3(\psi_S, th) + \left(1 - F^3\right) \cdot F^5(\psi_S, th)\right]$$
. *(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 $(F_{PQ}(\gamma)) \wedge L$ and the use of upper incomplete Gamma identities. The full derivation is omitted here for brevity but is straightforward.

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

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

Equations (1)–(3) give the hop-level decomposition used in Section 5. For fixed per-hop probabilities, adding independent hops cannot reduce either the end-to-end OP or the probability of interception on at least one hop. When the number of hops changes in the simulations, however, hop distances, thresholds and per-hop probabilities also change; the overall trends therefore depend on the operating configuration. For the DirecT baseline the cooperative branch is removed.

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 η = 3, the primary outage threshold is γ_P,th = 5, and the regulator-set primary outage target is ε_{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.

Table 1. α–μ Fading Parameters for Every Link

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.

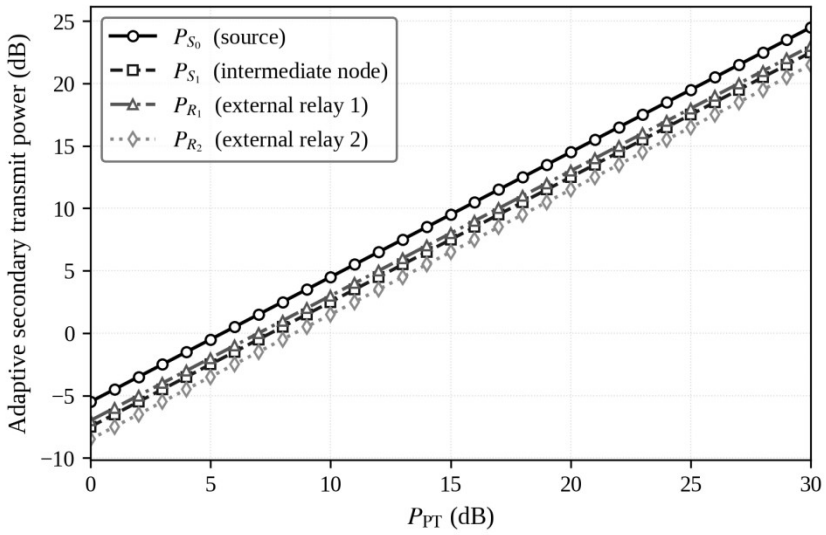


Figure 2. Adaptive Secondary Transmit Power versus Primary Transmit Power for M = 3 Hops

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 high P_{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].

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 ψ−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.

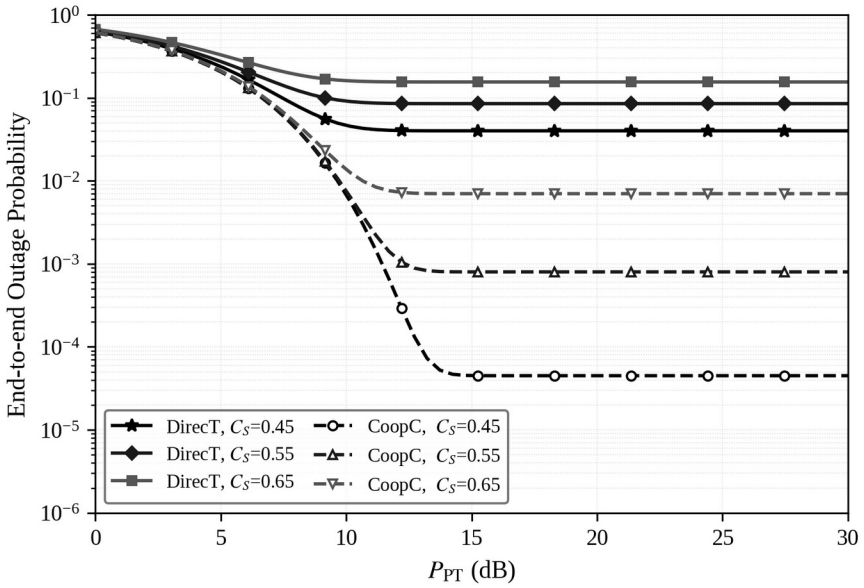


Figure 3. End-to-End Outage Probability of CoopC and DirecT versus Primary Transmit Power

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

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

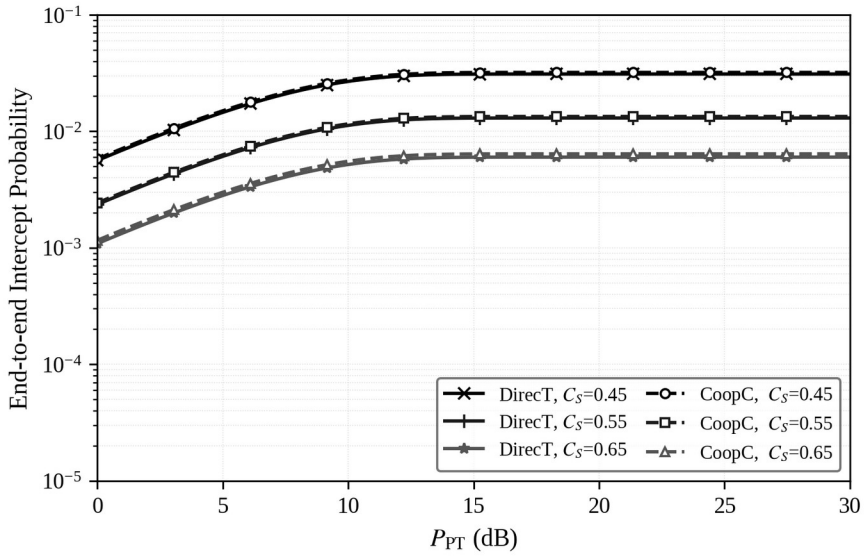


Figure 4. End-to-End Intercept Probability of CoopC and DirecT versus Primary Transmit Power

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.

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. Spatial diversity and antenna selection are well-established MIMO techniques [33–35]. The eavesdropper is also assumed to have the same L, so increasing L improves its reception as well. The legitimate transmitter selects its antenna, whereas the passive eavesdropper only applies receive-side selection combining.

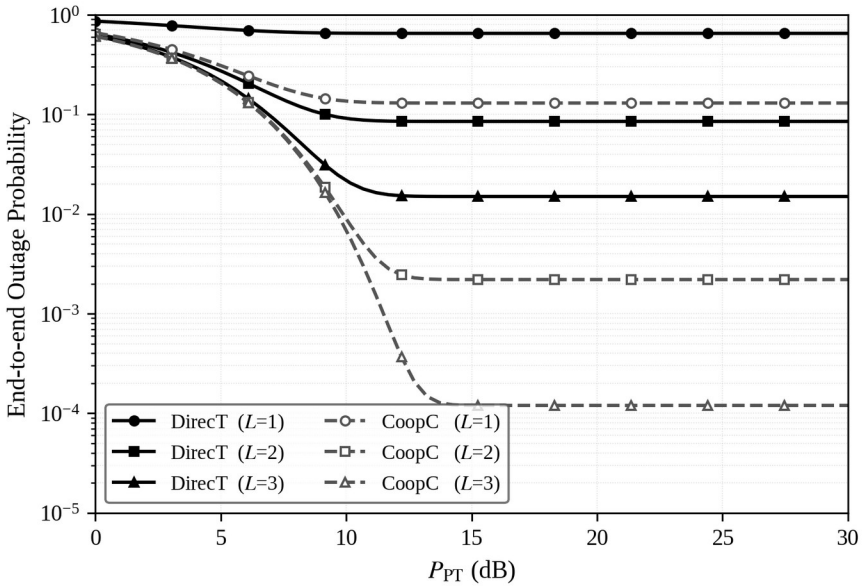


Figure 5. End-to-End Outage Probability versus Primary Transmit Power for Antenna Count L ∈{1, 2, 3}

Figure 5 indicates that increasing the antenna count reduces the plotted OP floor for both protocols, with a smaller additional gain from L = 2 to L = 3. The choice of antenna count should consider this reliability improvement alongside the cost and complexity of additional antennas. In this model the eavesdropper is also assumed to have the same antenna count, so the effect on interception risk must be considered as well.

5.6 Hop-Count Trade-Off Analytics

Figure 6 condenses the dual-objective analysis into a parametric Pareto-style view. We fix $P_{PT} = 20\ dB$, $C_S = 0.65 \wedge L = 2$, and we sweep the hop count M from 2 to 5. Every [M, protocol] combination is rendered as a point in the OP–IP plane, with M shown on the marker. For the displayed DirecT points, both reported risks decrease as M increases from 2 to 5. For CoopC, OP falls from M = 2 to M = 4 and rises at M = 5, whereas IP continues to fall. Thus M = 4 gives the lowest OP among the evaluated CoopC configurations; the preferred configuration for a joint score also depends on the weight assigned to each risk.

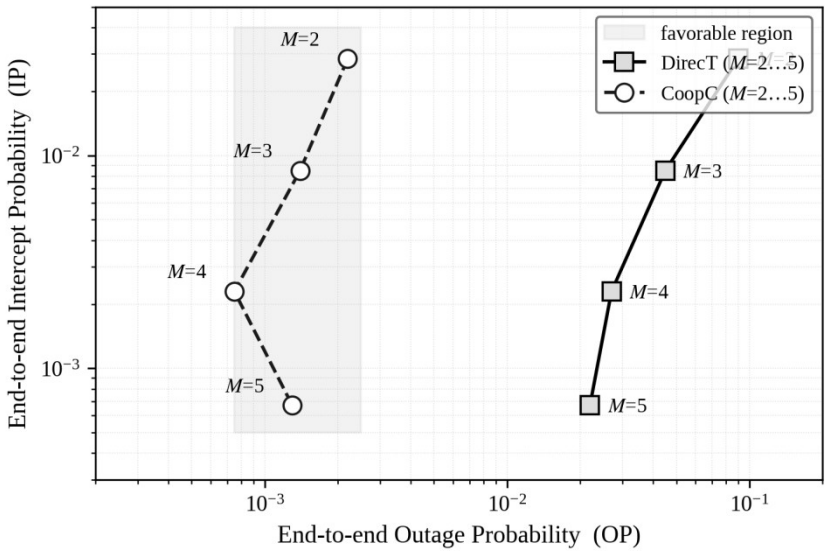


Figure 6. Pareto View of the OP–IP Trade-Off for Hop Count M ∈{2, 3, 4, 5}

Table 3 reports the underlying numbers and adds a derived column — a simple weighted sum $w_{OP} \cdot OP + w_{IP} \cdot IP$ *for* $w_{OP} = w_{IP} = 0.5$— that ranks the [M, protocol] configurations. The top three configurations are all CoopC: M = 5 ranks first, M = 4 second and M = 3 third. The first DirecT configuration (M = 5) ranks fourth. Thus, among these evaluated configurations, choose M = 5 for the lowest equal-weight score or M = 4 for the lowest OP. Different risk weights can lead to a different choice.

Table 3. Numerical OP/IP Values with Joint-Risk Scores

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 rate C_S; the largest joint-improvement lever is hop count M, which affects both metrics. Antenna count L also affects reliability and confidentiality and has a hardware cost. Under the values in Table 3, a route with M = 4 minimizes OP, while M = 5 minimizes the equally weighted OP–IP score; selection should reflect the application's priorities.

Table 4. Sensitivity of OP and IP to Design Levers

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 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 third thread concerns hop count. In the evaluated CoopC configurations, M = 4 has the lowest outage probability, while M = 5 has the lowest equally weighted OP–IP score in Table 3. These are results for the stated parameters and tested hop counts, not a universal optimum. Route planning should use weights appropriate to the application's reliability and confidentiality requirements.

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.

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.

Three operational findings emerge. First, the reported simulations show that incremental cooperation can substantially reduce outage probability with a relatively small interception-probability change at the examined points. Second, the proposed power-budget rule uses long-run channel averages and a primary outage target. Third, among the hop counts in Table 3, M = 4 minimizes OP and M = 5 minimizes the equally weighted OP–IP score. The preferred route depends on the chosen risk weights and operating conditions. Future work can examine active and colluding eavesdroppers, composite fading and secrecy throughput under rate adaptation.

Acknowledgement

The authors thank the anonymous reviewers for their constructive comments and suggestions.

Author Contributions

Conceptualization, H.M.S. and B.Y.Z.; Methodology, H.M.S. and B.Y.Z.; Formal Analysis, H.M.S. and B.Y.Z.; Investigation, H.M.S. and D.Z.; Data Curation, H.M.S. and D.Z.; Software, H.M.S. and D.Z.; Validation, H.M.S. and B.Y.Z. and D.Z.; Resources, D.Z.; Visualization, H.M.S. and D.Z.; Writing – Original Draft, H.M.S.; Writing – Review & Editing, H.M.S. and B.Y.Z. and D.Z.; Supervision, B.Y.Z.; Project Administration, H.M.S. and B.Y.Z. We have read and approved the final manuscript and take responsibility for the work.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethical Approval and Consent

Not applicable. This study did not involve human participants, personal data, or animals.

Data Availability Statement

The numerical data and parameter values used in the Monte-Carlo experiments are reported in the tables within this article. Further data or code may be obtained from the corresponding author upon reasonable request.

Declaration of Generative AI Use

The authors did not use generative AI tools in the preparation of this manuscript.

References

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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.2008.4481338

[6] Zhao, Q., & Swami, A. (2007). A survey of dynamic spectrum access: Signal processing and networking perspectives. In 2007 IEEE International Conference on Acoustics, Speech and Signal Processing (Vol. 4, pp. IV-1349–IV-1352). https://doi.org/10.1109/ICASSP.2007.367328

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] Simon, M. K., & Alouini, M.-S. (1998). 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/10.1109/5.705532

[15] 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

[16] 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/T-WC.2009.070265

[17] 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.2009.2018258

[18] 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.2007.910317

[19] 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.2012.030912.110222

[20] 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.2010.03.070409

[21] 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

[22] 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.2003.819238

[23] 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

[24] 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

[25] 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.2012.120203

[26] Liu, Y., Wang, L., Duy, T. T., 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.2014.2365808

[27] 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

[28] 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.2019.2904258

[29] 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.2020.2979267

[30] 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.2010.2068852

[31] 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

[32] Magableh, A. M., & Matalgah, M. M. (2009). Moment generating function of the generalized α-μ distribution with applications. IEEE Communications Letters, 13(6), 411–413. https://doi.org/10.1109/LCOMM.2009.090339

[33] Sanayei, S., & Nosratinia, A. (2004). Antenna selection in MIMO systems. IEEE Communications Magazine, 42(10), 68–73. https://doi.org/10.1109/MCOM.2004.1341263

[34] 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.2004.1284943

[35] Heath, R. W., & Paulraj, A. (2001). Antenna selection for spatial multiplexing systems based on minimum error rate. In Proc. IEEE Int. Conf. Commun. (ICC) (pp. 2276–2280). https://doi.org/10.1109/ICC.2001.937061