This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3503278

Active Reconfigurable Repeater-Assisted NOMA Networks in Internet-of-Things: Reliability, Security, and Covertness

Anh-Tu Le, Thai-Hoc Vu, Ngo Hoang Tu, Tan N. Nguyen, Lam-Thanh Tu, and Miroslav Voznak

***Abstract*—In the present paper, we describe a novel active reconfigurable repeater-aided non-orthogonal multiple access networks within the context of the Internet of Things. The study focuses on a scenario, where a source simultaneously transmits public information to an untrusted user and a covert signal to a legitimate user in the surveillance of an external warden or eavesdropper. We develop comprehensive analytical and optimization frameworks to evaluate the reliability, security, and covertness of the proposed system's performance, measuring three respective key metrics: outage probability (OP), secrecy OP (SOP), and detection error probability (DEP). First, we derive exact closed-form and asymptotic expressions for OP, SOP in internal and external eavesdropping scenarios, and DEP in external monitoring situations. Based on an asymptotic analysis of the OP, we propose two optimization methods for power allocation (PA) to achieve fairness in outage among users: a convex approximation method and an approximate closed-form solution. We then introduce an alternative method for optimizing PA to improve SOP in both eavesdropping scenarios while maintaining minimal OP requirements. In addition, we propose an effective approach for determining the warden's detection threshold to minimize the DEP, with low complexity and fast convergence, thereby improving communications covertness. Finally, we validate the theoretical and optimization frameworks through extensive Monte-Carlo simulations, exploring the impact of key system parameters on each performance metric.**

***Index Terms*—Active reconfigurable repeater, covert communication, detection error probability, intercept probability, non-orthogonal multiple access, performance analysis, physical-layer security, reliable communication, resource optimization.**

I. Introduction

A. Context and Motivation

The Internet-of-Things (IoT) has emerged as a transformative domain that connects billions of devices across various sectors, from smart homes and cities to industrial automation and healthcare [1]. The proliferation of IoT devices promises unprecedented levels of efficiency, automation, and data-driven decision-making. However, the rapid growth of IoT networks also introduces significant challenges, particularly concerning security [2], covert communications [3], and reliability [4]. Typically, IoT nodes are constrained by limited computational power, storage capacity, and energy resources, making IoT systems vulnerable to a range of security threats, such as eavesdropping, data interception, and unauthorized access. While traditional cryptographic methods remain essential for securing IoT systems, they often fail to address the full spectrum of security concerns [2], [5]. Even if encryption is employed, metadata (e.g., network traffic patterns) can still reveal sensitive information [6], leading to potential privacy breaches. For example, in high-security applications such as military or defense scenarios, communications must remain not only secure but also covert and thus, ensure that the existence of communication itself is undetectable by adversaries. Conventional encryption methods are insufficient in achieving this level of protection, necessitating more advanced techniques. Beyond the challenges of security and covert communications, establishing reliable communications in IoT networks is equally important [4]. Given the limited capabilities of individual IoT nodes, maintaining stable connectivity and consistent communication quality in dynamic or hostile environments can be challenging. Additional factors such as signal attenuation, interference, and network congestion can further compromise performance, resulting in unreliable communications and degraded quality-of-service.

To address these challenges, non-orthogonal multiple access (NOMA) technology offers certain advantages as a key enabler for the next generation of IoT networks [7], [8]. Unlike traditional orthogonal multiple access (OMA) techniques, which allocate distinct resources to each user, NOMA allows multiple users to share the same time slots, frequency bands, and spreading codes. This approach significantly improves spectral efficiency and enables the network to support massively connected devices, which is crucial in IoT scenarios characterized by diverse traffic demands and various power requirements. NOMA achieves its performance through power domain multiplexing, wherein users with different power levels are superimposed, and successive-interference cancellation (SIC) is applied at the receiver to separate the signals [9]–[12]. This technology improves network capacity and reliability by ensuring that users, even those with weaker signals, can be effectively served. Beyond its efficiency benefits, NOMA also offers inherent security and covert communication advantages. By dynamically allocating power and optimizing the coding and decoding processes, NOMA can further assist in mitigating the risks related to eavesdropping and unauthorized access [13], [14]. For example, in scenarios where a transmitter must communicate with a receiver without detection by a warden,

Anh-Tu Le and Miroslav Voznak are with the Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. Listopadu 2172/15, 708 00, Ostrava, Czechia (e-mail: tu.le.anh.st@vsb.cz, miroslav.voznak@vsb.cz). Thai-Hoc Vu is with the Department of Electrical, Electronic, and Computer Engineering, University of Ulsan, Ulsan 44610, Korea (e-mail: vuthaihoc1995@gmail.com). Ngo Hoang Tu is with the Department of Electrical and Information Engineering, Seoul National University of Science and Technology, Seoul 01811, South Korea, and the Department of Computer Engineering, Ho Chi Minh City University of Transport, Ho Chi Minh City 710372, Vietnam (e-mail: tu.ngo@ut.edu.vn). Lam-Thanh Tu (*corresponding author*) and Tan N. Nguyen are with the Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam (e-mail: tulamthanh@tdtu.edu.vn and nguyennhattan@tdtu.edu.vn).

This research is funded by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries ID No. CZ.10.03.01/00/22_003/0000048 of the European Just Transition Fund and by the Ministry of Education, Youth and Sports of the Czech Republic (MEYS CZ) through the project SGS ID No. SP 061/2024 conducted by VSB - Technical University of Ostrava.

NOMA can exploit noise and interference to mask the communication, thereby effectively enhancing covert transmission.

Although NOMA demonstrates significant advantages in IoT networks, additional strategies are necessary to further enhance coverage and reliability, particularly in environments with challenging conditions such as poor signal propagation or sparse scattering [15], [16]. A promising approach involves improving network performance without creating extra cells, but instead adding network components within existing cells. This has led to the exploration of solutions such as additional active relays [17]–[19], reconfigurable intelligent surfaces (RISs) [20]–[22], and active reconfigurable repeaters (ARRs) [23], [24]. Among these solutions, ARRs, also regarded as smart repeaters, have emerged as comparable effective candidates [25]. Compared to active relays and RISs, ARRs provide a simpler solution for amplifying incoming signals, without requiring complex signal processing at the physical layer [23], [26]. A detailed comparison of ARRs, RISs, and additional active relays in terms of form factor, power consumption, instantaneous channel state information (CSI) requirements, training, phase synchronization, backhaul consumption, active radiated power, noise sources, array gain, control overhead, deployment cost, flexibility, and band selectivity is presented in [25]. Unlike traditional repeaters, which primarily extend coverage in areas with weak signals [27], ARRs are designed to complement and enhance the wireless channel by introducing additional scattering and power gain. ARRs operate using a simple amplify-and-forward (AF) mechanism,[1] requiring minimal processing and providing a cost-effective and easily deployed solution. The inherent characteristics of ARRs provide an ideal complement to NOMA in IoT networks. By strategically deploying ARRs in areas with poor coverage or few scatterers, network operators can improve both coverage and signal quality and ensure that even resource-constrained IoT nodes maintain reliable communications.

While ARR technology primarily enhances network coverage and reliability, ensuring secure and covert communications in IoT networks lies with NOMA's advanced power allocation (PA) and interference management techniques. The combination of ARR and NOMA technologies thus presents a promising solution in addressing the challenges of reliable, secure, and covert communications in IoT networks while opening critical new avenues for research and innovation.

B. Literature Overview

NOMA in enhancing reliability: NOMA's superior capabilities in enhancing reliability for IoT networks have attracted considerable attention from the wireless research community. For instance, Park *et al.* [29] introduced a novel approach for allocating the target received power in uplink NOMA-based IoT systems, analyzing the tradeoff between reliability and sum-rate, and overall performance. Inspired by this, Sreya *et al.* [30] extended this system model to cellular IoT networks by proposing an adaptive rate NOMA scheme to meet capacity and delay conditions for IoT devices. Vu and Kim [31] examined the performance of wireless power transfer-assisted NOMA IoT systems, with evaluations of outage probability (OP), effective throughput (ETP), and energy efficiency (EE). Further extending this work to cognitive radio environments, Vu *et al.* [32] developed a solid mathematical analysis of these metrics. Their research also proposed optimization strategies for PA and energy harvesting time-switching factor configurations to minimize the OP and maximize the ETP.

NOMA in enhancing secure and covert communication: Several studies have explored the potential of NOMA in IoT systems across various aspects [13], [14], [33]–[39]. Lei *et al.* [33] analyzed the secrecy outage probability (SOP) of aerial eavesdropping in terrestrial-integrated aerial IoT NOMA systems. Xiang *et al.* [34] developed a secure transmission framework for NOMA-assisted IoT networks to deal with diverse short-packet communications (SPC) requirements, followed by a novel PA strategy to avoid the connection outage performance floor and a series of metric evaluations of connection outage probability (COP), SOP, effective secrecy throughput (EST), and trade-offs in security-reliability and security-efficiency. Xiang *et al.* [35] subsequently exploited the inherent characteristics of NOMA in securing SPC in IoT networks, deriving the expressions for effective secrecy rate (ESR) and sum-rate. Developing this work, Vu *et al.* [14] proposed a modified PA-integrated beamforming scheme to improve ESR and EST in SPC NOMA IoT networks embedded with untrusted near users. Examining security concepts, Jiang *et al.* [36] proposed a covert NOMA transmission scheme for cooperative device-to-device communication systems. The authors derived the minimum detection error probability (DEP) as a measure of covertness and introduced a solution for maximizing covert throughput (CTP). Tao *et al.* [37] further analyzed the COP, effective covert rate (ECR), and DEP for covert NOMA IoT systems, designing a PA strategy to maximize the ECR while obeying the constraints of the DEP and COP. In a related study, Zhang *et al.* [13] studied optimizing CTP under DEP and OP constraints in light of the network's uncertain CSI. Duan *et al.* [38] extended this network model by discussing different performance metrics and optimization formulations, focusing on maximizing the ECR through PA and detection threshold coefficient optimization. Li *et al.* [39] proposed a random artificial noise-based beamforming scheme for NOMA IoT systems, reducing the eavesdropping rate of the strong user while confusing the warden's monitoring.

Repeater investigation: Several studies have explored the performance of passive repeaters across various applications [26], [27], [40]–[42]. For example, Walkenhorst *et al.* [40] developed a full-duplex passive repeater to enhance the network capacity in environments with a dominant line-of-sight component. The authors' experimental results demonstrated that deploying a single additional repeater could elevate the channel to full rank, nearly doubling the link capacity. Similarly, Tsai and Shiu [26] showed that leveraging passive repeaters could improve coverage and capacity scaling to cellular systems. In another study, Ma *et al.* [41] proposed to improve channel

[1] Notably, the AF strategies of active relay nodes and ARRs differ. For AF-based active relay nodes, the signal is amplified along with the interference and noise [28], thereby increasing the vulnerability of the received signal. In contrast, AF-based ARRs instantaneously retransmit the incoming signal at the same frequency, ensuring that the forwarded signal remains within the cyclic prefix length to prevent unwanted interference [23], [26]. This allows ARRs to operate as additional channel scatterers with a power gain.

quality and reduce fronthaul costs by using a passive repeater-enhanced massive multiple-input multiple-output (MIMO) system. Besides, the authors also addressed potential drawbacks such as increased delay spread and compromised channel reciprocity by adopting distinct beamforming methods. Tang *et al.* [27] conducted experiments using a dual-antenna passive repeater with data-driven approaches to enhance received power gain, enable wide-angle scattering, and bring signal coverage to blind areas. Ahn *et al.* [42] demonstrated that a preamble cancellation strategy could benefit passive repeater-assisted broadcast networks containing multiple transmitters.

The interplay between AAR and NOMA and their promising: Despite the promising advantages of integrating repeater and NOMA technologies, as discussed in Section I-A, limited research has explored the use of repeater technology in NOMA-based IoT systems, with the exception of a single study by Ahuja *et al.* [43], which focused on bit error rate and SOP performance. The research field of ARRs remains relatively nascent, with only two notable studies [23], [24] on the topic, neither of which focuses on NOMA-based IoT networks. Specifically, Iimori *et al.* [23] proposed an amplification and phase optimization method to maximize the received signal-to-interference-plus-noise ratio (SINR) in distributed ARR-assisted communications systems. Leone *et al.* [24] examined network planning optimization for reliable millimeter-wave next-generation networks equipped with RISs and ARRs. Although such a joint implementation of RISs and ARRs can reconcile the strengths of each technology, achieving an optimal efficiency balance remains a topic that requires further investigation and careful analysis.

C. Novelty and Contributions

As discussed in Sections I-A and I-B, given the emerging nature of ARR technology and its significant potential to enhance NOMA-based IoT systems, it is evident that this area has received insufficient attention, particularly in the context of secure and covert communications. Therefore, it is both timely and essential to intensify research efforts on integrating ARR with NOMA for IoT networks. In response to this critical gap in the literature, the present study introduces a comprehensive analysis of the reliability, security, and covertness for ARR-assisted NOMA IoT systems. In addition to developing mathematical evaluation frameworks, we also formulate and solve optimization problems for each aspect, proposing efficient solutions to enhance overall system performance. The main contributions of the study are summarized as follows:

1) For the first time, we introduce and investigate a novel proposed ARR-assisted NOMA IoT system that exploits both public and covert signals for communications in the presence of either (*i*) an internal or external eavesdropper or (*ii*) an external warden. In this context, we analyze the key performance indicators of reliability, security, and covertness, to evaluate the system's overall performance.
2) From a reliability perspective, we derive exact and approximate closed-form expressions for the OP. To ensure OP fairness between users, robust PA configurations are designed to minimize the maximum OP between legitimate and untrusted users, while adhering to the principal PA constraints. We propose two efficient optimization methods: a convex approximation strategy and a closed-form approximation solution.
3) From a security perspective, we derive exact and approximate closed-form expressions for the SOP in both internal and external eavesdropping scenarios. PA optimization problems are formulated to minimize the SOP of the legitimate user while considering practical constraints, such as the PA criterion and the untrusted user's OP. We address the challenges posed by complex SOP expressions in these problems by using the approximate SOP formulation, which permits the conversion of these complex problems into simplified convex approximations that can be efficiently solved using the modified Newton–Raphson iterative root-finding algorithm.
4) From a covertness perspective, we derive a comprehensive mathematical framework for external monitoring scenarios, providing both exact and asymptotic closed-form expressions for the DEP. This analysis yields valuable insights into the effects of the transmit signal-to-noise ratio (SNR), PA policies, detection thresholds, and communication distance on DEP performance. Subsequently, we propose an alternative low-complexity approach with fast convergence to determine the optimal power detection threshold, effectively minimizing DEP.
5) All analytical results are validated with Monte-Carlo simulations to demonstrate the advantages of the proposed framework. The numerical findings reveal several key insights: (*i*) increasing the transmit SNR improves communications reliability but also increases vulnerability to internal eavesdropping; (*ii*) a low transmit SNR is effective in achieving low SOP in internal eavesdropping scenarios, while a high SNR is preferable in external eavesdropping scenarios; (*iii*) minimizing the SOP enhances both physical-layer security and communications reliability; (*iv*) the proposed detection threshold algorithm ensures that the optimal DEP is obtained.

D. Organization and Notations

The remainder of the paper is organized as follows. Section II describes the system model. Section III presents the reliability evaluation framework, including an analysis of the OP and its fairness optimization. Section IV provides the security evaluation framework, detailing SOP analysis and its minimization problems in internal and external eavesdropping scenarios. Section V focuses on the covertness evaluation framework, covering DEP analysis and its minimization problem. Section VI examines the numerical results and key findings to validate and highlight the advantages of the proposed framework. Finally, Section VII concludes the paper. The section organization of the paper is outlined in Fig. 1.

Mathematical Notations: $\Pr[\cdot]$ and $|\cdot|$ denote the probability operator and the magnitude of a scalar, respectively. $F_X(\cdot)$ and $f_X(\cdot)$ denotes the cumulative distribution function (CDF) and the probability density function (PDF) of a random variable X, respectively. $\mathcal{K}_1(\cdot)$ is the first-order modified Bessel function of the second kind [44, Eq. (8.432)]. $[a]^+ = \max\{a, 0\}$ denotes the positive part function. $\mathbb{E}\{\cdot\}$ represents the ex-

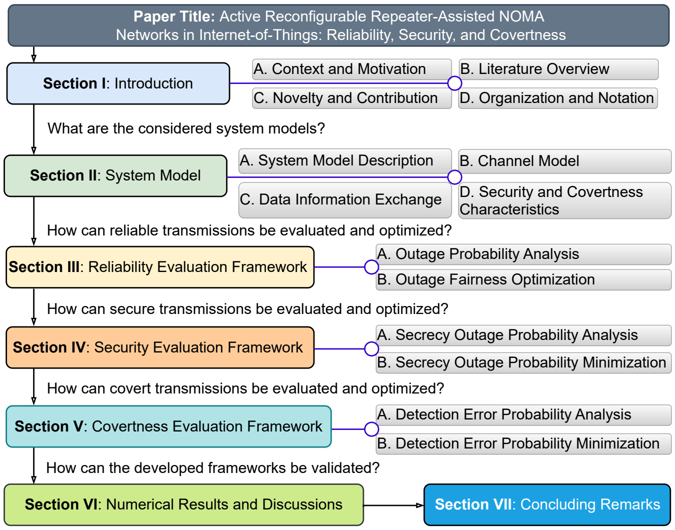

Paper Title: Active Reconfigurable Repeater-Assisted NOMA Networks in Internet-of-Things: Reliability, Security, and Covertness
Section I: Introduction
A. Context and Motivation
B. Literature Overview
C. Novelty and Contribution
D. Organization and Notation
What are the considered system models?
Section II: System Model
A. System Model Description
B. Channel Model
C. Data Information Exchange
D. Security and Covertness Characteristics
How can reliable transmissions be evaluated and optimized?
Section III: Reliability Evaluation Framework
A. Outage Probability Analysis
B. Outage Fairness Optimization
How can secure transmissions be evaluated and optimized?
Section IV: Security Evaluation Framework
A. Secrecy Outage Probability Analysis
B. Secrecy Outage Probability Minimization
How can covert transmissions be evaluated and optimized?
Section V: Covertness Evaluation Framework
A. Detection Error Probability Analysis
B. Detection Error Probability Minimization
How can the developed frameworks be validated?
Section VI: Numerical Results and Discussions
Section VII: Concluding Remarks

Fig. 1. Structure of the paper.

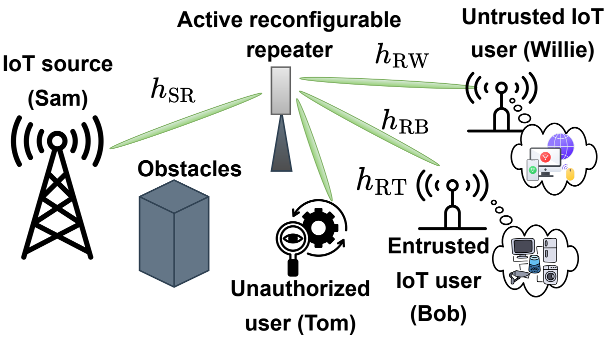


Fig. 2. Illustration of the considered system.

pectation operator. For a multi-variable function f, $\partial f/\partial x$ and $\partial^2 f/\partial x^2$ denote the first-order and second-order partial derivatives of f with respect to the variable x, respectively, whereas $\partial^2 f/\partial x\partial y$ denotes the second-order mixed derivative with respect to the variables x and y. For a single-variable function $g(x)$, $g'(x)$ and $g''(x)$ represent the first-order and second-order derivatives of $g(x)$, respectively. Furthermore, $\{a \wedge b\}$ expresses the mathematical conjunction between conditioned sets a and b. Finally, $\ln(\cdot)$ and $\exp(\cdot)$ present the natural logarithm and exponential functions, respectively.

II. System Model

A. System Model Description

As illustrated in Fig. 2, we consider a downlink ARR-based NOMA system. In this system, an IoT source, referred to as Sam (S), transmits a public signal x_{W} to an untrusted IoT user, Willie (W), while simultaneously transmitting a covert signal x_{B} to a trusted IoT user, Bob (B). This transmission occurs with the assistance of an ARR, denoted R, using NOMA signaling, expressed as $x = \sqrt{\alpha_{\mathsf{W}} P} x_{\mathsf{W}} + \sqrt{\alpha_{\mathsf{B}} P} x_{\mathsf{B}}$, where P is the transmit power of S while α_{W} and α_{B} are the PA levels for Willie' signal x_{W} and Bob' signal x_{B}, respectively, with $\mathbb{E}\{|x_{\mathsf{W}}|^2\} = 1$ and $\mathbb{E}\{|x_{\mathsf{B}}|^2\} = 1$. Suppose that the direct links from Sam to both Willie and Bob are significantly attenuated and can be ignored due to the effects of severe shadowing and obstacles. To prevent Willie from intercepting Bob's signal, the PA rule is set as $\alpha_{\mathsf{W}} > \alpha_{\mathsf{B}}$ and $\alpha_{\mathsf{W}} + \alpha_{\mathsf{B}} = 1$ [14]. In this setup, Willie decodes x_{W} directly, while Bob performs SIC to recover x_{B}. Meanwhile, an unauthorized user, Tom (T), also receives the signal from Sam, due to the inherent broadcasting nature of wireless communications. This study focuses on the scenario where Willie, after decoding x_{W}, attempts to intercept x_{B}. Additionally, Tom is considered for two possible roles: either as a warden (trying to detect whether Sam is sending x_{B} to Bob) or as an eavesdropper (eavesdropping on x_{B}).

B. Channel Model Description

Let h_{XY} be the channel coefficient between nodes X and Y. Under quasi-static Rayleigh block fading channels, $|h_{\mathsf{XY}}|^2$ follows the exponential distribution with respect to scale parameter $1/\lambda_{\mathsf{XY}}$, where $\lambda_{\mathsf{XY}} = (d_{\mathsf{XY}}/d_0)^{\eta}$, d_{XY} is the average distance between X and Y, η is the path-loss exponent, and d_0 is the reference distance. Therefore, the CDF and PDF of $|h_{\mathsf{XY}}|^2$ are given, respectively, by [31]

$$F_{|h_{\mathsf{XY}}|^2}(x) = 1 - \exp(-\lambda_{\mathsf{XY}} x), \tag{1}$$

$$f_{|h_{\mathsf{XY}}|^2}(x) = \lambda_{\mathsf{XY}} \exp(-\lambda_{\mathsf{XY}} x). \tag{2}$$

Furthermore, it is assumed that Sam is able to obtain the CSI for both Bob and Willie through uplink channel estimation, but due to the lack of pilot signal feedback, only has access to Tom's statistical CSI [36]–[39].

C. Data Information Exchange

At the n-th time-slot, the signal received at the receiving node $\mathsf{D} \in \{\mathsf{W}, \mathsf{B}, \mathsf{T}\}$ can be expressed as

$$y_{\mathsf{D}}[n] = \sqrt{\varpi} h_{\mathsf{SR}} h_{\mathsf{RD}} x[n] + w_{\mathsf{D}}[n], \tag{3}$$

where $w_{\mathsf{D}}[n]$ is the additive white Gaussian noise (AWGN) signal with zero mean and variance σ^2, and ϖ is the weight (i.e., phase rotation and power gain [23]) applied at R.

Based on (3), the SINR at Willie or Bob for decoding x_{W} and the SNR at Bob for decoding x_{B} after performing SIC are given, respectively, as

$$\Psi_{\mathsf{U}} = \frac{\varpi \alpha_{\mathsf{W}} \bar{\gamma} |h_{\mathsf{SR}}|^2 |h_{\mathsf{RU}}|^2}{\varpi \alpha_{\mathsf{B}} \bar{\gamma} |h_{\mathsf{SR}}|^2 |h_{\mathsf{RU}}|^2 + 1}, \psi_{\mathsf{B}} = \varpi \alpha_{\mathsf{B}} \bar{\gamma} |h_{\mathsf{SR}}|^2 |h_{\mathsf{RB}}|^2, \tag{4}$$

where $\mathsf{U} \in \{\mathsf{W}, \mathsf{B}\}$ and $\bar{\gamma} = P/\sigma^2$ is the transmit SNR.

D. Security and Covertness Characteristics

1) Eavesdropping on Propagation Information: To evaluate the physical layer security, we examine the scenario where Willie (acting as an internal eavesdropper), after decoding his message, attempts to intercept information transmitted by Sam to Bob. Specifically, the SNR for decoding x_{B} after performing SIC at Willie can be written as

$$\psi_{\mathsf{W}} = \varpi \alpha_{\mathsf{B}} \bar{\gamma} |h_{\mathsf{SR}}|^2 |h_{\mathsf{RW}}|^2. \tag{5}$$

Likewise, we study the case where Tom, acting as an external eavesdropper, separately decodes both x_{B} and x_{W} from his received signal y_{T} using parallel decoding for the worst-case scenario. The SNR for Tom to decode x_{B} is given by

$$\psi_{\mathsf{T}} = \varpi \alpha_{\mathsf{B}} \bar{\gamma} |h_{\mathsf{SR}}|^2 |h_{\mathsf{RT}}|^2. \tag{6}$$

2) Monitoring on Covert Signal: In a different scenario, Tom acts as an external warden and attempts to detect a covert signal transmitted by Sam to Bob using a binary hypothesis test. Specifically, Tom distinguishes between two hypotheses based on his received signal:

$$y_{\mathsf{T}}[n] = \begin{cases} h_{\mathsf{SR}} h_{\mathsf{RT}} \sqrt{\varpi} x[n] + w_{\mathsf{T}}[n], & \mathcal{H}_1, \\ h_{\mathsf{SR}} h_{\mathsf{RT}} \sqrt{\varpi \alpha_{\mathsf{W}} P} x_{\mathsf{W}}[n] + w_{\mathsf{T}}[n], & \mathcal{H}_0, \end{cases} \tag{7}$$

where $\mathcal{H}_1$ and $\mathcal{H}_0$ imply the true and false hypotheses, respectively, of detecting Bob's covert signal. Using a radiometer, Tom's detection strategy, modelled by the Neyman-Pearson method, is expressed as [36]–[39]

$$\Phi_{\mathsf{T}} = \frac{1}{M} \sum_{m=1}^{M} |y_{\mathsf{T}}^m[n]|^2 \underset{\mathrm{D}_0}{\overset{\mathrm{D}_1}{\gtrless}} \omega, \tag{8}$$

where M is the total channel use quantity, ω is the detection threshold, while D_1 and D_0 represent the decisions favoring $\mathcal{H}_1$ and $\mathcal{H}_0$, respectively. Following the reasoning in [36]–[39], for a sufficiently large M, i.e., $M \to \infty$, the average power of the signal received by Tom can be expressed as

$$\Phi_{\mathsf{T}} = \begin{cases} \varpi(\alpha_{\mathsf{W}} + \alpha_{\mathsf{B}}) P |h_{\mathsf{SR}}|^2 |h_{\mathsf{RT}}|^2 + \sigma^2, & \mathcal{H}_1, \\ \varpi \alpha_{\mathsf{W}} P |h_{\mathsf{SR}}|^2 |h_{\mathsf{RT}}|^2 + \sigma^2, & \mathcal{H}_0. \end{cases} \tag{9}$$

Based on the mentioned above, the subsequent sections analyze the system's performance in terms of the OPs for Willie and Bob, the SOP for the internal and external eavesdropping scenarios, and the DEP for the covert signal transmission.

III. Reliability Evaluation Framework

A. Outage Probability Analysis

The OP is defined as the probability that the received SINR/SNR for decoding x_{U} at the receiving node falls below a predefined decoding threshold γ_{U}, with $\gamma_{\mathsf{U}} = 2^{r_{\mathsf{U}}} - 1$, where r_{U} is the target data rate [bps/Hz]. Accordingly, the OP for decoding x_{W} at Willie, while ensuring a successful SIC procedure at Bob, can be expressed as [31]

$$p_{\mathrm{op}}^{\mathsf{W}} = \Pr[\min\{\Psi_{\mathsf{W}}, \Psi_{\mathsf{B}}\} \le \gamma_{\mathsf{W}}]. \tag{10}$$

Meanwhile, the SNR for decoding x_{B} at Bob after canceling x_{W} from $y_{\mathsf{B}}[n]$ can be expressed as

$$p_{\mathrm{op}}^{\mathsf{B}} = \Pr[\psi_{\mathsf{B}} \le \gamma_{\mathsf{B}}]. \tag{11}$$

From (10) and (11), the OP of decoding x_{W} at Willie and x_{B} at Bob can be effectively evaluated by the following lemma.

Lemma 1: Conditioned on $\gamma_{\mathsf{W}} < \alpha_{\mathsf{W}}/\alpha_{\mathsf{B}}$ (otherwise, the system always experiences an outage event), the exact OP expressions for decoding x_{W} at Willie and x_{B} at Bob can be obtained in closed-form expressions, respectively, as

$$p_{\mathrm{op}}^{\mathsf{W}} = 1 - \sqrt{4\lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}}/\varpi\bar{\gamma}}\, \mathcal{K}_1\left(\sqrt{4\lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}}/\varpi\bar{\gamma}}\right), \tag{12}$$

$$p_{\mathrm{op}}^{\mathsf{B}} = 1 - \sqrt{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}}/\varpi\bar{\gamma}}\, \mathcal{K}_1\left(\sqrt{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}}/\varpi\bar{\gamma}}\right), \tag{13}$$

where $\tau_{\mathsf{W}} = \gamma_{\mathsf{W}}/(\alpha_{\mathsf{W}} - \alpha_{\mathsf{B}}\gamma_{\mathsf{W}})$, $\tau_{\mathsf{B}} = \gamma_{\mathsf{B}}/\alpha_{\mathsf{B}}$, and $\lambda_{\Sigma} = \lambda_{\mathsf{RW}} + \lambda_{\mathsf{RB}}$.

Proof: See Appendix A. ■

Lemma 1 indicates that when allotting α_{W} for x_{W} and α_{B} for x_{B} satisfies $\gamma_{\mathsf{W}} < \alpha_{\mathsf{W}}/\alpha_{\mathsf{B}}$, the OP of decoding x_{U} is indeed a function of fading parameters, the predefined decoding thresholds, and the transmit SNR. However, the complexity of the OP expressions for decoding x_{U} problematizes the determination of the effects of key system parameters on OP performance. To address this, we investigate the asymptotic OP behavior by applying the first-order series expansion for the Bessel function, as described in [44, Eq. (8.446.2)], to get

$$\mathcal{K}_1(x) \overset{x \to 0}{\simeq} \ln(x/2)\, x/2 + 1/x. \tag{14}$$

Thus, the respective OPs in (12) and (13) can be simplified as

$$p_{\mathrm{op}}^{\mathsf{W},\mathrm{ap}} = -\lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}} \ln(\lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}}/\varpi\bar{\gamma})/\varpi\bar{\gamma}, \tag{15}$$

$$p_{\mathrm{op}}^{\mathsf{B},\mathrm{ap}} = -\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}} \ln\left(\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}}/\varpi\bar{\gamma}\right)/\varpi\bar{\gamma}. \tag{16}$$

Thus, for any $x, y > 0$, we apply the following connection:

$$\ln(y/x)/x = \ln(y)/x - \ln(x)/x \overset{x \to \infty}{\simeq} -\ln(x)/x, \tag{17}$$

which enables us to simplify the OPs in (15) and (16) to

$$p_{\mathrm{op}}^{\mathsf{W},\mathrm{ap}} \approx \lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}} \ln(\varpi\bar{\gamma})/\varpi\bar{\gamma}, \tag{18}$$

$$p_{\mathrm{op}}^{\mathsf{B},\mathrm{ap}} \approx \lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}} \ln(\varpi\bar{\gamma})/\varpi\bar{\gamma}. \tag{19}$$

Then, applying L'Hospital's rule to $f(x) = \ln(x)/x$ yields the following asymptotic result:

$$\lim_{x \to \infty} f(x) = 1/x = 0. \tag{20}$$

Remark 1: From the results obtained in (18)–(20), several key insights can be drawn:

1) Increasing $\bar{\gamma}$ improves $p_{\mathrm{op}}^{\mathsf{W}}$ and $p_{\mathrm{op}}^{\mathsf{B}}$. Specifically, both OP expressions exhibit the same diversity order of one, as $p_{\mathrm{op}}^{\mathsf{W}}$ in (18) and $p_{\mathrm{op}}^{\mathsf{B}}$ in (19) are proportional to $1/\bar{\gamma}$.
2) Since λ_{SR} and λ_{RU} are proportional to d_{SR} and d_{RU}, respectively, increasing the distance of communication between Sam and the AAR, as well as between the AAR and Willie or Bob, leads to an increase in $p_{\mathrm{op}}^{\mathsf{U}}$.
3) Considering $\tau_{\mathsf{W}} = \gamma_{\mathsf{W}}/(\alpha_{\mathsf{W}} - \alpha_{\mathsf{B}}\gamma_{\mathsf{W}})$, we observe that $p_{\mathrm{op}}^{\mathsf{W}}$ improves as γ_{W} decreases or α_{W} increases. Similarly, when $\tau_{\mathsf{B}} = \gamma_{\mathsf{B}}/\alpha_{\mathsf{B}}$, $p_{\mathrm{op}}^{\mathsf{B}}$ improves with an increase in α_{B} or a decrease in γ_{B}. However, due to their interdependence, configuring α_{W} and α_{B} involves a performance trade-off: increasing α_{W} to improve $p_{\mathrm{op}}^{\mathsf{W}}$ decreases α_{B}, yielding an increase in $p_{\mathrm{op}}^{\mathsf{B}}$, and vice versa.

B. Outage Fairness Optimization

1) Problem Formulation: From Remark 1, we are interested in optimizing α_{W} and α_{B} to achieve OP fairness between users, motivated by the following key considerations. First, fairness ensures that both Willie and Bob experience similar levels of service quality, regardless of their respective locations or network conditions. Second, managing OPs fairly permits more efficient network resource allocation, thereby reducing the likelihood of Bob experiencing poor service while Willie benefits from excess capacity. Finally, optimizing fairness can improve the overall network performance by minimizing the probability of service interruptions and ensuring a more consistent user experience, especially in terms of reliability and latency requirements. In summary, the optimization problem can be mathematically formulated as follows:

$$\mathbf{P}_1: \min_{\alpha_{\mathsf{W}},\alpha_{\mathsf{B}}} \max\left\{p_{\text{op}}^{\mathsf{W}}, p_{\text{op}}^{\mathsf{B}}\right\} \tag{21a}$$

$$\text{s.t } \alpha_{\mathsf{W}} + \alpha_{\mathsf{B}} = 1, \alpha_{\mathsf{W}} > \alpha_{\mathsf{B}}\gamma_{\mathsf{W}}, \alpha_{\mathsf{W}} > 0, \alpha_{\mathsf{B}} > 0, \tag{21b}$$

where the objective functions in (21a) are given by (12) and (13), and the constraints in (21b) correspond to the initial condition and prevent operation in a zero-coverage scenario.

2) Solution Approaches: Problem (21) is non-convex due to the non-convexity of the objective functions in (21a). The OP expressions in (12) and (13) also contain the Bessel–K function, which is a special function and complex to handle analytically. To this end, we propose two approaches: 1) a convex approximation problem negotiated using interior-point methods or a CVX solver [10] and 2) closed-form approximations for the optimal values $\alpha_{\mathsf{W}}^{\star}$ and $\alpha_{\mathsf{B}}^{\star}$.

Convex Approximation: To deal with the non-convexity nature of (21), we introduce a slack variable $\theta \geq \max\{p_{\text{op}}^{\mathsf{W}}, p_{\text{op}}^{\mathsf{B}}\}$ and exploit the approximations $p_{\text{op}}^{\mathsf{W},\text{ap}} \simeq p_{\text{op}}^{\mathsf{W}}$ and $p_{\text{op}}^{\mathsf{B},\text{ap}} \simeq p_{\text{op}}^{\mathsf{B}}$. This enables us to reformulate (21) into a more manageable form as

$$\min_{\alpha_{\mathsf{W}},\alpha_{\mathsf{B}}} \theta \quad \text{s.t} \quad \theta \geq \max\left\{p_{\text{op}}^{\mathsf{W},\text{ap}}, p_{\text{op}}^{\mathsf{B},\text{ap}}\right\} \text{ and } (21\text{b}). \tag{22}$$

Since $x \geq \max(a, b)$ is equivalent to $\{x \geq a \wedge x \geq b\}$, the constraint $\theta \geq \max\{p_{\text{op}}^{\mathsf{W},\text{ap}}, p_{\text{op}}^{\mathsf{B},\text{ap}}\}$ in (22) can be rewritten as

$$\begin{cases} \theta \geq \lambda_{\mathsf{SR}}\lambda_{\Sigma}\gamma_{\mathsf{W}} \ln(\varpi\bar{\gamma})/[\varpi\bar{\gamma}(\alpha_{\mathsf{W}} - \alpha_{\mathsf{B}}\gamma_{\mathsf{W}})], & (23) \\ \theta \geq \lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} \ln(\varpi\bar{\gamma})/[\varpi\bar{\gamma}\alpha_{\mathsf{B}}]. & (24) \end{cases}$$

As a result, (22) can be reformulated as

$$\min_{\alpha_{\mathsf{W}},\alpha_{\mathsf{B}}} \theta \quad \text{s.t} \quad (21\text{b}), (23), \text{ and } (24). \tag{25}$$

To solve (25), we introduce the following lemma.

Lemma 2: Over the feasible domain $x > ay$ with $a > 0$, $f(x, y) = 1/(x - ay)$ is a convex function.

Proof: We first consider the Hessian matrix of $f(x, y)$ as

$$\mathbf{H}(x,y) = \begin{bmatrix} \partial^2 f(x,y)/\partial x^2 & \partial^2 f(x,y)/\partial x\partial y \\ \partial^2 f(x,y)/\partial y\partial x & \partial^2 f(x,y)/\partial y^2 \end{bmatrix}.$$

Since $\partial^2 f(x,y)/\partial x^2 = 2/(x-ay)^3$, $\partial^2 f(x,y)/\partial y^2 = 2a^2/(x-ay)^3$, and $\partial^2 f(x,y)/\partial x\partial y = \partial^2 f(x,y)/\partial y\partial x = -2a/(x-ay)^3$, $\mathbf{H}(x,y)$ is a symmetric matrix. Furthermore, for $x > ay$, its principal minors are non-negative, i.e., $\partial^2 f(x,y)/\partial x^2 > 0$ and

$$\frac{\partial^2 f(x,y)}{\partial x^2}\frac{\partial^2 f(x,y)}{\partial y^2} - \frac{\partial^2 f(x,y)}{\partial x\partial y}\frac{\partial^2 f(x,y)}{\partial y\partial x} = 0.$$

Since $\mathbf{H}(x,y)$ is positive semi-definite, $f(x,y) = 1/(x-ay)$ is a convex function, ending the proof. ■

Notably, the constraint $\alpha_{\mathsf{W}} + \alpha_{\mathsf{B}} = 1$ in (21b) is affine, which forms a convex set. Along with Lemma 2, we conclude that (25) is a convex optimization problem. To this end, CVX can be adopted to achieve the optimal solutions $\alpha_{\mathsf{B}}^{\star}$ and $\alpha_{\mathsf{W}}^{\star}$.

Closed-form Approximation: In the feasible domain where $\gamma_{\mathsf{W}} < \alpha_{\mathsf{W}}/\alpha_{\mathsf{B}}$, the OPs for decoding x_{W} at Willie and x_{B} at Bob are said to be fair if and only if $p_{\text{op}}^{\mathsf{W}} = p_{\text{op}}^{\mathsf{B}}$. Using the approximations $p_{\text{op}}^{\mathsf{W},\text{ap}} \simeq p_{\text{op}}^{\mathsf{W}}$ and $p_{\text{op}}^{\mathsf{B},\text{ap}} \simeq p_{\text{op}}^{\mathsf{B}}$, and substituting the results from (18) and (19) into the equality $p_{\text{op}}^{\mathsf{W},\text{ap}} = p_{\text{op}}^{\mathsf{B},\text{ap}}$, we derive the following equality

$$\begin{aligned} &\lambda_{\mathsf{SR}}\lambda_{\Sigma}\tau_{\mathsf{W}} \ln(\varpi\bar{\gamma})/[\varpi\bar{\gamma}] = \lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\tau_{\mathsf{B}} \ln\left(\varpi\bar{\gamma}\right)/\varpi\bar{\gamma} \\ &\Rightarrow \alpha_{\mathsf{B}}\left(\gamma_{\mathsf{W}} + \gamma_{\mathsf{W}}\lambda_{\Sigma}/[\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}}]\right) - \alpha_{\mathsf{W}} = 0. \end{aligned} \tag{26}$$

Combining the above equality and the PA rule $\alpha_{\mathsf{B}} + \alpha_{\mathsf{W}} = 1$, we analytically derive the closed-form approximation solutions for the min-max OP optimization problem as

$$\alpha_{\mathsf{B}}^{\star} = \lambda_{\mathsf{RB}}\gamma_{\mathsf{B}}/[\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} + \gamma_{\mathsf{W}}(\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} + \lambda_{\Sigma})], \tag{27}$$

$$\alpha_{\mathsf{W}}^{\star} = \gamma_{\mathsf{W}}(\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} + \lambda_{\Sigma})/[\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} + \gamma_{\mathsf{W}}(\lambda_{\mathsf{RB}}\gamma_{\mathsf{B}} + \lambda_{\Sigma})]. \tag{28}$$

Note that the above solutions eliminate the need for complex iterative calculations, significantly reducing the computational complexity compared to interior-point methods or convex solvers while yielding the same optimal solution.

IV. Security Evaluation Framework

A. Secrecy Outage Probability Analysis

The SOP is defined as the probability that the secrecy capacity, given by $C_s = [C_{\mathsf{B}} - C_{\mathsf{E}}]^{+}$, falls below a specified secrecy rate R_{B}, where $C_{\mathsf{B}} = \log_2(1 + \psi_{\mathsf{B}})$ is the legitimate link's channel capacity, while $C_{\mathsf{E}} = \log_2(1 + \psi_{\mathsf{E}})$, with $\mathsf{E} \in \{\mathsf{W}, \mathsf{T}\}$, is the eavesdropper link's channel capacity. Mathematically, the SOP is expressed as

$$p_{\text{sop}} = \Pr\left[C_s < R_{\mathsf{B}}\right] = \Pr\left[\frac{1 + \psi_{\mathsf{B}}}{1 + \psi_{\mathsf{E}}} < 2^{R_{\mathsf{B}}}\right]. \tag{29}$$

For convenience, we denote $\phi = 2^{R_{\mathsf{B}}}$ and $\rho = 2^{R_{\mathsf{B}}} - 1$.

1) Internal Eavesdropping Scenario: Using (5) and (29), the SOP that Willie intercepts x_{B} is expressed as

$$p_{\text{sop}}^{\text{int}} = \Pr\left[\Psi_{\mathsf{W}} \geq \gamma_{\mathsf{W}}, \psi_{\mathsf{B}} < \rho + \phi\psi_{\mathsf{W}}\right]. \tag{30}$$

Based on this relation, the SOP for internal eavesdropping can be evaluated precisely through the following lemma.

Lemma 3: Provided that $\gamma_{\mathsf{W}} < \alpha_{\mathsf{W}}/\alpha_{\mathsf{B}}$ (otherwise, the system always experiences a secrecy outage event), the SOP for the case where Willie eavesdrops on Bob' signal is given by

$$\begin{aligned} p_{\text{sop}}^{\text{int}} = &\sqrt{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RW}}\tau_{\mathsf{W}}/\varpi\bar{\gamma}}\,\mathcal{K}_1\left(\sqrt{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RW}}\tau_{\mathsf{W}}/\varpi\bar{\gamma}}\right) \\ &- \lambda_{\mathsf{RW}}\sqrt{4\zeta\lambda_{\mathsf{SR}}/\varpi\bar{\gamma}}\,\mathcal{K}_1\left(\sqrt{4\zeta\lambda_{\mathsf{SR}}/\varpi\bar{\gamma}}\right)/[\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}], \end{aligned} \tag{31}$$

where $\zeta = \tau_{\mathsf{W}}\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}\tau_{\mathsf{W}} + \lambda_{\mathsf{RB}}\rho/\alpha_{\mathsf{B}}$.

Proof: See Appendix B. ■

To gain a deeper insight into the impact of system parameters on $p_{\text{sop}}^{\text{int}}$, (31) can be simplified using (14) and (17) as

$$\begin{aligned} p_{\text{sop}}^{\text{int,ap}} &= \lambda_{\mathsf{SR}}\lambda_{\mathsf{RW}}\tau_{\mathsf{W}} \ln(\lambda_{\mathsf{SR}}\lambda_{\mathsf{RW}}\tau_{\mathsf{W}}/\varpi\bar{\gamma})/\varpi\bar{\gamma} + 1 \\ &\quad - \frac{\lambda_{\mathsf{RW}}}{\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}}\left(\zeta\lambda_{\mathsf{SR}} \ln(\zeta\lambda_{\mathsf{SR}}/\varpi\bar{\gamma})/\varpi\bar{\gamma} + 1\right) \quad (32) \\ &\approx \frac{\lambda_{\mathsf{RB}}\phi}{\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}} + \frac{\lambda_{\mathsf{RB}}\rho\lambda_{\mathsf{RW}}\lambda_{\mathsf{SR}} \ln(\varpi\bar{\gamma})}{(\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}\varpi\bar{\gamma}\alpha_{\mathsf{B}})}. \quad (33) \end{aligned}$$

Remark 2: The approximation $p_{\text{sop}}^{\text{int,ap}}$ in (33) indeed describes a decreasing and strictly concave function to α_{B}, as indicated by $\partial p_{\text{sop}}^{\text{int,ap}}/\partial \alpha_{\mathsf{B}} < 0$ and $\partial^2 p_{\text{sop}}^{\text{int,ap}}/\partial {\alpha_{\mathsf{B}}}^2 > 0$. Furthermore, based on the results in (33) and (20), it is implied that the SOP for Willie eavesdropping on x_{B} reaches a SOP floor at $\lambda_{\mathsf{RB}}\phi/(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}}) = 1-\lambda_{\mathsf{RW}}/(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}})$. Combining this observation with $\phi = 2^{R_{\mathsf{B}}}$, it is straightforward to show that decreasing R_{B} proportionally improves the SOP.

2) External Eavesdropping Scenario: Using (6) and (29), the SOP that Tom eavesdrops on x_{B} is expressed as

$$p_{\text{sop}}^{\text{ext}} = \Pr\left(\psi_{\mathsf{B}} < \rho + \phi\psi_{\mathsf{T}}\right). \tag{34}$$

Based on this relation, the SOP for external eavesdropping can be evaluated precisely through the following lemma.

Lemma 4: The SOP for the case where Tom eavesdrops on Bob's signal can be expressed as

$$p_{\text{sop}}^{\text{ext}} = 1-\frac{\lambda_{\mathsf{RT}}\sqrt{\frac{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho}{\alpha_{\mathsf{B}}\varpi\overline{\gamma}}}}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}})}\mathcal{K}_1\left(\sqrt{\frac{4\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho}{\alpha_{\mathsf{B}}\varpi\overline{\gamma}}}\right). \tag{35}$$

Proof: See Appendix C. ∎

Next, we shift the focus to obtain insights into the SOP of the external eavesdropping scenario at high SNR. By applying (14) and (20) to (35), we obtain the asymptotic SOP as

$$\begin{aligned} p_{\text{sop}}^{\text{ext,ap}} = 1 &- \frac{\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho/\alpha_{\mathsf{B}}\varpi\overline{\gamma}}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}})/\lambda_{\mathsf{RT}}}\ln\left(\frac{\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho}{\alpha_{\mathsf{B}}\varpi\overline{\gamma}}\right) && (36)\\ &- \lambda_{\mathsf{RT}}/(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}}) \\ \approx&\ \frac{\lambda_{\mathsf{RB}}\phi}{\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}}} + \frac{\lambda_{\mathsf{RT}}\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}})\alpha_{\mathsf{B}}\varpi\overline{\gamma}}\ln(\varpi\overline{\gamma}). && (37)\end{aligned}$$

Remark 3: The approximation $p_{\text{sop}}^{\text{ext,ap}}$ in (37) indeed describes a decreasing and strictly concave function with respect to α_{B} since $\partial p_{\text{sop}}^{\text{ext,ap}}/\partial\alpha_{\mathsf{B}} < 0$ and $\partial^2 p_{\text{sop}}^{\text{int,ap}}/\partial{\alpha_{\mathsf{B}}}^2 > 0$. Besides, applying (20) for (37) yields $p_{\text{sop}}^{\text{ext,ap}} \to \lambda_{\mathsf{RB}}\phi/(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}}) = 1-\lambda_{\mathsf{RT}}/(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}})$, which equals to the SOP floor for the internal eavesdropping scenario in Remark 2. This is to say, $p_{\text{sop}}^{\text{ext}}$ does not improve as $\overline{\gamma}$ increases. In this case, the SOP floor is primarily dominated by the fading parameters (λ_{RB} and λ_{RT}) and the required security rate R_{B}, while remaining independent of λ_{SR}.

B. Secrecy Outage Probability Minimization

1) Internal Eavesdropping Scenario: From a practical point of view, minimizing the SOP helps improve Bob's OP and precludes Willie from eavesdropping on Bob's secure information. Nevertheless, focusing solely on minimizing the SOP could impact Willie's reliable performance and lead to an outage. Hence, we aim to optimize the PA budget to minimize the SOP for internal eavesdropping while ensuring that Willie's minimum reliability requirement is met. Mathematically, this optimization problem can be formulated as

$$\begin{aligned} \mathbf{P}_2 : \min_{\alpha_{\mathsf{W}},\alpha_{\mathsf{B}}}\ & p_{\text{sop}}^{\text{int}} && (38a)\\ \text{s.t}\ & \alpha_{\mathsf{W}}+\alpha_{\mathsf{B}} = 1, \alpha_{\mathsf{W}} > 0, \alpha_{\mathsf{B}} > 0, \alpha_{\mathsf{W}} > \alpha_{\mathsf{B}}\gamma_{\mathsf{W}}, && (38b)\\ & p_{\text{op}}^{\mathsf{W}} \le \epsilon, && (38c)\end{aligned}$$

where $p_{\text{sop}}^{\text{int}}$ and $p_{\text{op}}^{\mathsf{W}}$ are given in (31) and (12), respectively, and (38c) ensures Willie's minimal reliability constraint, with ϵ being Willie's OP threshold.

Algorithm 1: Find $\alpha_{\mathsf{B}}^{\star}$ to minimize $g(\alpha_{\mathsf{B}})$.

```
Initialization: The threshold $\epsilon$, step search $\chi = 10^{-3}$,
                starting point $\alpha_0 \in [\varphi, 1/(1+\gamma_{\mathsf{W}})-\varphi]$,
                and $\alpha_{\mathsf{B}}^{\star} = \alpha_0$.
while $q(\alpha_l) \le \epsilon$ do
    Update: $\alpha_{l+1} \leftarrow \alpha_l - \chi g'(\alpha_l)/g''(\alpha_l)$;
    Update: $\alpha_{\mathsf{B}}^{\star} \leftarrow \alpha_l$ and $q(\alpha_{l+1})$;
    Compute: $g(\alpha_{l+1})$ and $g(\alpha_l)$;
    if $g(\alpha_{l+1}) \le g(\alpha_l)$ then
        Output: $\alpha_{\mathsf{B}}^{\star}$ and break loop;
    else
        Update: $\alpha_l \leftarrow \alpha_{l+1}$;
```

Given the complexity of solving (38) due to the coupling of the Bessel–K function in the exact SOP and OP functions, we substitute the approximations in (18) and (33) with the functions $p_{\text{op}}^{\mathsf{W}}$ and $p_{\text{sop}}^{\text{int}}$, respectively, then plug in $\alpha_{\mathsf{W}} = 1-\alpha_{\mathsf{B}}$. The optimization problem (38) is thus simplified to

$$\min_{\alpha_{\mathsf{B}}}\ g(\alpha_{\mathsf{B}})\ \text{s.t}\ q(\alpha_{\mathsf{B}}) \le \epsilon, \varphi \le \alpha_{\mathsf{B}} \le 1/(1+\gamma_{\mathsf{W}})-\varphi, \tag{39}$$

where

$$g(x) \triangleq \frac{\lambda_{\mathsf{RB}}\phi}{\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}}} + \frac{\lambda_{\mathsf{RB}}\rho\lambda_{\mathsf{RW}}\lambda_{\mathsf{SR}}\ln(\varpi\overline{\gamma})}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}})\varpi\overline{\gamma}x}, \tag{40}$$

$$q(x) \triangleq \frac{\lambda_{\mathsf{SR}}\lambda_{\Sigma}\gamma_{\mathsf{W}}\ln(\varpi\overline{\gamma})/\varpi\overline{\gamma}}{1-x(1+\gamma_{\mathsf{W}})}, \tag{41}$$

and φ is a small arbitrary value belonging to $(10^{-5}, 10^{-2})$.

Since the problem in (39) contains a convex objective function and convex sets of constraints, it is a convex optimization problem. Consequently, interior-point methods or standard convex solvers can be used to determine the optimal solution. However, using such methods typically results in relatively high computational complexity. Fortunately, the problem involves only one optimization variable α_{B}, and thus, the modified Newton-Raphson iterative root-finding algorithm is well-suited to employ and offers both fast convergence and high accuracy in determining $\alpha_{\mathsf{B}}^{\star}$. The details of this method are outlined in Algorithm 1, where $g'(x) = -\frac{\lambda_{\mathsf{RB}}\rho\lambda_{\mathsf{RW}}\lambda_{\mathsf{SR}}\ln(\varpi\overline{\gamma})}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}})\varpi\overline{\gamma}x^2}$ and $g''(x) = 2\frac{\lambda_{\mathsf{RB}}\rho\lambda_{\mathsf{RW}}\lambda_{\mathsf{SR}}\ln(\varpi\overline{\gamma})}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RW}})\varpi\overline{\gamma}x^3}$. Assuming that $l^{\star}$ represents the total number of iterations required to meet the conditions $q(\alpha_l) \le \epsilon$ and $g(\alpha_{l+1}) \le g(\alpha_l)$, the computational complexity of solving Algorithm 1 is determined by $\mathcal{O}(l^{\star})$.

2) External Eavesdropping Scenario: As with the solution to (38), our objective is to optimize the PA budget to minimize the SOP of external eavesdropping while ensuring that Willie's minimum reliability demand is met. Mathematically, this optimization problem can be formulated as

$$\begin{aligned} \mathbf{P}_3 : \min_{\alpha_{\mathsf{W}},\alpha_{\mathsf{B}}}\ & p_{\text{sop}}^{\text{ext}} && (42a)\\ \text{s.t}\ & \alpha_{\mathsf{W}}+\alpha_{\mathsf{B}} = 1, \alpha_{\mathsf{W}} > 0, \alpha_{\mathsf{B}} > 0, \alpha_{\mathsf{W}} > \alpha_{\mathsf{B}}\gamma_{\mathsf{W}}, && (42b)\\ & p_{\text{op}}^{\mathsf{W}} \le \epsilon. && (42c)\end{aligned}$$

Similar to the method used to solve $\mathbf{P}_2$, we first replace $p_{\text{op}}^{\mathsf{W}}$ and $p_{\text{sop}}^{\text{ext}}$ with (18) and (37), respectively, and combine them with $\alpha_{\mathsf{W}} = 1 - \alpha_{\mathsf{B}}$. As a result, (42) can be simplified to

$$\min_{\alpha_{\mathsf{B}}} \ \vartheta(\alpha_{\mathsf{B}}) \text{ s.t } q(\alpha_{\mathsf{B}}) \le \epsilon, \varphi \le \alpha_{\mathsf{B}} \le 1/(1+\gamma_{\mathsf{W}}) - \varphi, \quad (43)$$

where $\vartheta(x) \triangleq \frac{\lambda_{\mathsf{RB}}\phi}{\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}}} + \frac{\lambda_{\mathsf{RT}}\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho}{(\lambda_{\mathsf{RB}}\phi+\lambda_{\mathsf{RT}})\varpi\overline{\gamma}x} \ln(\varpi\overline{\gamma})$.

The problem (43) is a convex optimization problem due to the coupling of a convex objective function and convex sets of constraints. Therefore, finding the optimal solution $\alpha_{\mathsf{B}}^{\star}$ can be performed similar to Algorithm 1 by replacing $q(\alpha_{\mathsf{B}})$ with $\vartheta(\alpha_{\mathsf{B}})$, $q'(\alpha_{\mathsf{B}})$ with $\vartheta'(\alpha_{\mathsf{B}})$, and $q''(\alpha_{\mathsf{B}})$ with $\vartheta''(\alpha_{\mathsf{B}})$, where

$$\vartheta'(x) = -\lambda_{\mathsf{RT}}\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho \ln(\varpi\overline{\gamma})/[(\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RT}})\varpi\overline{\gamma}x^2], \quad (44)$$

$$\vartheta''(x) = 2\lambda_{\mathsf{RT}}\lambda_{\mathsf{SR}}\lambda_{\mathsf{RB}}\rho \ln(\varpi\overline{\gamma})/[(\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RT}})\varpi\overline{\gamma}x^3]. \quad (45)$$

V. Covertness Evaluation Framework

A. Detection Error Probability Analysis

The DEP refers to the likelihood that a warden, which is an entity that attempts to detect the presence of covert communications, incorrectly identifies whether such a signal is being transmitted. In other words, DEP represents the probability of erroneous detection of covert transmissions, including either the false detection of covert communications when it is absent (false alarm) or the failure to detect covert communications when it is present (missed detection).

Using (8) and (9), the probability that Tom detects Bob's covert signal with an equal priori probabilities of $\mathcal{H}_0$ and $\mathcal{H}_1$ can be expressed as [36]–[39]

$$p_{\text{dep}} = \underbrace{\Pr[\text{D}_1|\mathcal{H}_0]}_{\text{false alarm}} + \underbrace{\Pr[\text{D}_0|\mathcal{H}_1]}_{\text{missed detection}}. \quad (46)$$

Denoted by $p_f \triangleq \Pr[\text{D}_1|\mathcal{H}_0]$ and $p_m \triangleq \Pr[\text{D}_0|\mathcal{H}_1]$, the DEP can be effectively evaluated using the following lemma.

Lemma 5: The DEP can be calculated as follows:

$$p_{\text{dep}} = \begin{cases} 1, & \kappa \triangleq \omega - \sigma^2 \le 0, \\ p_f + p_m, & \kappa > 0. \end{cases} \quad (47)$$

where the false alarm probability (FAP) p_f and missed detection probability (MDP) p_m can be derived, respectively, as

$$p_f = 2\sqrt{\Delta\kappa/[\alpha_{\mathsf{W}}\overline{\gamma}]}\mathcal{K}_1(2\sqrt{\Delta\kappa/[\alpha_{\mathsf{W}}\overline{\gamma}]}), \quad (48)$$

$$p_m = 1 - 2\sqrt{\Delta\kappa/\overline{\gamma}}\mathcal{K}_1(2\sqrt{\Delta\kappa/\overline{\gamma}}). \quad (49)$$

where $\Delta \triangleq \lambda_{\mathsf{SR}}\lambda_{\mathsf{RT}}/\varpi\sigma^2$.

Proof: See Appendix D. ■

From (47), it is evident that when $\omega \le \sigma^2$, $p_f = 1$ and $p_m = 0$, we have $p_{\text{dep}} = 1$. Thus, Tom receives a false alarm because he fails to detect the covert signal. For the case where $\omega > \sigma^2$, it is observed that when $\alpha_{\mathsf{W}} = 1$, i.e., without covert signal's transmission, the DEP becomes $p_{\text{dep}} = p_f + p_m = 1$. These instances shed light on the fact that Tom cannot form a correct judgment due to his monitoring results being either a false alarm or a missed detection.

To deeply understand the DEP's behaviour, we study its performance under low and high transmit SNR conditions. We begin by invoking [44, Eq. (8.451.6)] to get the approximation

$$\mathcal{K}_1(x) \overset{x\to\infty}{\simeq} \sqrt{\pi/2x}\exp(-x). \quad (50)$$

Accordingly, for a low transmit SNR regime, i.e., $\overline{\gamma} \to 0$, p_f and p_m can be approximated as

$$p_f^{\text{lo}} \overset{\overline{\gamma}\to 0}{\simeq} \sqrt{\pi\sqrt{\Delta\kappa/[\alpha_{\mathsf{W}}\overline{\gamma}]}}\exp(-2\sqrt{\Delta\kappa/[\alpha_{\mathsf{W}}\overline{\gamma}]}), \quad (51)$$

$$p_m^{\text{lo}} \overset{\overline{\gamma}\to 0}{\simeq} 1 - \sqrt{\pi\sqrt{\Delta\kappa/\overline{\gamma}}}\exp(-2\sqrt{\Delta\kappa/\overline{\gamma}}). \quad (52)$$

Subsequently, we apply the L'Hospital's rule for $s(x) = \sqrt{x}\exp(-x) = \sqrt{x}/\exp(x)$, for $x \to \infty$, to get

$$\lim_{x\to\infty} s(x) = \lim_{x\to\infty} \frac{1}{2\sqrt{x}\exp(x)} = 0. \quad (53)$$

Substituting for $x = 2\sqrt{\Delta\kappa/[\alpha_{\mathsf{W}}\overline{\gamma}]}$ and $x = 2\sqrt{\Delta\kappa/\overline{\gamma}}$ for the corresponding results in (51) and (52) to (53), we deduce that $p_f^{\text{lo}} \to 0$ and $p_m^{\text{lo}} \to 1$. This indicates that the output judgment represents a missed detection, and consequently, Tom is unable to detect the covert signal since $p_{\text{dep}}^{\text{lo}} = p_f^{\text{lo}} + p_m^{\text{lo}} \to 1$. Covert transmission is thus ensured in the low SNR region.

In the case of high SNR (i.e., $\overline{\gamma} \to \infty$), by using (14), p_f and p_m can be approximated, respectively, as

$$p_f^{\text{up}} \simeq 1 + \frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}} \ln\left(\frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}}\right), p_m^{\text{up}} \simeq -\frac{\Delta\kappa}{\overline{\gamma}} \ln\left(\frac{\Delta\kappa}{\overline{\gamma}}\right). \quad (54)$$

Based on the characteristics of (20), we can readily deduce that $p_f^{\text{up}} \to 1$ and $p_m^{\text{up}} \to 0$. This implies that Tom's monitoring results in a false alarm, and thus, the covert transmission remains secure in the high SNR regions since $p_{\text{dep}}^{\text{up}} = p_f^{\text{up}} + p_m^{\text{up}} \to 1$.

From the above two analyses, it is evident that covert communications are favored at low and high SNR levels. When moderate SNR levels are employed, the likelihood of information leakage increases, rendering the system more vulnerable to detection by Tom. Compared to low SNR levels, employing a high SNR improves communications between Sam and Bob, necessitating the study of the operating range of the transmit SNR that does not minimize the DEP. Specifically, taking the partial derivative of $p_{\text{dep}}^{\text{up}}$ with respect to $\overline{\gamma}$ yields

$$\frac{\partial p_{\text{dep}}^{\text{up}}}{\partial\overline{\gamma}} = -\frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}^2}\left[\ln\left(\frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}}\right) + 1\right] + \frac{\Delta\kappa}{\overline{\gamma}^2}\left[\ln\left(\frac{\Delta\kappa}{\overline{\gamma}}\right) + 1\right]. \quad (55)$$

It is evident that the SNR should be configured such that the DEP is an increasing function of SNR, i.e., $\partial p_{\text{dep}}^{\text{up}}/\partial\overline{\gamma} > 0$. From this observation, the operating range of the transmit SNR in Watts can be configured as

$$\overline{\gamma} > \exp\left(1 + \ln(\Delta\kappa) - \frac{\ln(\alpha_{\mathsf{W}})}{1-\alpha_{\mathsf{W}}}\right). \quad (56)$$

Furthermore, an examination of ω reveals that as $\omega \to \sigma^2$, or equivalently as $\kappa \to 0$, we can deduce that $p_f \to 1$ and $p_m \to 0$. When $\omega \to \infty$, i.e., $\kappa \to \infty$, we can deduce that $p_f \to 0$ and $p_m \to 1$. Intuitively, selecting an unsuitable ω at Tom causes $p_{\text{dep}} = p_f + p_m \to 1$, thereby providing robust protection for covert communication between Sam and Bob. However, a large communication distance between Sam and AAR and between AAR and Tom also increases the DEP.

B. Detection Error Probability Minimization

In practice, Sam cannot know the detection threshold ω, and thus, the DEP obtained from (47) is evaluated for an arbitrary value ω. Nevertheless, Tom can optimally set ω to minimize the DEP, i.e., $\min_\omega p_{\text{dep}}$. Therefore, finding the optimal solution for ω becomes crucial in reflecting the worst-case scenario of covert communications, thus aiding the development of new, efficient security transmission methods. Mathematically, this problem can be formulated as

$$\min_{\kappa}\ p_{\text{dep}}(\kappa) \quad \text{s.t.} \quad \kappa > 0. \tag{57}$$

The involvement of the Bessel–K function in (47) complicates the determination of the convexity of $p_{\text{dep}}(\kappa)$ on the set containing the interval $\kappa \in (0, \infty)$. To untangle the analysis, we first use the approximation in (14) for a small value of κ to obtain a simplified expression for $p_{\text{dep}}(\kappa)$ as

$$p_{\text{dep}}(\kappa) \simeq 1 + \frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}} \ln\left(\frac{\Delta\kappa}{\alpha_{\mathsf{W}}\overline{\gamma}}\right) - \frac{\Delta\kappa}{\overline{\gamma}} \ln\left(\frac{\Delta\kappa}{\overline{\gamma}}\right). \tag{58}$$

Proposition 1: $p_{\text{dep}}(\kappa)$ in (58) is a strictly convex function of κ. Accordingly, the global optimal solution is calculated as $\kappa_1 = \overline{\gamma}\exp\left(\ln\left(\alpha_{\mathsf{W}}\right)/(1-\alpha_{\mathsf{W}}) - 1\right)/\Delta$.

Proof: Taking the first and second order derivatives of $p_{\text{dep}}(\kappa)$ in (58) with respect to κ yields $p'_{\text{dep}}(\kappa) = \frac{\Delta}{\alpha_{\mathsf{W}}\overline{\gamma}}\left[(1-\alpha_{\mathsf{W}})[\ln\left(\Delta\kappa/\overline{\gamma}\right)+1] + \ln\left(1/\alpha_{\mathsf{W}}\right)\right]$ and $p''_{\text{dep}}(\kappa) = (1-\alpha_{\mathsf{W}})\Delta/[\alpha_{\mathsf{W}}\overline{\gamma}\kappa] > 0$, respectively. Next, solving $p'_{\text{dep}}(\kappa)$ equal to zero and after some algebraic steps, we obtain the desired result, ending the proof. ■

Similarly, denoting $u(x) = v(x)/\sqrt{\alpha_{\mathsf{W}}}$, $v(x) = 2\sqrt{\Delta x/\overline{\gamma}}$, and $p(x) = \sqrt{x}\exp(x)$, we use the approximation (50) for a large κ to simplify $p_{\text{dep}}(\kappa)$ as

$$p_{\text{dep}}(\kappa) \simeq 1 + \sqrt{\pi/2}[p(u(\kappa)) - p(v(\kappa))]. \tag{59}$$

Proposition 2: $p_{\text{dep}}(\kappa)$ in (59) is a quasi-convex function with respect to κ. A root κ_2 exists such that $p_{\text{dep}}(\kappa)$ is minimized.

Proof: Taking the first-order and second-order derivatives of $p_{\text{dep}}(\kappa)$ in (59) to κ and multiplying with $\sqrt{2/\pi}$ yields

$$\begin{aligned} p'_{\text{dep}}(\kappa) &= \sqrt{\frac{\pi}{2}}\left[\frac{\partial p(u(\kappa))}{\partial u(\kappa)}\frac{\partial u(\kappa)}{\partial \kappa} - \frac{\partial p(v(\kappa))}{\partial v(\kappa)}\frac{\partial v(\kappa)}{\partial \kappa}\right] \\ &= \sqrt{\frac{\pi}{2}}\underbrace{\left[\frac{1}{\sqrt{\alpha_{\mathsf{W}}}}\frac{\partial p(u(\kappa))}{\partial u(\kappa)} - \frac{\partial p(v(\kappa))}{\partial v(\kappa)}\right]}_{\Lambda(\kappa)}\frac{\partial v(\kappa)}{\partial \kappa}, \end{aligned} \tag{60}$$

$$\begin{aligned} p''_{\text{dep}}(\kappa) &= \sqrt{\frac{\pi}{2}}\left[\frac{\partial^2 p(u(\kappa))}{\partial u(\kappa)^2}\left[\frac{\partial u(\kappa)}{\partial \kappa}\right]^2 + \frac{\partial p(u(\kappa))}{\partial u(\kappa)}\frac{\partial^2 u(\kappa)}{\partial \kappa^2}\right. \\ &\quad \left. - \frac{\partial^2 p(v(\kappa))}{\partial v(\kappa)^2}\left[\frac{\partial v(\kappa)}{\partial \kappa}\right]^2 - \frac{\partial p(v(\kappa))}{\partial v(\kappa)}\frac{\partial^2 v(\kappa)}{\partial \kappa^2}\right] \\ &= \underbrace{\left[\frac{1}{\alpha_{\mathsf{W}}}\frac{\partial^2 p(u(\kappa))}{\partial u(\kappa)^2} - \frac{\partial^2 p(v(\kappa))}{\partial v(\kappa)^2}\right]}_{\Xi(\kappa)}\left[\frac{\partial v(\kappa)}{\partial \kappa}\right]^2 \\ &\quad + \Lambda(\kappa)\frac{\partial^2 v(\kappa)}{\partial \kappa^2}. \end{aligned} \tag{61}$$

Since $p_{\text{dep}}(\kappa)$ in (59) is a continuous function of κ on the feasible domain, it is said to be a quasi-convex function if we can further prove that $p''_{\text{dep}}(\kappa_2) > 0$ with $p'_{\text{dep}}(\kappa_2) = 0$ [36].

Since, $\partial v(\kappa)/\partial\kappa = \sqrt{\Delta/\overline{\gamma}\kappa} > 0$, we find that $p'_{\text{dep}}(\kappa_2) = 0$ if and only if $\Lambda(\kappa_2) = 0$. Next, we prove that $\Xi(\kappa_2) > 0$, then $p''_{\text{dep}}(\kappa_2) > 0$. By taking the first-order and second-order derivatives of $p(x)$ with respect to x, we get

$$\frac{\partial p(x)}{\partial x} = -\frac{2x-1}{2\sqrt{x}}\exp(-x), \tag{62}$$

$$\frac{\partial^2 p(x)}{\partial x^2} = \frac{(2x-1)^2-2}{4x\sqrt{x}}\exp(-x). \tag{63}$$

By substituting $u(x)$ and $v(x)$ into (62) and (63), we obtain

$$\begin{aligned} \Lambda(x) = &-\frac{2v(x)-\sqrt{\alpha_{\mathsf{W}}}}{2\sqrt{v(x)\alpha_{\mathsf{W}}\sqrt{\alpha_{\mathsf{W}}}}}\exp(-v(x)/\sqrt{\alpha_{\mathsf{W}}}) \\ &+ \frac{2v(x)-1}{2\sqrt{v(x)}}\exp(-v(x)). \end{aligned} \tag{64}$$

Similarly, after some manipulation, we get the following result:

$$\begin{aligned} \Xi(x) = &\frac{\exp(-2\sqrt{\Delta x/\overline{\gamma}})\sqrt{\overline{\gamma}\sqrt{\overline{\gamma}}}}{8\alpha_{\mathsf{W}}\sqrt[4]{\alpha_{\mathsf{W}}}\sqrt{2\Delta x\sqrt{\Delta x}}}\left[\exp(2\sqrt{\Delta x/\overline{\gamma}}[1-\sqrt{\alpha_{\mathsf{W}}}])\right. \\ &\left. - \alpha_{\mathsf{W}}\sqrt[4]{\alpha_{\mathsf{W}}}\frac{(4\sqrt{\Delta x/\overline{\gamma}}-1)^2-2}{(4\sqrt{\Delta x/\overline{\gamma}}-\alpha_{\mathsf{W}})^2-\alpha_{\mathsf{W}}}\right]. \end{aligned} \tag{65}$$

It is evident that $\alpha_{\mathsf{W}} < 1$, $(4\sqrt{\Delta x/\overline{\gamma}}-1)^2-2 < (4\sqrt{\Delta x/\overline{\gamma}}-\alpha_{\mathsf{W}})^2-\alpha_{\mathsf{W}}$, and $\alpha_{\mathsf{W}}\sqrt[4]{\alpha_{\mathsf{W}}} < 1$; thus, $\Xi(x) > 0$ always holds for all $x > 0$. The proof is concluded. ■

Since the DEP obtained in (47) can be approximated by the convex function $p_{\text{dep}}(\kappa)$ in (58) for a small κ and the quasi-convex function $p_{\text{dep}}(\kappa)$ in (59) for a large κ, the golden-section search (GSS) method [31] can be applied to the DEP in (47) to achieve the optimal solution $\kappa^\star$, if the feasible domain $[\kappa_1, \kappa_2]$ can be determined. However, the exact solution for $\Lambda(x) = 0$ cannot be obtained in any direct manner. Finding $\kappa^\star$ can therefore be done in two steps. First, we apply Newton's method [18] to $p_{\text{dep}}(\kappa)$ in (59) to obtain κ_2, based on the obtained value κ_1. Second, we apply the GSS to the DEP obtained in (47) to find $\kappa^\star$ within the feasible domain $[\kappa_1, \kappa_2]$. In summary, the algorithm for determining $\kappa^\star$ involves two iterative search phases. The total complexity of the algorithm is $\mathcal{O}(L+M)$, where L and M are the numbers of iterations to find κ_2 and $\kappa^\star$, respectively.

VI. Numerical Results and Discussion

To validate the previously developed analytical frameworks, this section provides some illustrative examples using Monte-Carlo simulations, followed by discussions on the impact of key system parameters on the OP, SOP, and DEP. Without loss of generality, we assume that $d_{\mathsf{SR}} = d_{\mathsf{RW}} = d_{\mathsf{RT}} = 10$ m, $d_{\mathsf{RB}} = 8$ m, $d_0 = 10$ m, $\eta = 3$, $\varpi = 10$ dBm [23], $r_{\mathsf{W}} = 0.5$ bps/Hz, $r_{\mathsf{B}} = 1.5$ bps/Hz, and $R_{\mathsf{B}} = 0.5$ bps/Hz.

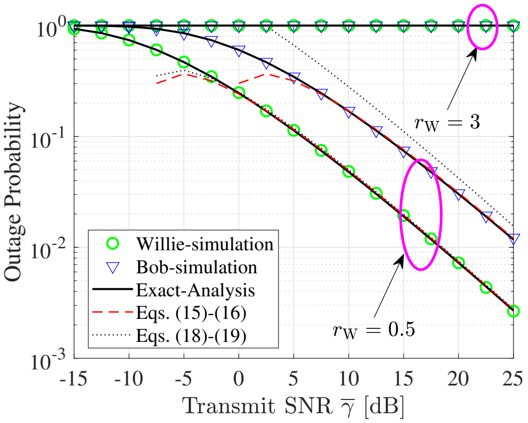


Fig. 3. OP performance at $\alpha_W = 0.7$ and $\alpha_B = 0.3$.

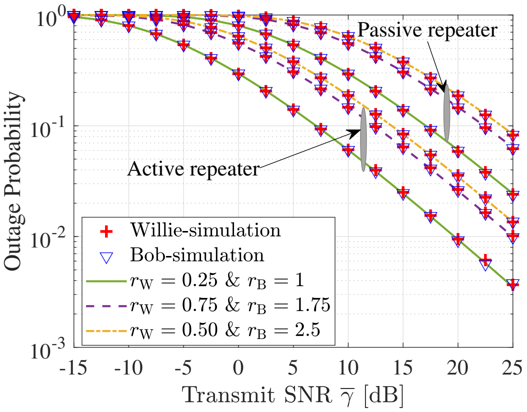


Fig. 5. OP fairness under varying requirements of r_W and r_B.

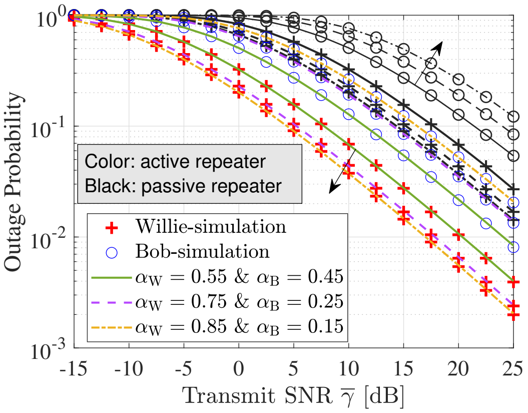


Fig. 4. OP performance under varying combinations of α_W and α_B.

A. Outage Probability Evaluation

Fig. 3 plots the OPs of both Willie and Bob as a function of SNR. The system is considered to be non-operating when $r_W = 3$ bps/Hz and in an operating state (i.e., $\gamma_W < \alpha_W/\alpha_B$) when $r_W = 0.5$ bps/Hz. Moreover, the analytical results closely align with the Monte-Carlo simulations and tend to converge with the approximated results in the high SNR region. For $r_W = 0.5$, all OP curves exhibit a diversity order of one, as stated in Remark 1. However, no diversity increase is observed with $r_W = 3$ since the OP curves converge to one.

Fig. 4 illustrates the OP performance of passive and active reconfigurable repeaters under different configurations of α_W and α_B. As observed, utilizing AAR improves the OPs of users compared to the passive reconfigurable repeater (i.e., $\varpi = 1$). The figure also reveals that, as the value of α_W increases, Willie's OP decreases. However, this trend is reversed in the case of Bob's OP performance, where the smaller the power level allocated to Bob's signal (i.e., α_B), the poorer the signal reception. This aligns with the findings in Remark 1.

To address the performance tradeoff observed in Fig. 4, the results in Fig. 5 depict the OP of Willie and Bob using the proposed closed-form solutions in (27) and (28). It is worth mentioning that the use of a standard convex solver such as CVX yields the same results in the figure. As expected, the OP curves of Willie and Bob align closely across the low SNR range but also in the moderate and high SNR regions, regardless of their target data rate requirements.

B. Secrecy Outage Probability Evaluation

1) Internal eavesdropping scenario: Fig. 6 presents the SOP when Willie attempts to intercept Bob's signal after decoding his message, at the settings of $\alpha_W = 0.6$ and $\alpha_B = 0.4$. The analytical results closely match the simulation results and converge with the asymptotic results in the high SNR region, illustrating the robustness of the developed mathematical frameworks. In detail, when $r_W = 1.5$, the SOP reaches an ideal state in which all information transmitted to Bob is fully protected from Willie's eavesdropping. This occurs because the operating condition $\gamma_W = 2^{r_W} - 1 < \alpha_W/\alpha_B$ is not satisfied, meaning that Willie is unable to decode his message. However, this also results in Bob being unable to detect his own message. When $\gamma_W = 2^{r_W} - 1 < \alpha_W/\alpha_B$, we observe that at $r_W = 0.5$, transmitting at a low or moderate SNR yields better SOP performance than with a high SNR. This is because, in the latter case, Willie has more opportunities to decode his message, thereby increasing Bob's message-decoding capability. However, the SOP floor phenomenon resulting from a high SNR can be controlled by adjusting Bob's safe target data rate. Notably, the SOP increases significantly with an increment of R_B. This aligns with the findings in Remark 2.

In Fig. 7, we examine the relationship between the OP and the SOP to the transmit SNR. As observed, increasing the transmit SNR improves the OPs of both Willie and Bob for a fixed PA coefficient. However, this also enhances Willie's ability to intercept Bob's signal, highlighting a tradeoff between reliability and security. For Willie's minimum OP requirement of $\epsilon = 0.5$, applying Algorithm 1 permits an improvement in Bob's security performance. Notably, when the transmit SNR exceeds 12.5 dB, the considered system significantly improves both the SOP and Bob's OP.

2) External eavesdropping scenario: Fig. 8 presents the SOP as Tom attempts to decode Bob's signal, with the configuration of $\alpha_W = 0.6$ and $\alpha_B = 0.4$. The analytical and simulation results align perfectly, confirming the effectiveness

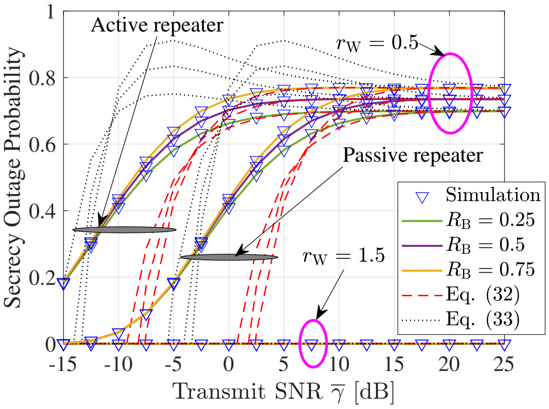


Fig. 6. SOP of the internal eavesdropping scenario under varying R_B.

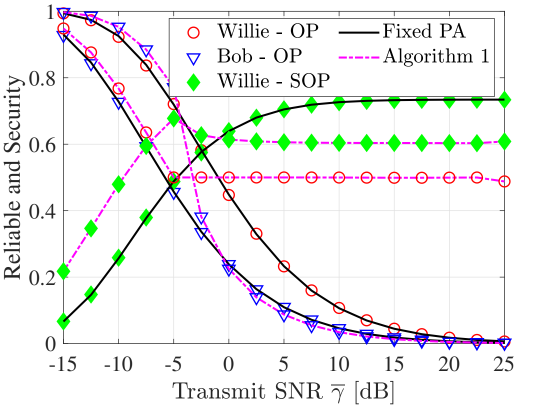


Fig. 7. OPs of Willie and Bob, and the SOP of the internal eavesdropping scenario, where $\epsilon = 0.5$, $R_B = r_B = 0.5$, and $r_W = 0.75$ are assumed. For the case of fixed PA, $\alpha_W = 0.6$ and $\alpha_B = 0.4$ are assumed.

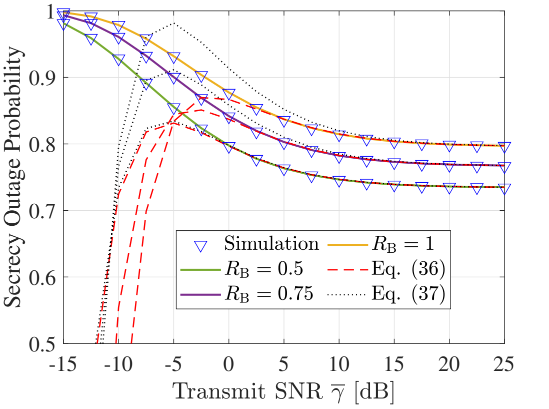


Fig. 8. SOP of the external eavesdropping scenario under varying R_B.

of the proposed mathematical framework. Unlike the SOP behavior in Fig. 6, increasing the transmit SNR from the low to moderate regions significantly improves the SOP shown in Fig. 8, but offers no improvement in the high SNR region, which is consistent with the analysis in Remark 3. However, both Figs. 6 and 8 share the same trend that increasing Bob's secure target data rate R_B dramatically increases the SOP.

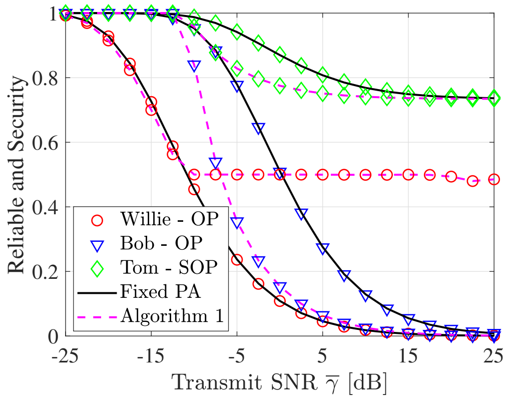


Fig. 9. OPs of Willie and Bob, and the SOP of the external eavesdropping scenario, where $\epsilon = 0.5$, $R_B = r_B = 0.5$, and $r_W = 0.25$ are assumed. For the case of fixed PA, $\alpha_W = 0.6$ and $\alpha_B = 0.4$ are assumed.

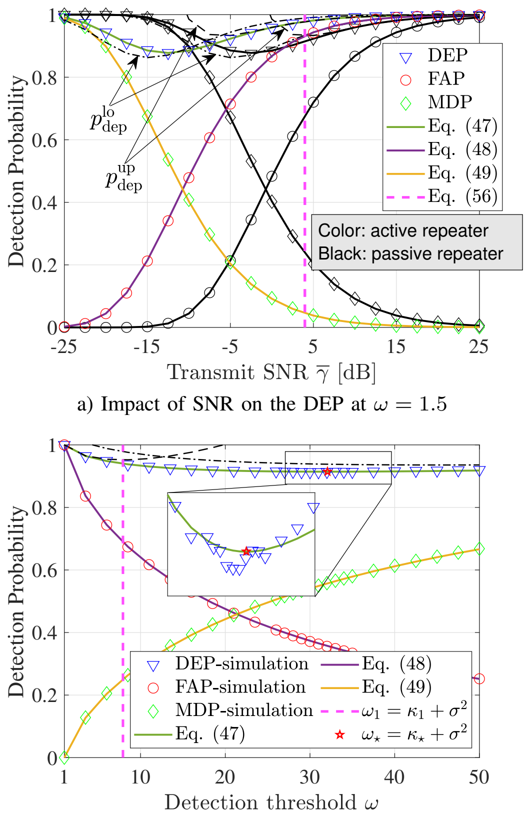
Fig. 9 illustrates the relationship between the OP and the SOP in the external eavesdropping scenario for the transmit SNR. In contrast to the performance trend observed in Fig. 6, both the OP and SOP for a fixed PA coefficient improve significantly as the transmit SNR increases. This occurs because Tom does not decode Willie's signal. As a result, increasing the transmit SNR enhances the received SNR for decoding Bob's signal at both Bob and Tom, as described by (6) and (4). Similar to the internal eavesdropping scenario, for Willie's minimum OP requirement of $\epsilon = 0.5$, using Algorithm 1 strengthens Bob's security performance against Tom's eavesdropping while improving Bob's OP.

C. Detection Error Probability Evaluation

Fig. 10 plots the DEP at Tom under two different conditions. In Fig. 10(a), the detection threshold is fixed at $\omega = 1.5$, while the SOP is plotted as a function of the transmit SNR. The results illustrate excellent agreement between the derived expressions and the simulated results. As the transmit SNR approaches zero or infinity, the DEP converges with the asymptotic solutions, represented by dash-dotted lines for low SNR and dashed lines for high SNR. We can also observe that as the transmit SNR increases, the MDP decreases, whereas the FAP tends to increase. Notably, when the FAP and MDP intersect, the DEP reaches its minimum value. Application of the proposed solution in (56) prevents the DEP from falling into its worst-case performance. Fig. 10(b) depicts a reversal of this setting, with the SOP plotted as a function of the detection threshold, while the transmit SNR is fixed at 10 dB. We observe that as ω increases, the DEP initially decreases, approaches its minimum value, and then increases, with the optimal value lying between 2 and 7. By using the proposed approach, the sub-optimal detection threshold value can be effectively determined through $\omega^{\star}$.

VII. Concluding Remarks

The present study provides comprehensive analysis and optimization frameworks for evaluating the performance of ARR-assisted NOMA networks, specifically addressing the presence of internal and external eavesdroppers and an external warden. The proposed analytical frameworks, including exact



a) Impact of SNR on the DEP at $\omega = 1.5$

b) Impact of the detection threshold on the DEP at $\overline{\gamma} = 10$ dB

Fig. 10. DEP performance under the impact of (a) the SNR and (b) the detection thresholds, where $\alpha_{\mathsf{W}} = 0.6$ and $\alpha_{\mathsf{B}} = 0.4$ are assumed.

and approximate solutions, were thoroughly validated through Monte-Carlo simulations that demonstrate the efficacy of the optimization approaches. Several key observations emerged from the analysis. First, increasing the transmit SNR significantly improves communications reliability but also provides greater opportunities for internal eavesdroppers to compromise the legitimate signal. Second, a lower transmit SNR favors the SOP in internal eavesdropping scenarios whereas higher SNR modes are more effective in mitigating external eavesdropping risks. Third, minimizing the SOP performance enhances the physical-layer security and simultaneously improves communications reliability. Eventually, a detection threshold algorithm that guarantees optimal DEP is developed.

Besides the technical contributions, this study also presents open challenges and several interesting research topics for future analysis. For example, leveraging MIMO or massive MIMO technologies could further enhance system performance but presents challenges for energy-constrained IoT devices, necessitating adaptive design reconsideration. Analyzing multiple ARRs is another potential area, given the uncertain trade-off between cumulative multi-hop latency, implementation cost, and performance gains. Moreover, investigating the effects of imperfect CSI, SIC, and hardware impairments is crucial to better capture characteristics of practical systems. Furthermore, exploring performance fairness between cell-edge and cell-center users in massive connectivity scenarios is an important research direction.

Appendix A: Proof of Lemma 1

We begin the proof by expressing (10) as

$$\begin{aligned} p_{\text{op}}^{\mathsf{W}} &= 1 - \Pr[|h_{\mathsf{SR}}|^2 \min\{|h_{\mathsf{RW}}|^2, |h_{\mathsf{RB}}|^2\} > \tau_{\mathsf{W}}/(\varpi\overline{\gamma})] \\ &= 1 - \int_0^\infty \prod_{\mathsf{U}} [1 - F_{|h_{\mathsf{RU}}|^2}(\tau_{\mathsf{W}}/(\varpi\overline{\gamma}x))] f_{|h_{\mathsf{SR}}|^2}(x)dx. \quad (66) \end{aligned}$$

By plugging $F_{|h_{\mathsf{RU}}|^2}(\cdot)$ and $f_{|h_{\mathsf{SR}}|^2}(\cdot)$ into (66), $p_{\text{op}}^{\mathsf{W}}$ can be rewritten as

$$p_{\text{op}}^{\mathsf{W}} = 1 - \int_0^\infty \exp(-\lambda_\Sigma \tau_{\mathsf{W}}/(\varpi\overline{\gamma}x) - \lambda_{\mathsf{SR}}x)\lambda_{\mathsf{SR}}dx. \quad (67)$$

By invoking [44, Eq. (3.471.9)] for (67), we can obtain the final solution for $p_{\text{op}}^{\mathsf{W}}$. Applying the same method, the solution for $p_{\text{op}}^{\mathsf{B}}$ is also attained. The proof is concluded.

Appendix B: Proof of Lemma 3

By substituting Ψ_{W} and ψ_{B} in (4) and ψ_{W} in (5) into (30), the SOP of internal eavesdropping can be rewritten as

$$\begin{aligned} p_{\text{sop}}^{\text{int}} &= \Pr\left[|h_{\mathsf{RW}}|^2 \geq \frac{\tau_{\mathsf{W}}/\varpi}{|h_{\mathsf{SR}}|^2\overline{\gamma}}, |h_{\mathsf{RB}}|^2 < \frac{\rho/[\alpha_{\mathsf{B}}\varpi]}{\overline{\gamma}|h_{\mathsf{SR}}|^2} + \phi|h_{\mathsf{RW}}|^2\right] \\ &= \int_0^\infty \int_{\frac{\tau_{\mathsf{W}}}{x\varpi\overline{\gamma}}}^\infty F_{|h_{\mathsf{RB}}|^2}\left(\frac{\rho/\varpi\overline{\gamma}}{x\alpha_{\mathsf{B}}} + \phi y\right) f_{|h_{\mathsf{RW}}|^2}(y) f_{|h_{\mathsf{SR}}|^2}(x)dydx \\ &= \lambda_{\mathsf{SR}} \int_0^\infty \exp\left(-\lambda_{\mathsf{RW}}\frac{\tau_{\mathsf{W}}}{x\varpi\overline{\gamma}} - \lambda_{\mathsf{SR}}x\right) dx \\ &\quad - \frac{\lambda_{\mathsf{RW}}\lambda_{\mathsf{SR}}}{\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}} \int_0^\infty \exp\left(-\frac{\zeta}{x\varpi\overline{\gamma}} - \lambda_{\mathsf{SR}}x\right) dx. \quad (68) \end{aligned}$$

Subsequently, by invoking [44, Eq. (3.471.9)] for the integrals in (68), we obtain the desired result. The proof is concluded.

Appendix C: Proof of Lemma 4

By substituting ψ_{B} in (4) and ψ_{T} in (6) into (34), the SOP of external eavesdropping can be rewritten as

$$\begin{aligned} p_{\text{sop}}^{\text{ext}} &= \Pr\left[|h_{\mathsf{RB}}|^2 < \frac{\rho/\varpi\overline{\gamma}}{\alpha_{\mathsf{B}}|h_{\mathsf{SR}}|^2} + \phi|h_{\mathsf{RT}}|^2\right] \\ &= \int_0^\infty \int_0^\infty F_{|h_{\mathsf{RB}}|^2}\left(\frac{\rho/\varpi\overline{\gamma}}{x\alpha_{\mathsf{B}}} + \phi y\right) f_{|h_{\mathsf{RT}}|^2}(y) f_{|h_{\mathsf{SR}}|^2}(x)dydx \\ &= 1 - \frac{\lambda_{\mathsf{RT}}\lambda_{\mathsf{SR}}}{\lambda_{\mathsf{RB}}\phi + \lambda_{\mathsf{RW}}} \int_0^\infty \exp\left(-\frac{\lambda_{\mathsf{RB}}\rho}{\alpha_{\mathsf{B}}\varpi\overline{\gamma}x} - \lambda_{\mathsf{SR}}x\right)dx. \quad (69) \end{aligned}$$

Invoking [44, Eq. (3.471.9)] for the above integral yields the desired result. The proof is concluded.

Appendix D: Proof of Lemma 5

From (8) and (9), the FAP p_f can be derived as follows:

$$\begin{aligned} p_f &= \Pr[\alpha_{\mathsf{W}}\varpi P|h_{\mathsf{SR}}|^2|h_{\mathsf{RT}}|^2 + \sigma^2 \geq \omega] \\ &= \begin{cases} 1, & \kappa \leq 0, \\ \Pr\left[|h_{\mathsf{SR}}|^2|h_{\mathsf{RT}}|^2 \geq \frac{\kappa}{\alpha_{\mathsf{W}}\varpi\sigma^2\overline{\gamma}}\right], & \kappa > 0. \end{cases} \quad (70) \end{aligned}$$

Similarly, the MDP p_m is given by

$$\begin{aligned} p_m &= \Pr[\varpi P|h_{\mathsf{SR}}|^2|h_{\mathsf{RT}}|^2 + \sigma^2 \leq \omega] \\ &= \begin{cases} 0, & \kappa \leq 0, \\ \Pr\left[|h_{\mathsf{SR}}|^2|h_{\mathsf{RT}}|^2 \leq \frac{\kappa}{\varpi\sigma^2\overline{\gamma}}\right], & \kappa > 0. \end{cases} \quad (71) \end{aligned}$$

Using the same method to (66), p_f and p_m are combined to yield the desired result, ending the proof.

References

[1] S. K. Lee, M. Bae, and H. Kim, “Future of IoT networks: A survey,” *Appl. Sci.*, vol. 7, no. 10, p. 1072, Oct. 2017.

[2] O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen *et al.*, “A survey on intelligent internet of things: Applications, security, privacy, and future directions,” *IEEE Commun. Surv. Tutorials*, Jul. 2024, in press.

[3] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, “Covert communications: A comprehensive survey,” *IEEE Commun. Surv. Tut.*, vol. 25, no. 2, pp. 1173–1198, Secondquarter 2023.

[4] L. Xing, “Reliability in Internet of Things: Current status and future perspectives,” *IEEE Internet Thing J.*, vol. 7, no. 8, pp. 6704–6721, Aug. 2020.

[5] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, “Hiding information in noise: Fundamental limits of covert wireless communication,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, Dec. 2015.

[6] J. Hu, C. Lin, and X. Li, “Relationship privacy leakage in network traffics,” in *2016 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Waikoloa, HI, USA, 2016, pp. 1–9.

[7] Y. Yuan, S. Wang, Y. Wu, H. V. Poor, Z. Ding, X. You, and L. Hanzo, “NOMA for next-generation massive IoT: Performance potential and technology directions,” *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 115–121, Jul. 2021.

[8] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, “Grant-free non-orthogonal multiple access for IoT: A survey,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1805–1838, Thirdquarter 2020.

[9] X. Chen, R. Jia, and D. W. K. Ng, “On the design of massive non-orthogonal multiple access with imperfect successive interference cancellation,” *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2539–2551, Mar. 2019.

[10] T.-H. Vu, Q.-V. Pham, T.-T. Nguyen, D. B. da Costa, and S. Kim, “Enhancing RIS-aided two-way full-duplex communication with non-orthogonal multiple access,” *IEEE Internet Thing J.*, vol. 11, no. 11, pp. 19 963 – 19 977, Jun. 2024.

[11] T.-T. Nguyen, T.-H. Vu, L.-T. Tu, T. T. Duy, Q.-S. Nguyen, and D. B. da Costa, “A low-complexity relaying protocol for cooperative short-packet NOMA-based spectrum sharing systems,” *IEEE Trans. Veh. Technol.*, vol. 73, Jun. 2024.

[12] P. Thi Dan Ngoc, T. T. Duy, N. Luong Nhat, T. Hanh, Y. H. Chung, and L.-T. Tu, “On the performance of outage probability in cognitive NOMA random networks with hardware impairments,” *J. Inf. Telecommun.*, vol. 8, no. 3, pp. 325–348, Dec. 2023.

[13] Y. Zhang, W. He, X. Li, H. Peng, K. Rabie, G. Nauryzbayev, B. M. ElHalawany, and M. Zhu, “Covert communication in downlink NOMA systems with channel uncertainty,” *IEEE Sensors J.*, vol. 22, no. 19, pp. 19 101–19 112, Oct. 2022.

[14] T.-H. Vu, Q.-V. Pham, D. B. da Costa, M. Debbah, and S. Kim, “Physical-layer security in short-packet NOMA systems with untrusted near users,” in *2023 IEEE Int. Conf. Commun. Workshop (ICC Workshops)*, Rome, Italy, 2023, pp. 1830–1835.

[15] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[16] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[17] N. H. Tu and K. Lee, “Performance analysis and optimization of multihop MIMO relay networks in short-packet communications,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4549–4562, Jun. 2022.

[18] N. T. Y. Linh, N. H. Tu, P. N. Son, and V. N. Q. Bao, “Dual-hop relaying networks for short-packet URLLCs: Performance analysis and optimization,” *J. Commun. Netw.*, vol. 24, no. 4, pp. 408–418, Aug. 2022.

[19] N. H. Tu, T.-D. Hoang, and K. Lee, “Short-packet URLLCs for MIMO underlay cognitive multihop relaying with imperfect CSI,” *IEEE Access*, vol. 11, pp. 81 672–81 689, 2023.

[20] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, “Intelligent reflecting surface-aided wireless communications: A tutorial,” *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, May 2021.

[21] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, “Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 4, pp. 2283–2314, Fourthquarter 2020.

[22] N. H. Tu and K. Lee, “IRS-assisted coordinated direct and multiantenna relay transmission for MIMO SWIPT systems,” *IEEE Syst. J.*, vol. 18, no. 2, pp. 1208–1219, Jun. 2024.

[23] H. Iimori, E. Kurihara, T. Yoshida, J. Vieira, and S. Malomsoky, “Amplification strategy in repeater-assisted MIMO systems via minorization maximization,” in *GLOBECOM 2023 IEEE Int. Conf. Commun.*, Kuala Lumpur, Malaysia, 2023, pp. 4989–4994.

[24] G. Leone, E. Moro, I. Filippini, A. Capone, and D. De Donno, “Towards reliable mmWave 6G RAN: Reconfigurable surfaces, smart repeaters, or both?” in *2022 20th Int. Symp. Model. Optim. Mobile, Ad hoc Wireless Netw. (WiOpt)*, Torino, Italy, 2022, pp. 81–88.

[25] S. Willhammar, H. Iimori, J. Vieira, L. Sundström, F. Tufvesson, and E. G. Larsson, “Achieving distributed mimo performance with repeater-assisted cellular massive MIMO,” *arXiv preprint arXiv:2406.00142*, 2024.

[26] L.-S. Tsai and D.-s. Shiu, “Capacity scaling and coverage for repeater-aided MIMO systems in line-of-sight environments,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1617–1627, May 2010.

[27] T. Tang, T. Hong, C. Liu, W. Zhao, and M. Kadoch, “Design of 5G dual-antenna passive repeater based on machine learning,” in *2019 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Tangier, Morocco, 2019, pp. 1907–1912.

[28] M. Dong, M. Hajiaghayi, and B. Liang, “Optimal fixed gain linear processing for amplify-and-forward multichannel relaying,” *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 6108–6114, Nov. 2012.

[29] T. Park, G. Lee, W. Saad, and M. Bennis, “Sum rate and reliability analysis for power-domain nonorthogonal multiple access (PD-NOMA),” *IEEE Internet Thing J.*, vol. 8, no. 12, pp. 10 160–10 169, Jun. 2021.

[30] G. Sreya, S. Saigadha, P. D. Mankar, G. Das, and H. S. Dhillon, “Adaptive rate NOMA for cellular IoT networks,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 478–482, Mar. 2022.

[31] T.-H. Vu and S. Kim, “Performance evaluation of power-beacon-assisted wireless-powered NOMA IoT-based systems,” *IEEE Internet Thing J.*, vol. 8, no. 14, pp. 11 655–11 665, Jul. 2021.

[32] T.-H. Vu, T.-V. Nguyen, and S. Kim, “Wireless powered cognitive NOMA-based IoT relay networks: Performance analysis and deep learning evaluation,” *IEEE Internet Thing J.*, vol. 9, no. 5, pp. 3913–3929, Mar. 2022.

[33] H. Lei, C. Zhu, K.-H. Park, W. Lei, I. S. Ansari, and T. A. Tsiftsis, “On secure NOMA-based terrestrial and aerial IoT systems,” *IEEE Internet Thing J.*, vol. 9, no. 7, pp. 5329–5343, Arp. 2022.

[34] Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding, and Y. Song, “Secure transmission in a NOMA-assisted IoT network with diversified communication requirements,” *IEEE Internet Thing J.*, vol. 7, no. 11, pp. 11 157–11 169, Nov. 2020.

[35] Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, “NOMA-assisted secure short-packet communications in IoT,” *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 8–15, Aug. 2020.

[36] Y. Jiang, L. Wang, H. Zhao, and H.-H. Chen, “Covert communications in D2D underlaying cellular networks with power domain NOMA,” *IEEE Syst. J.*, vol. 14, no. 3, pp. 3717–3728, Feb. 2020.

[37] L. Tao, W. Yang, S. Yan, D. Wu, X. Guan, and D. Chen, “Covert communication in downlink NOMA systems with random transmit power,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 2000–2004, Nov. 2020.

[38] Z. Duan, X. Yang, Y. Gong, D. Wang, and L. Wang, “Covert communication in uplink NOMA systems under channel distribution information uncertainty,” *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1282–1286, May 2023.

[39] Q. Li, D. Xu, K. Navaie, and Z. Ding, “Covert and secure communications in NOMA networks with internal eavesdropping,” *IEEE Wireless Commun. Lett.*, Dec. 2023.

[40] B. T. Walkenhorst and M. A. Ingram, “Repeater-assisted capacity enhancement (RACE) for MIMO links in a line-of-sight environment,” in *2009 IEEE Int. Conf. Commun.*, Dresden, Germany, 2009, pp. 1–6.

[41] Y. Ma, D. Zhu, B. Li, and P. Liang, “Channel estimation error and beamforming performance in repeater-enhanced massive MIMO systems,” in *2015 IEEE 26th Annual Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Hong Kong, China, 2015, pp. 672–677.

[42] S. Ahn, S. Kwon, S.-I. Park, J.-y. Lee, N. Hur, and J. Kang, “Outage probability performance of preamble cancellation-assisted RF-watermark TxID detection in repeater networks,” in *2020 IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Paris, France, 2020, pp. 1–4.

[43] S. Ahuja, H. Chhabra, and A. Jain, “Performance enhancement of NOMA for emerging wireless networks using SIC repeaters,” in *2024 Second Int. Conf. Emerg. Trends Inf. Technol. Eng. (ICETITE)*, Vellore, India, 2024, pp. 1–7.

[44] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Elsevier, 2007.