Regular Article

Enhancing Average Secrecy Capacity and Secure Energy Efficiency of SISO System Using RIS with Artificial Jamming over Nakagami-m Fading Channels

Vo Ta Ty[1], **Tran Trung Duy**[2], **Pham Ngoc Son**[1], **Tran Manh Hoang**[3]

[1] Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam
[2] Posts and Telecommunications Institute of Technology, Ha Noi, Vietnam
[3] Faculty of Basic Techniques, Telecommunications University, Khanh Hoa, Vietnam

Correspondence: Pham Ngoc Son, sonpndtvt@hcmute.edu.vn

Communication: received 15 July 2025, revised 22 August 2025, accepted 09 September 2025
Online publication: 13 September 2025, Digital Object Identifier: 10.21553/rev-jec.413

Abstract– **This paper investigates the average secrecy capacity (ASC), secure energy efficiency (SEE) of a single-input single-output (SISO) system assisted by a reconfigurable intelligent surface (RIS) and with/without artificial jamming (AJ). We conduct a detailed ASC and SEE of the proposed system under Nakagami-m fading channels. First, we derive the cumulative distribution functions (CDFs) of the SNRs for jamming and non-jamming schemes. The derived CDFs are then used to obtain closed-form theoretical expressions for ASC and SEE. Moreover, the effect of imperfect successive interference cancellation (SIC) at legitimate receivers has been taken into account to better reflect realistic system implementations. The numerical evaluations confirm that the proposed RIS-Jammer-SISO scheme consistently achieves superior secrecy performance when compared to the RIS-Only configuration. A comprehensive analysis has also been conducted to examine the impact of key system parameters, including the number of reflecting elements, jammer positioning, carrier frequency, and SIC accuracy. Finally, the validity of the analytical results has been corroborated through extensive Monte Carlo simulations.**

Keywords– **Physical layer security, artificial jamming, reconfigurable intelligent surface, average secrecy capacity, secure energy efficiency.**

1 Introduction

1.1 Background

In recent years, the rapid evolution of digital technologies and the growing demand for ubiquitous connectivity have lead to a substantial increase in the number of wireless devices and ecosystems. This trend is especially evident with the widespread deployment of fifth-generation (5G) and beyond 5G (B5G) wireless communication networks [1].

However, the broadcast nature inherent to wireless transmissions renders such systems highly susceptible to various security threats, including confidential data leakage and intentional jamming, particularly in security-critical applications such as smart cities, healthcare systems, military operations, financial services, and environmental monitoring. These concerns are further amplified in emerging wireless scenarios involving sensitive IoT actuators, remote surgery platforms, and the 5G tactile internet.

To address these challenges, physical layer security (PLS) has emerged as a promising paradigm for enhancing the confidentiality of wireless communication systems. Unlike conventional cryptographic approaches, which rely heavily on computational algorithms, PLS leverages the stochastic properties of wireless channels to ensure secure communications, independent of encryption techniques [2]. This method not only improves security performance but also maintains low computational complexity, making it particularly suitable for resource-constrained devices. Owing to these advantages, PLS has garnered significant attention as a pivotal research direction in securing modern wireless networks [3].

Among the advanced techniques proposed to boost PLS performance is the utilization of reconfigurable intelligent surfaces (RIS). RIS comprises metasurfaces capable of dynamically reflecting radio frequency (RF) signals without requiring active signal processing or dedicated power supply [4, 5]. Research has demonstrated that RIS can substantially enhance system performance while reducing deployment and operational costs.

In parallel, artificial jamming (AJ) generation stands out as a key strategy within the PLS framework. This approach involves transmitting controlled jamming signals to degrade the eavesdropper's channel quality, while minimally affecting legitimate users. By exploiting the disparity in channel characteristics between authorized users and potential eavesdroppers, AJ-based techniques effectively impair unauthorized access to information [6]. Notably, by introducing controlled jamming signals to impair the reception quality at eavesdroppers, the secrecy capacity scaling can be improved from $\mathcal{O}(\sqrt{n})$ to $\mathcal{O}(n)$ over n transmitted symbols [7].

Consequently, the integration of RIS and artificial noise for physical layer security has attracted increasing interest from the research community, offering a promising pathway toward robust and energy-efficient secure wireless communications [8].

1.2 Related works

Recent advances in PLS have leveraged RIS to enhance confidentiality in wireless communications. In [9], the authors investigated PLS performance in an IoT network with RIS deployed in the presence of an eavesdropper. The secrecy outage probability (SOP) was derived as the key performance metric, revealing that increasing the number of reflecting elements significantly boosts secrecy performance. In [10], Cao *et al*. proposed a multi-RIS architecture to improve security over Nakagami-m fading channels. They derived a closed-form expression for the average secrecy capacity (ASC) and compared it with systems lacking either a direct transmission path or RIS assistance. In [11], the ASC of a satellite-UAV cooperative relay network with integrated RIS was evaluated under practical deployment conditions, further validating the security benefits of RIS in hybrid wireless environments. Study [12] examined two distinct cases for a RIS-assisted system: (i) the eavesdropper intercepts only the direct signal from the source, and (ii) it intercepts only the reflected signal via RIS. Both ASC and the probability of non-zero secrecy capacity (PNSC) were comprehensively analyzed. In [13], a comparative analysis was conducted between RIS-assisted and relay-assisted non-orthogonal multiple access (NOMA) systems, showing that RIS provides a notable improvement in average secrecy rate (ASR) over conventional relays. Building upon this, [14] derived the effective secrecy capacity (ESC) for RIS-enabled NOMA systems, assessing the achievable secrecy gain in multi-user scenarios.

Despite these significant contributions, works [9–14] primarily focus on RIS-assisted PLS without incorporating artificial jamming (AJ), a known strategy for enhancing secrecy by disrupting the eavesdropper's channel. In contrast, [15] adopted a different approach by combining UAV relays with friendly jamming (FJ) in a NOMA network, albeit without considering RIS. In [16], a RIS-aided system integrating AJ and energy harvesting was proposed to improve security reliability. Similarly, [17] introduced a cooperative framework that combined RIS, relaying, and jamming to enhance PLS. However, neither study accounted for scenarios where both legitimate users and eavesdroppers have access to the direct transmission link, nor did they consider the potential degradation of legitimate users' performance due to jamming. Crucially, a common limitation across studies [9–17] is the lack of evaluation of secrecy energy efficiency (SEE), a vital metric for sustainable wireless communications, especially in dense 5G and B5G networks. Without assessing SEE, these works fall short in analyzing the trade-off between security performance and energy consumption, which is essential for real-world deployment. This gap highlights the need for a new model that simultaneously addresses secrecy enhancement and energy efficiency.

In order to improve the clarity of the discussion, Table I compiles a comparative summary of the most pertinent prior works

Table I
Comparison with the Existing Works

Paper	RIS	AJ	Metrics
[9]	Yes	No	SOP
[10]	Yes	No	ASC
[11]	Yes	No	ASC
[12]	Yes	No	PNSC, ASC
[13]	Yes	No	ASR
[14]	Yes	No	ESC
[15]	No	Yes	ASR
[16]	Yes	Yes	SOP, SC
[17]	Yes	Yes	SIP
This article	Yes	Yes	ASC, SEE

1.3 Motivation and contributions

Thank to conducting an extensive literature review, we identified a significant research gap in the PLS analysis of systems employing RIS and AJ within 5G and B5G networks. To the best of our knowledge, there remains a limited number of studies addressing PLS for wireless networks that integrate RIS and AJ in the presence of eavesdroppers. Motivated by the promising potential of RIS-AJ integration to enhance security performance, this work aims to leverage such synergy for improved confidentiality in wireless communications. Furthermore, the proposed system model takes into account the practical impact of imperfect interference cancellation at legitimate users. The key contributions of this paper are summarized as follows:

- Unlike with [18, 19], which evaluate the secrecy performance of RIS-assisted systems under the assumption that the eavesdropper receives only the direct signal from the transmitter. We introduce an integrated RIS-AJ framework to improve the ASC and SEE of the SISO system under a passive eavesdropping scenario. Additionally, the impact of imperfect jamming suppression at the legitimate user is taken into account to assess the system performance under practical scenarios. Insights into how channel fading severity (m parameter) affects the ASC and SEE in mathematical and numerical results.
- Approximate analytical closed-form expressions for the ASC and SEE have been derived for both jamming-assisted and non-jammer scenarios in general fading channels. Channel and system parameters are selected based on empirical measurements and technical specifications defined in 5G and B5G standards, ensuring high feasibility and practical relevance for future wireless deployments. Although the incorporation of realistic

channel modeling increases the analytical complexity, it enables a more accurate representation of next-generation wireless systems.

- The validity of the analytical findings has been confirmed via extensive Monte Carlo simulations, which demonstrate that the proposed system significantly enhances both ASC and SEE in comparison with its without jamming counterpart, especially when a sufficient number of RIS elements is deployed. Moreover, the effects of critical system parameters, including the jammer's position, carrier frequency, fading parameter and the level of interference cancellation at legitimate users, have been thoroughly examined to provide insightful understanding of the system's behavior under practical conditions. Additionally, the Golden Search algorithm is employed to determine the optimal jamming power P_{J}, thereby enhancing both the ASC and SEE of the system.

The rest of the paper is organized as follows. Section 2 describes the system model. Section 3 presents detailed analysis of the proposed system and comparison system by mathematically deriving the ASC and SEE. Numerical results and discussions are given in Section 4. Finally, Section 5 concludes the paper.

2 System Model

Figure 1 illustrates the system architecture of the proposed single-input single-output (SISO) communication model, in which a RIS and an AJ terminal are incorporated under the presence of a passive eavesdropper. In this setup, the confidential information is transmitted from the source (S) to the legitimate user (D) via two transmission paths: a direct link (S–D) and an indirect reflected link through the RIS (S–RIS–D). Similar to D, the eavesdropper (E) is assumed to receive both the direct signal and the reflected signal from the RIS. To further strengthen physical layer security, an AJ has been incorporated into the system. Artificial interference is emitted by the jammer to intentionally disrupt the reception capability of the eavesdropper. Importantly, the potential degradation experienced by the legitimate user due to jamming interference has also been considered, as such effects are likely in practical implementations. In this study, the channel state information (CSI) of the source node S is assumed to be perfectly available at the RIS to facilitate the maximization of the received SNR at the D. It is worth noting that various channel estimation techniques for RIS, as introduced in [20, 21], can be employed to acquire the required CSI. Additionally, all communication entities, including S, D, E, and J, are assumed to be equipped with a single antenna.

The received signal at D, accounting for both the direct transmission and RIS reflection, is formulated as

$$y_{\mathrm{D}} = \left(h_{\mathrm{SD}} + \sum_{t=1}^{L} h_{\mathrm{SR}_t} h_{\mathrm{R}_t\mathrm{D}} e^{j\Psi_t}\right)\sqrt{P_{\mathrm{S}}}\,x_{\mathrm{S}} + \sqrt{\Delta P_{\mathrm{J}}}\; h_{\mathrm{JD}} x_{\mathrm{J}} + z_{\mathrm{D}}, \tag{1}$$

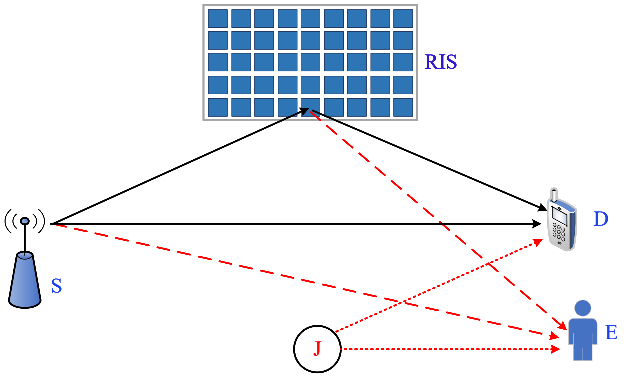

Figure 1. System model of the proposed RIS-Jammer-SISO communication system in the presence of an eavesdropper.

where h_{SD}, h_{SR_t}, $h_{\mathrm{R}_t\mathrm{D}}$ and h_{JD} are the channel coefficients from S to D, S to the t^{th} element of RIS, from the t^{th} element of RIS to D and from J to D, respectively; ψ_t is the adjustable phase shift caused by the t^{th} element of the RIS; Δ represents the ability to eliminate jamming signals from D, $0 \leq \Delta \leq 1$ (see Remark 1); z_{D} is the additive white Gaussian noise (AWGN) at D with zero mean and variance of δ_{D}^2, i.e., $z_{\mathrm{D}} \sim CN(0, \delta_{\mathrm{D}}^2)$. The transmitted signal from the source node S is denoted by x_{S}, with an associated transmit power of P_{S}. The jamming node J transmits the signal x_{J}, corresponding to a transmit power of P_{J}. As the channel coefficients are complex-valued, they can be expressed in terms of their amplitude and phase components as follows: $h_{\mathrm{SD}} = a_{\mathrm{SD}} e^{-j\Psi_{\mathrm{SD}}}$, $h_{\mathrm{SR}_t} = a_{\mathrm{SR}_t} e^{-j\Psi_{\mathrm{SR}_t}}$, $h_{\mathrm{R}_t\mathrm{D}} = a_{\mathrm{R}_t\mathrm{D}} e^{-j\Psi_{\mathrm{R}_t\mathrm{D}}}$, $h_{\mathrm{JD}} = a_{\mathrm{JD}} e^{-j\Psi_{\mathrm{JD}}}$ where $(a_{\mathrm{SD}}, \Psi_{\mathrm{SD}})$, $(a_{\mathrm{SR}_t}, \Psi_{\mathrm{SR}_t})$, $(a_{\mathrm{R}_t\mathrm{D}}, \Psi_{\mathrm{R}_t\mathrm{D}})$ and $(a_{\mathrm{JD}}, \Psi_{\mathrm{JD}})$ are magnitude–phase shift pairs of h_{SD}, h_{SR_t}, $h_{\mathrm{R}_t\mathrm{D}}$ and h_{JD}, respectively.

Remark 1: To estimate or set Δ in practice, it can be determined based on the residual interference power after cancellation. Specifically, in [22], a cooperative jamming cancellation architecture was proposed and a testbed was implemented to verify its feasibility. Experimental results in a laboratory environment under line-of-sight (LoS) conditions demonstrate that the proposed architecture can achieve approximately 51 dB of interference suppression, while the noise floor is increased by about 5 dB (with a noise floor of −95 dBm, the residual interference after cancellation is approximately −90 dBm) due to imperfect time–frequency synchronization and channel estimation. In practical scenarios, due to various non-ideal factors, the value of Δ may vary within a certain range. For example, in [15], Δ was observed to lie approximately between 0.01 and 0.1. These observations provide a useful guideline for selecting Δ to realistically reflect the interference cancellation capability in actual systems.

The optimization of phase shifts to maximize the SINR at D follows the approach proposed in [23] (see Remark 2).

$$\Psi_t = \Psi_{\mathrm{SR}_t} + \Psi_{\mathrm{R}_t\mathrm{D}} - \Psi_{\mathrm{SD}}. \tag{2}$$

Since the phase shifts perfectly aligned, we can rewritten (1) as

$$y_{\mathrm{D}} = e^{-j\Psi_{\mathrm{SD}}}\big(a_{\mathrm{SD}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}\big)\sqrt{P_{\mathrm{S}}}x + a_{\mathrm{JD}} e^{-j\Psi_{\mathrm{JD}}}\sqrt{\Delta P_{\mathrm{J}}} + z_{\mathrm{D}}. \quad (3)$$

From (3), the SINR at D is formulated as follows

$$\gamma_{\mathrm{D}} = \frac{|e^{-j\Psi_{\mathrm{SD}}}|^2\big(a_{\mathrm{SD}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}\big)^2 P_{\mathrm{S}}}{|e^{-j\Psi_{\mathrm{JD}}}|^2 a_{\mathrm{JD}}^2 \Delta P_{\mathrm{J}} + \delta_{\mathrm{D}}^2}. \quad (4)$$

Since $|e^{-j\Psi_{\mathrm{SD}}}|^2 = |e^{-j\Psi_{\mathrm{JD}}}|^2 = 1$, formula (4) simplifies to

$$\gamma_{\mathrm{D}} = \frac{\big(a_{\mathrm{SD}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}\big)^2 P_{\mathrm{S}}}{a_{\mathrm{JD}}^2 \Delta P_{\mathrm{J}} + \delta_{\mathrm{D}}^2}. \quad (5)$$

The received signal at E from both the direct and RIS-assisted links can be expressed as

$$y_{\mathrm{E}} = \big(h_{\mathrm{SE}} + \sum_{t=1}^{L} h_{\mathrm{SR}_t} h_{\mathrm{R}_t\mathrm{E}} e^{j\Psi_t}\big)\sqrt{P_{\mathrm{S}}}x + \sqrt{P_{\mathrm{J}}}\, h_{\mathrm{JE}} x_{\mathrm{J}} + z_{\mathrm{E}}, \quad (6)$$

where h_{SE}, $h_{\mathrm{R}_t\mathrm{E}}$ and h_{JE} are the channel coefficients from S to E, from the t^{th} element of RIS to E and from J to E, respectively. z_{E} represents the additive white Gaussian noise (AWGN) at E with zero mean and variance δ_{E}^2, i.e., $z_{\mathrm{E}} \sim CN(0, \delta_{\mathrm{E}}^2)$.

The channel coefficients, being complex-valued, can be formulated in terms of their magnitudes and phases as follows: $h_{\mathrm{SE}} = a_{\mathrm{SE}} e^{-j\Psi_{\mathrm{SE}}}$, $h_{\mathrm{R}_t\mathrm{E}} = a_{\mathrm{R}_t\mathrm{E}} e^{-j\Psi_{\mathrm{R}_t\mathrm{E}}}$, $h_{\mathrm{JE}} = a_{\mathrm{JE}} e^{-j\Psi_{\mathrm{JE}}}$ where (a_{SE}, Ψ_{SE}), ($a_{\mathrm{R}_t\mathrm{E}}$, $\Psi_{\mathrm{R}_t\mathrm{E}}$) and ($a_{\mathrm{JE}}$, Ψ_{JE}) are magnitude-phase shift pairs of h_{SE}, $h_{\mathrm{R}_t\mathrm{E}}$ and h_{JE}, respectively.

From (6), the SINR at E can be formulated as (see Remark 3)

$$\gamma_{\mathrm{E}} = \frac{|e^{-j\Psi_{\mathrm{SE}}}|^2\big(a_{\mathrm{SE}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{E}}\big)^2 P_{\mathrm{S}}}{|e^{-j\Psi_{\mathrm{JE}}}|^2 a_{\mathrm{JE}}^2 P_{\mathrm{J}} + \delta_{\mathrm{E}}^2}. \quad (7)$$

Since $|e^{-j\Psi_{\mathrm{SE}}}|^2 = |e^{-j\Psi_{\mathrm{JE}}}|^2 = 1$, formula (7) is simplified to

$$\gamma_{\mathrm{E}} = \frac{\big(a_{\mathrm{SE}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{E}}\big)^2 P_{\mathrm{S}}}{a_{\mathrm{JE}}^2 P_{\mathrm{J}} + \delta_{\mathrm{E}}^2}. \quad (8)$$

In addition, we analyze the secrecy performance of the proposed systems over Nakagami-m fading channels. Accordingly, the CDF and PDF of the channel magnitudes $\mathcal{X} \in \{a_{\mathrm{SD}}, a_{\mathrm{SE}}, a_{\mathrm{SR}_t}, a_{\mathrm{R}_t\mathrm{D}}, a_{\mathrm{R}_t\mathrm{E}}, a_{\mathrm{JD}}, a_{\mathrm{JE}}\}$, are expressed as follows [24]:

$$F_{\mathcal{X}}(y) = \frac{1}{\Gamma(m_{\mathcal{X}})}\gamma(m_{\mathcal{X}}, \frac{m_{\mathcal{X}}}{\Omega_{\mathcal{X}}}y^2) = 1 - \frac{1}{\Gamma(m_h)}\Gamma\left(m_h, \frac{m_h y^2}{\Omega_h}\right), \quad y \geq 0 \quad (9)$$

$$f_{\mathcal{X}}(y) = \frac{2m_{\mathcal{X}}^{m_{\mathcal{X}}} y^{2m_{\mathcal{X}}-1}}{\Gamma(m_{\mathcal{X}})\Omega_{\mathcal{X}}^{m_{\mathcal{X}}}}\exp\left(-\frac{m_{\mathcal{X}} y^2}{\Omega_{\mathcal{X}}}\right), \quad y \geq 0 \quad (10)$$

where, $\Omega_{\mathcal{X}}$ and $m_{\mathcal{X}}$ denote the spread and shape parameters, respectively.

Remark 2: To acquire perfect channel state information (CSI), two common approaches are typically employed in RIS-assisted communication systems based on training signals: with and without radio frequency (RF) chains [4, 21]. When RF chains are adopted, the estimation of the S–RIS and RIS–user channels can be independently carried out at the RIS. In contrast, in scenarios without RF chains, the estimation process focuses on the cascaded S–RIS–user channels [20, 21]. With the rapid advancement of computing hardware and software, particularly in deep learning and optimization algorithms, channel estimation in RIS-assisted wireless networks can be effectively realized [20]. These methods facilitate the acquisition of perfect CSI in the proposed SISO-RIS system. It should also be noted that the assumption of perfect CSI has been widely adopted in prior works [25, 26]. On the other hand, one of the key advantages of RIS lies in its ability to adapt the phase configuration Ψ_t to maximize the received power at the intended receivers. Specifically, the number of feasible phase states for RIS is limited due to the discrete nature of phase shifts. Hence, by employing high-resolution phase settings and intelligent controllers at the RIS, optimal phase configurations can be achieved under the perfect CSI assumption such that Ψ_t = 0 or $\Psi_{\mathrm{SR}_t} + \Psi_{\mathrm{R}_t\mathrm{D}} - \Psi_{\mathrm{SD}}$ = 0 [10, 16].

Remark 3: In studies on RIS-assisted wireless communications, when the RIS phases are configured to maximize the SINR of a specific user, the SINR experienced by other users is generally not maximized [27]. Nevertheless, many works adopt the simplifying assumption that the maximum SINR can be simultaneously achieved for all users [28]. This assumption has been extensively applied not only to legitimate users but also to eavesdroppers [10, 16, 26, 29]. In practical scenarios, the distance between the RIS and the user/eavesdropper is typically much larger than that between the user and the eavesdropper. As a result, the angular difference observed at the RIS with respect to the user and eavesdropper is negligible and can be ignored. This geometric assumption has also been widely employed in prior studies. Following this line of research, we consider in this paper the case where the received signal at the E can also be maximized. In other words, we focus on a worst-case security scenario in which the eavesdropper attains its maximum SINR. Such a worst-case assumption is widely used in physical layer security analysis, as it provides a worst-case reference that guarantees robustness of the proposed scheme even under highly adverse conditions.

3 Secrecy performance analysis

This section we shown the analytical derivation of closed-form expressions for both ASC and SEE within the proposed framework. To provide a comparative performance baseline, we further investigate these metrics for a system configuration that excludes artificial jamming.

3.1 Average Secrecy Capacity

For the proposed system, the ASC can be mathematically formulated as follows [10]

$$\mathrm{ASC} = \Big[\mathbb{E}\Big\{ \log_2(1+\gamma_\mathrm{D}) - \log_2(1+\gamma_\mathrm{E})\Big\}\Big]^+, \quad (11)$$

with γ_D defined in Equation (5) and γ_E defined in Equation (7), $[x]^+ = \max\{x, 0\}$.

$$\begin{aligned}\mathrm{ASC} &= \Big[\mathbb{E}\{\log_2(1+\gamma_\mathrm{D})\} - \mathbb{E}\{\log_2(1+\gamma_\mathrm{E})\}\Big]^+ \\ &= \Big[\mathbb{E}\{\mathrm{C_D}\} - \mathbb{E}\{\mathrm{C_E}\}\Big]^+, \quad (12)\end{aligned}$$

where $\mathbb{E}\{\mathrm{C_D}\}$ and $\mathbb{E}\{\mathrm{C_E}\}$ are

$$\mathbb{E}\{\mathrm{C_D}\} = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_{\gamma_\mathrm{D}}(x)}{1+x}dx, \quad (13)$$

$$\mathbb{E}\{\mathrm{C_E}\} = \frac{1}{\ln 2}\int_0^\infty \frac{1-F_{\gamma_{\mathrm{E}_\mathrm{max}}}(x)}{1+x}dx. \quad (14)$$

It is worth noting that γ_D and γ_E are not independent due to a_{SR_t}; nevertheless, Equation (12) remains valid owing to the properties of expectation [30, Equation (6.162)]. Consequently, Equation (12) has been extensively applied in the computation of the ASC for RIS-assisted wireless systems [5, 9, 10, 31].

Theorem 1. The ASC of the considered system, operating in the presence of an eavesdropper and subject to Nakagami-*m* fading channels, is mathematically expressed as follows

$$\begin{aligned}\mathrm{ASC} \approx{}& \frac{1}{\ln 2}\sum_{n=1}^{N}\sum_{m=1}^{M}\varepsilon_n\varepsilon_m\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{\mathrm{A_D}}{P_\mathrm{S}}\frac{1-v_m}{1+v_m}}\,\Big) \\ &- \frac{1}{\ln 2}\sum_{w=1}^{W}\sum_{q=1}^{Q}\varepsilon_w\varepsilon_q\Gamma\Big(\omega_2, \phi_2\sqrt{\frac{\mathrm{A_E}}{P_\mathrm{S}}\frac{1-v_q}{1+v_q}}\,\Big), \quad (15)\end{aligned}$$

where $\mathrm{A_D} = \Delta P_\mathrm{J}\dfrac{1}{\alpha_\mathrm{JD}}\ln\dfrac{2}{v_n+1} + \delta_\mathrm{D}^2$,

$\mathrm{A_E} = P_\mathrm{J}\,\dfrac{1}{\alpha_\mathrm{JE}}\ln\dfrac{2}{v_w+1} + \delta_\mathrm{E}^2$,

$\xi_n = \dfrac{1}{\Gamma(\omega_1)\Gamma(m_\mathrm{JD})}\Big(\ln\dfrac{2}{v_n+1}\Big)^{m_\mathrm{JD}-1}\dfrac{\pi}{2N}\sqrt{1-v_n^2}$,

$\varepsilon_m = \dfrac{\pi\sqrt{1-v_m^2}}{2M}\dfrac{2}{1+v_m}$, $\varepsilon_q = \dfrac{\pi\sqrt{1-v_q^2}}{2Q}\dfrac{2}{1+v_q}$,

$\xi_w = \dfrac{1}{\Gamma(\omega_2)\Gamma(m_\mathrm{JE})}\Big(\ln\dfrac{2}{v_w+1}\Big)^{m_\mathrm{JE}-1}\dfrac{\pi}{2W}\sqrt{1-v_w^2}$.

From equation (15), it can be observed that the ASC is influenced by several key parameters, including the source power P_S, jamming power P_J, the number of REs L, the locations of devices, carrier frequencies, and the interference cancellation capabilities at the legitimate user.

Proof : Further analytical derivations can be found in Appendix A.

3.2 The ASC of the Non-Jammer System

To ensure a fair comparison between the proposed system and the non-jammer system, the transmit power for the without jamming system is set as $P_\mathrm{S}^\mathrm{NJ} = P_\mathrm{S} + P_\mathrm{J} = (1+\mu)P_\mathrm{S}$, where μP_S $(0 < \mu < 1\ )$ corresponds to the jamming power in the proposed scheme.

Following a similar approach to that in (12), the ASC of the non-jammer system is analytically characterized in the following theorem.

Theorem 2. The ASC corresponding to the proposed system in the absence of jamming are expressed as follows

$$\begin{aligned}\mathrm{ASC^{NJ}} \approx{}& \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_1)}\varepsilon_{k_1}\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{\delta_\mathrm{D}^2}{P_\mathrm{S}^\mathrm{NJ}}\frac{1-v_{k_1}}{1+v_{k_1}}}\,\Big) \\ &- \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_2)}\varepsilon_{k_2}\Gamma\Big(\omega_2, \phi_2\sqrt{\frac{\delta_\mathrm{D}^2}{P_\mathrm{S}^\mathrm{NJ}}\frac{1-v_{k_2}}{1+v_{k_2}}}\,\Big), \quad (16)\end{aligned}$$

where $\varepsilon_{k_1} = \dfrac{\pi\sqrt{1-v_{k_1}^2}}{2K_1}\dfrac{2}{1+v_{k_1}}$,

$\varepsilon_{k_2} = \dfrac{\pi\sqrt{1-v_{k_2}^2}}{2K_2}\dfrac{2}{1+v_{k_2}}$.

Proof : Refer to Appendix B for further details.

3.3 Secure energy efficiency

SEE is a metric in wireless communications. It simultaneously addresses the demands for enhanced security and efficient energy utilization. Therefore, SEE has become a fundamental criterion in the design and performance assessment of modern communication systems. Mathematically, the SEE of the proposed system is defined as follows [32]

$$\eta = \frac{R_\mathrm{sec}}{P_i}, \quad (17)$$

here, R_sec denotes the secure transmission rate of the system, while $P_i \in \{P_\mathrm{tol}, P_\mathrm{tol}^\mathrm{NJ}\}$ represents the total power consumption. The secure rate for both the proposed system and its non-jammer counterpart is obtained from (15) and (16). On the other hand, the total power for the proposed and non-jammer systems are adopted from [23, 32]

$$P_\mathrm{tol} = P_\mathrm{S} + P_\mathrm{J} + L\tilde{P}_t + \tilde{P}_\mathrm{S} + \tilde{P}_\mathrm{J} + \tilde{P}_\mathrm{D} + \tilde{P}_\mathrm{E}, \quad (18)$$

$$P_\mathrm{tol}^\mathrm{NJ} = (1+\mu)P_\mathrm{S} + L\tilde{P}_t + \tilde{P}_\mathrm{S} + \tilde{P}_\mathrm{D} + \tilde{P}_\mathrm{E}, \quad (19)$$

where $\tilde{P}_t$, $\tilde{P}_\mathrm{S}$, $\tilde{P}_\mathrm{J}$, $\tilde{P}_\mathrm{D}$ and $\tilde{P}_\mathrm{E}$ denote the circuit power consumption associated with the t^{th} reflecting element of the RIS and nodes S, J, D, and E, respectively.

4 Numerical results

Based on the ASC and SEE expressions derived in the previous section, the operational characteristics of the proposed system are thoroughly analyzed in this section. Monte Carlo simulations are carried out to verify the accuracy of the theoretical formulas obtained.

Additionally, to clearly demonstrate the advantages of employing RIS and AJ in enhancing secrecy performance, the ASC and SEE values of a benchmark system without jamming (denoted as "Non-Jammer") are also simulated for comparison. In the simulation setup, a two-dimensional Cartesian coordinate system is employed for the RIS- and AJ-assisted communication system. Unless otherwise specified, the system parameters are configured as follows. The source node S is placed at the origin (0, 0) meters, while the RIS is located at (70, 5) meters. The legitimate destination nodes D is positioned at (90, 0) meters. The eavesdropper E and J are situated at coordinates (150, -5) meters and (130, -5) meters, respectively. The circuit power dissipation at the t^{th} RE of the RIS is assumed to be $\tilde{P}_t$ = 7 dBm. For all remaining nodes, including S, J, D, and E, the circuit power consumption is uniformly set to $\tilde{P}_S = \tilde{P}_J = \tilde{P}_D = \tilde{P}_E$ = 10 dBm, as specified in [23]; the antenna gains $G_S = G_{RIS} = G_D = 5$ dB, and $G_E = 0$ dB [24]. In all considered scenarios, Δ = 0.05 and N = 90. The transmit powers of nodes S and J are constrained by the relationship $P_J = \mu P_S$, where μ is a positive constant such that $0 < \mu < 1$. For performance benchmarking, the transmit power of the source in the system without the jammer is adjusted as $P_S^{NJ} = P_S + P_J = (1 + \mu) P_S$. Unless otherwise specified, the value of μ is fixed at 0.003 for all simulations. The shape parameters of all considered channel magnitude distributions are assumed to be identical, denoted as $m_{\mathcal{X}}$ = 2, $\mathcal{X} \in \{a_{SD}, a_{SE}, a_{SR_t}, a_{R_tD}, a_{R_tE}, a_{JD}, a_{JE}\}$. Meanwhile, the noise power at the receivers is determined based on the system bandwidth BW (in Hz), the receiver noise figure NF (in dBm), and the thermal noise power density N_0 (in dBm/Hz), as expressed in [24] by

$$\delta_D^2 = \delta_E^2 = 10\log(\text{BW}) + \text{NF} + N_0, \tag{20}$$

where BW = 10 MHz, N_0 = -174 dBm/Hz, and NF = 10 dB. Furthermore, the proposed systems adopt the channel model recommended in 5G/B5G standards. Accordingly, the value of $\Omega_{\mathcal{X}}$ under the non-line-of-sight (NLoS) condition is determined as in [24, 33]

$$\Omega_{\mathcal{X}} = G_{tx} - 22.7 - 26\log(f_c) - 36.7\log(d) + G_{rx}, \tag{21}$$

here, G_{tx} and G_{rx} denote the antenna gains of the transmitter and receiver, respectively; f_c represents the carrier frequency ($2 \leq f_c \leq 6$ GHz); and d is the distance between the transmitter and receiver.

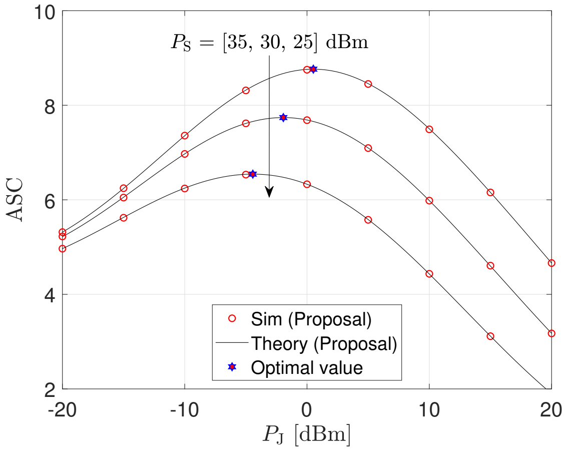

Figure 2. The ASC of the considered system versus the P_J for P_S = 25, 30, 35 dBm, f_c = 3 GHz and L = 40.

Figure 2 illustrates the impact of P_J on the ASC of the proposed system, with P_S = 25, 30, 35 dBm, f_c = 3 GHz and L = 40. It is observed that as P_J increases from –20 dBm to 20 dBm, the ASC initially rises, reaching a peak at a specific value of P_J, and subsequently decreases. This behavior can be explained as follows. When P_J increases, the eavesdropper's channel capacity is reduced due to elevated interference, as indicated by formula (8), thereby enhancing the ASC. However, according to formula (5), the legitimate user's capacity is also degraded due to the same interference. Consequently, once the eavesdropper's capacity becomes saturated, any further increase in P_J results in a decline in the legitimate user's capacity, leading to a reduction in the ASC. Furthermore, Figure 2 demonstrates that each curve exhibits a distinct peak, indicating the existence of an optimal jamming power P_J that maximizes the average secrecy capacity ASC. It is important to note that a closed-form expression for the optimal P_J is intractable. Consequently, the Golden Search algorithm [34, 35] is employed to numerically determine the optimal P_J through iterative computations, with the results summarized in Table II. The optimal values obtained via the Golden Search method demonstrate a perfect match with those derived from theoretical analysis. Therefore, an optimal value of P_J should be selected in system design to strike a balance between maximizing ASC and maintaining energy efficiency, especially in the context of 5G and B5G networks. Specifically, for P_S values of 25, 30, and 35 dBm, the ASC achieves its maximum at P_J = -4, -2, and 0.5 dBm, respectively.

Table II
Optimization Algorithm to find P_J^*

```
Input: Establish $P_{J_{min}}$ = -20 dBm, $P_{J_{max}}$ = 20 dBm, the golden section search $\omega = \frac{\sqrt{5}-1}{2}$, and a stopping threshold $\delta = 10^{-3}$.
Output: The optimal $P_J^*$ that maximizes ASC.
Begin:
1. Build sets $\epsilon_1 = P_{J_{min}} + (P_{J_{max}} - P_{J_{min}})\omega$ and
      $\epsilon_2 = P_{J_{max}} - (P_{J_{max}} - P_{J_{min}})\omega$.
2. While $P_{J_{max}} - P_{J_{min}} \geq \delta$ do
      Update: ASC($\epsilon_1$).
      Update: ASC($\epsilon_2$).
      If ASC($\epsilon_2$) > ASC($\epsilon_1$) then
         Update: $P_{J_{min}} \leftarrow \epsilon_1$.
      Else
         Update: $P_{J_{max}} \leftarrow \epsilon_2$.
      End If.
3. End While.
4. Return $P_J^* = \frac{P_{J_{max}} + P_{J_{min}}}{2}$.
End.
```

Figure 3 demonstrates the ASC of the proposed system and the system without jamming, corresponding to different numbers of L = 10, 30, 50 and f_c = 2 GHz. The analytical ASC curves are obtained from expressions

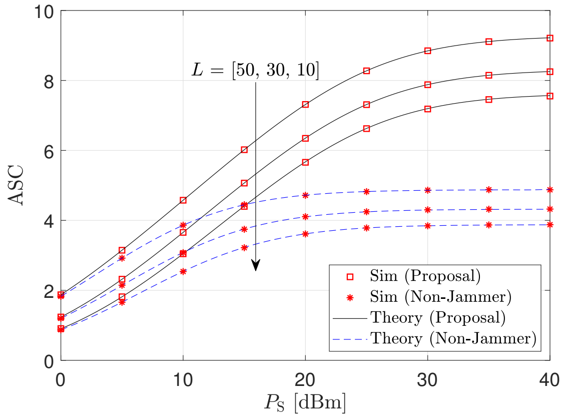

Figure 3. The ASC of the considered system versus the P_S for L = 10, 30, 50 and f_c = 2 GHz.

(15) and (16). As observed, a close match between analytical and simulation results is achieved, confirming the accuracy of the derived expressions. The results in Figure 3 demonstrate that the proposed system significantly outperforms the non-jammer counterpart in terms of secrecy performance. Additionally, it is observed that the ASC of the system without jamming saturates when $P_S > 20$ dBm, whereas saturation in the proposed system occurs only when $P_S > 40$ dBm. Moreover, the parameter L exerts a substantial influence on the ASC in both scenarios. To achieve an ASC of 6 bps/Hz, a transmit power of 21.5 dBm is required at the source when L = 10, while only 15 dBm is needed when L = 50. These findings confirm that increasing the number of L, combined with an effective jamming strategy, substantially enhances secrecy performance while reducing the required transmit power.

Figure 4 analyzes the impact of carrier frequency on the ASC for both the proposed system and the counterpart without jamming, considering L = 40. It is observed that the secrecy performance of the proposed system significantly deteriorates as the carrier frequency increases. Specifically, to achieve an ASC of 7 bps/Hz, a transmit power of P_S = 38 dBm is required at f_c = 6 GHz, whereas only P_S = 21 dBm is needed at f_c = 2 GHz. Furthermore, it can be clearly seen that throughout the entire examined frequency range, the proposed system consistently maintains a considerably higher level of secrecy compared to the system without jamming, thereby validating the effectiveness of the adopted jamming technique.

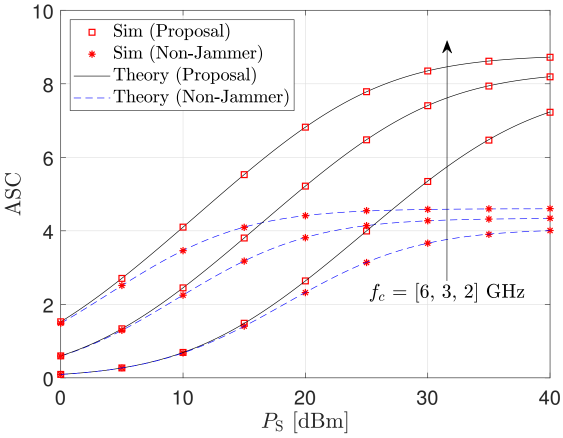

Figure 4. The ASC of the considered system versus the P_S for f_c = 2, 3, 6 GHz and L = 40.

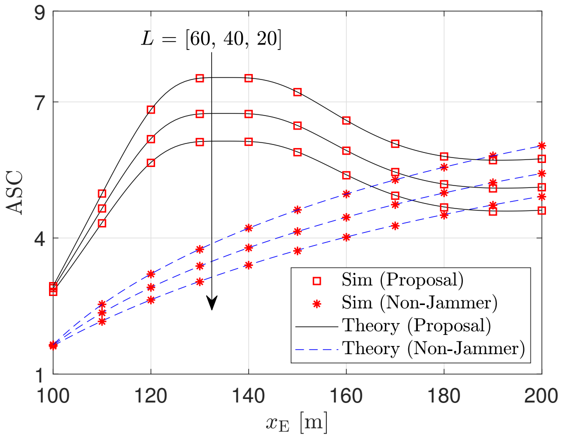

Figure 5. The ASC of the considered system versus the x_E for P_S = 25 dBm, f_c = 3 GHz and L = 20, 40, 60.

Figure 5 shows the impact of the eavesdropper's position on the ASC of the proposed system under various values of L. It is observed that as the position of the eavesdropper x_E increases from 110 m to 135 m, the ASC of the proposed system gradually improves and reaches its maximum at x_E = 135 m. Following this position, as x_E continues to increase toward 180 m, the ASC is reduced and eventually saturates. This behavior can be attributed to the fixed location of the jamming device at 135 m, whereby the received signal at the eavesdropper is most severely degraded when x_E = 135 m, thus maximizing the secrecy performance. In contrast, for the system without jamming, the ASC increases monotonically with x_E across the range from 110 m to 200 m. However, throughout the entire examined region, the proposed system consistently outperforms the non-jamming counterpart, highlighting the effectiveness of the adopted jamming strategy. Moreover, increasing the number of REs L further enhances the secrecy capacity in both configurations, with more pronounced improvements observed in the RIS-AJ-assisted system.

Figure 6 illustrates the impact of interference cancellation effectiveness on legitimate users under two conditions: ideal ($\Delta = 0$) and non-ideal ($\Delta = 0.05$). It is observed that when the transmit power P_S varies from 0 to 20 dBm, the difference in average secrecy capacity (ASC) between the two scenarios remains negligible. However, as P_S increases from 20 to 40 dBm, the ideal interference cancellation case yields a significantly higher ASC compared to the non-ideal scenario with $\Delta = 0.05$. This behavior can be explained by the proportional relationship between the jamming power and the transmit power, expressed as $P_J = \mu P_S$. As P_S increases, the corresponding rise in P_J results in a degradation of the channel capacity at the legitimate destination D, as described in (5). These findings high-

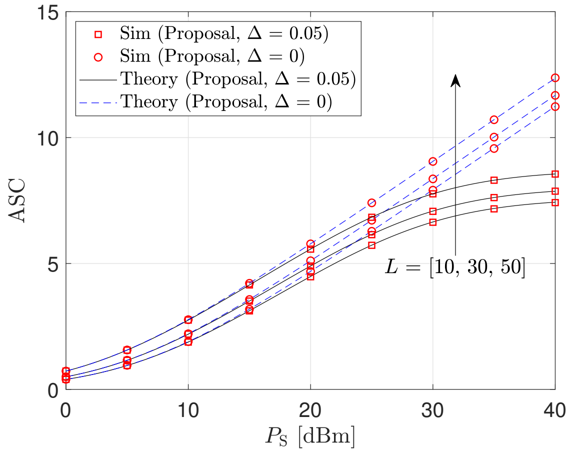

Figure 6. The impact of Δ on ASC of the considered system with L = 10, 30, 50 and f_c = 3 GHz.

light the crucial role of interference cancellation effectiveness in enhancing the secrecy performance of the system. Therefore, optimizing interference cancellation techniques is essential to improve secure communication for legitimate users.

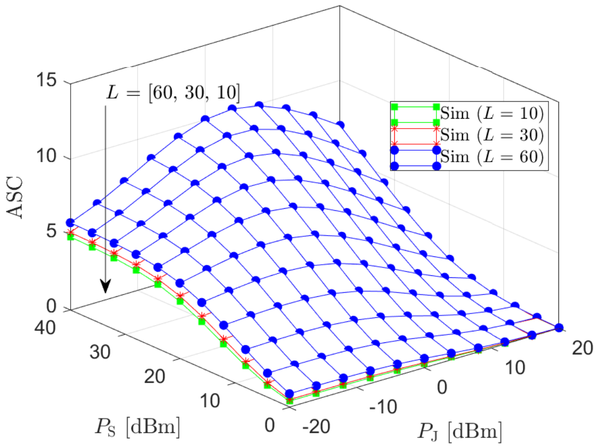

Figure 7. The impact of P_S and P_J on ASC with L = 10, 30, 60 and f_c = 3 GHz.

Figure 7 depicts the impact of the transmit power P_S and the jamming power P_J on the ASC of the system for L = 10, 30, and 60. As shown in Figure 7, when P_S increases from 0 to 40 dBm, the ASC initially increases, reaches its peak, and then saturates, consistent with the trend observed in Figure 2. Similarly, as P_J increases from –20 to 20 dBm, the ASC rises gradually, attains a maximum value, and subsequently decreases. This behavior can be explained as follows: the increase in P_J initially leads to a reduction in the channel capacity at the eavesdropper E. However, once ASC saturation is reached, further increases in P_J no longer affect E significantly. At this stage, the negative impact of P_J on the legitimate destination D becomes more pronounced, ultimately causing a decline in ASC. Additionally, an increase in the number of REs L is observed to significantly enhance the ASC, further demonstrating the benefits of RIS deployment.

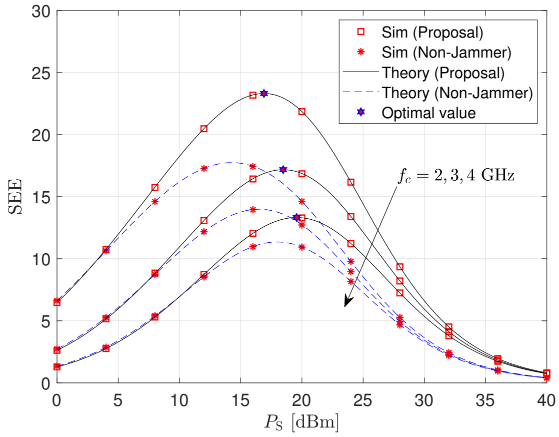

Figure 8. The SEE of the considered system versus the P_S for f_c = 2, 3, 4 and L = 30.

Figure 8 represents the SEE (bit/J) of the proposed system and the non-jammer system as a function of P_S, with f_c = 2, 3, 4 GHz. In this figure, the analytical curves are plotted based on equation (17). The results in Figure 8 reveal that when P_S $<$ 10 dBm, the SEE values of both systems are nearly identical. However, for P_S $>$ 10 dBm, the proposed system achieves a significantly higher SEE compared to the non-jammer counterpart. Importantly, for each value of f_c, there exists an optimal transmit power P_S at which SEE is maximized. Specifically, the optimal P_S values corresponding to the maximum SEE are 17, 18.7, and 20 dBm for f_c = 2, 3, and 4 GHz, respectively. This highlights that selecting an appropriate transmit power is critical to simultaneously optimizing both ASC and SEE in system design. Furthermore, it is observed that the SEE of both systems decreases as f_c increases, which can be explained by the same rationale discussed in Figure 4. Following the procedure outlined in Table II, each value of f_c corresponds to an optimal P_S that maximizes the SEE. For instance, when f_c = 2, 3, and 4, the maximum SEE is attained at P_S = 16.9, 18.5, and 19.6 dBm, respectively.

Figure 9 illustrates the SEE of the proposed system and the non-jammer system as a function of transmit power P_S, for different values of the shape parameter

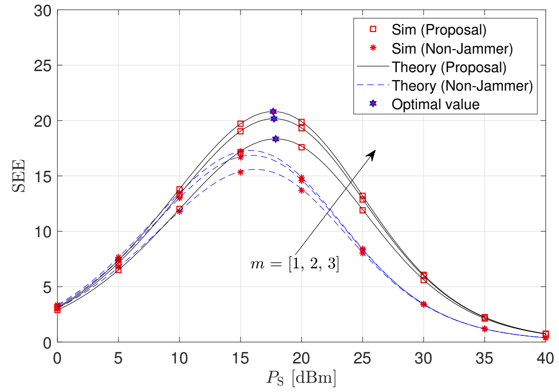

Figure 9. The SEE of the considered system versus the P_S for m = 1, 2, 3 and L = 20.

m, with L = 20. The results in Figure 9 indicate that the shape parameter has a significant impact on the SEE performance of both systems. In addition, for each value of m, an optimal transmit power P_{S} can be identified at which the SEE reaches its maximum. Moreover, it is observed that the proposed system consistently achieves higher SEE values compared to the non-jammer system, demonstrating the effectiveness of the jamming technique in enhancing SEE communication. Similar to Figure 2 and Figure 8, for each value of m, there exists an optimal transmit power P_{S} at which the SEE metric reaches its maximum.

5 Conclusion

Enhancing the secrecy performance of wireless communication systems has become an essential requirement due to the inherent physical limitations of the wireless propagation environment. In this paper, RIS in conjunction with AJ have been employed to strengthen the physical layer security of wireless systems in the presence of an eavesdropper. Approximate analytical expressions for the ASC and SEE have been successfully derived for both the proposed system and the baseline system without jamming. Simulation results have demonstrated that the integration of RIS and AJ significantly outperforms the configuration without jamming in terms of both ASC and SEE. Furthermore, the impact of key system parameters, such as carrier frequency, fading parameter, and distances between critical entities (i.e., transmitter–eavesdropper and transmitter–jammer), as well as the interference cancellation capability at the legitimate user, has been thoroughly investigated to gain deeper insights into system behavior under practical conditions. Based on the obtained findings, several effective strategies have been recommended to optimize the secrecy performance of the proposed system across various deployment scenarios.

Appendix A

The appendix details the step-by-step derivation of the ASC for the proposed systems.

From (5) and (8), let $\mathcal{X}_1 = a_{\mathrm{SD}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}$, $\mathcal{X}_2 = a_{\mathrm{SE}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{E}}$, we have

$$\gamma_{\mathrm{D}} = \frac{{\mathcal{X}_1}^2 P_{\mathrm{S}}}{\Delta P_{\mathrm{J}}\ {a_{\mathrm{JD}}}^2 + \delta_{\mathrm{D}}^2}, \tag{22}$$

$$\gamma_{\mathrm{E}} = \frac{\mathcal{X}_2^2 P_{\mathrm{S}}}{P_{\mathrm{J}}\ {a_{\mathrm{JE}}}^2 + \delta_{\mathrm{E}}^2}. \tag{23}$$

Based on (22), the CDF of γ_{D} is derived as

$$\begin{aligned} F_{\gamma_{\mathrm{D}}}(x) &= \Pr\{\gamma_{\mathrm{D}} < x\} = \Pr\{\frac{\mathcal{X}_1^2 P_{\mathrm{S}}}{\Delta_1 P_{\mathrm{J}}\ {a_{\mathrm{JD}}}^2 + \delta_{\mathrm{D}}^2} < x\} \\ &= \Pr\Big\{\mathcal{X}_1^2 < \frac{x(\Delta P_{\mathrm{J}}\ {a_{\mathrm{JD}}}^2 + \delta_{\mathrm{D}}^2)}{P_{\mathrm{S}}}\Big\} \\ &= \int_0^\infty F_{\mathcal{X}_1}\left(\sqrt{\frac{x(\Delta P_{\mathrm{J}}\ y + \delta_{\mathrm{D1}}^2)}{P_{\mathrm{S}}}}\right) f_{{a_{\mathrm{JD}}}^2}(y)dy. \end{aligned} \tag{24}$$

Following a similar derivation to that of γ_{D}, the CDF of γ_{E} can be expressed as

$$\begin{aligned} F_{\gamma_{\mathrm{E}}}(x) &= \Pr\{\gamma_{\mathrm{E}} < x\} = \Pr\{\frac{\mathcal{X}_2^2 P_{\mathrm{S}}}{P_{\mathrm{J}}\ {a_{\mathrm{JE}}}^2 + \delta_{\mathrm{E}}^2} < x\} \\ &= \Pr\Big\{\mathcal{X}_2^2 < \frac{x(P_{\mathrm{J}}\ {a_{\mathrm{JE}}}^2 + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}\Big\} \\ &= \int_0^\infty F_{\mathcal{X}_2}\left(\sqrt{\frac{x(P_{\mathrm{J}}\ y + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}}\right) f_{{a_{\mathrm{JE}}}^2}(y)dy. \end{aligned} \tag{25}$$

To evaluate the integrals presented in equations (24) and (25), it is essential to determine the CDFs of $\mathcal{X}_1$ and $\mathcal{X}_2$. Specifically, the CDF of $\mathcal{X}_1 = a_{\mathrm{SD}} + \sum_{t=1}^{L} a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}$ can be obtained through the utilization of moment functions [36].

Based on equations (9) and (10), the n^{th} moment of a_{SD} is expressed as follows [24]

$$\mu_{a_{\mathrm{SD}}}(n) \equiv \mathbb{E}\{a_{\mathrm{SD}}^n\} = \frac{\Gamma(m_{a_{\mathrm{SD}}} + n/2)}{\Gamma(m_{a_{\mathrm{SD}}})}\Big(\frac{m_{a_{\mathrm{SD}}}}{\Omega_{a_{\mathrm{SD}}}}\Big)^{-n/2}. \tag{26}$$

As a result, specific moments of a_{SD} can be extracted from equation (26) as follows:

$$\mu_{a_{\mathrm{SD}}}(1) = \frac{\Gamma(m_{a_{\mathrm{SD}}} + 1/2)}{\Gamma(m_{a_{\mathrm{SD}}})}\sqrt{\frac{\Omega_{a_{\mathrm{SD}}}}{m_{a_{\mathrm{SD}}}}}, \tag{27}$$

$$\mu_{a_{\mathrm{SD}}}(2) = \frac{\Gamma(m_{a_{\mathrm{SD}}} + 1)}{\Gamma(m_{a_{\mathrm{SD}}})}\Big(\frac{m_{a_{\mathrm{SD}}}}{\Omega_{a_{\mathrm{SD}}}}\Big)^{-1} = \Omega_{a_{\mathrm{SD}}}. \tag{28}$$

Additionally, the PDF of $a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}$ can be expressed as follows

$$f_{a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}}(x) = \int_0^\infty \frac{1}{u} f_{a_{\mathrm{R}_t\mathrm{D}}}\left(\frac{x}{u}\right) f_{a_{\mathrm{SR}_t}}(u)du. \tag{29}$$

By substituting (10) into (29), we have

$$\begin{aligned} f_{a_{\mathrm{SR}_t} a_{\mathrm{R}_t\mathrm{D}}}(x) &= \frac{4}{\Gamma(m_{a_{\mathrm{SR}_t}})\Gamma(m_{a_{\mathrm{R}_t\mathrm{D}}})}\left(\frac{m_{a_{\mathrm{SR}_t}}}{\Omega_{a_{\mathrm{SR}_t}}}\right)^{m_{a_{\mathrm{SR}_t}}} \\ &\times \left(\frac{m_{a_{\mathrm{R}_t\mathrm{D}}}}{\Omega_{a_{\mathrm{R}_t\mathrm{D}}}}\right)^{m_{a_{\mathrm{R}_t\mathrm{D}}}} x^{2m_{a_{\mathrm{R}_t\mathrm{D}}}-1} \int_0^\infty u^{2m_{a_{\mathrm{SR}_t}}-2m_{a_{\mathrm{R}_t\mathrm{D}}}-1} \\ &\times \exp\left(-\frac{m_{a_{\mathrm{SR}_t}} u^2}{\Omega_{a_{\mathrm{SR}_t}}} - \frac{x^2 m_{a_{\mathrm{R}_t\mathrm{D}}}}{\Omega_{a_{\mathrm{R}_t\mathrm{D}}} u^2}\right) du. \end{aligned} \tag{30}$$

Using [37, Equation (3.478.4)], the PDF given in (30) is defined as follows

$$f_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(x) = \frac{4\left(\frac{m_{a_{\mathrm{SR}_t}} m_{a_{\mathrm{R}_t\mathrm{D}}}}{\Omega_{a_{\mathrm{SR}_t}}\Omega_{a_{\mathrm{R}_t\mathrm{D}}}}\right)^{\frac{m_{a_{\mathrm{SR}_t}}+m_{a_{\mathrm{R}_t\mathrm{D}}}}{2}}}{\Gamma(m_{a_{\mathrm{SR}_t}})\Gamma(m_{a_{\mathrm{R}_t\mathrm{D}}})} \times x^{m_{a_{\mathrm{SR}_t}}+m_{a_{\mathrm{R}_t\mathrm{D}}}-1} \kappa_{m_{a_{\mathrm{SR}_t}}-m_{a_{\mathrm{R}_t\mathrm{D}}}}\left(2x\sqrt{\frac{m_{a_{\mathrm{SR}_t}} m_{a_{\mathrm{R}_t\mathrm{D}}}}{\Omega_{a_{\mathrm{SR}_t}}\Omega_{a_{\mathrm{R}_t\mathrm{D}}}}}\right). \tag{31}$$

Subsequently, the n^{th} moment of $a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}$ is derived as follows

$$\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(n) \triangleq \mathbb{E}\left\{(a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}})^n\right\} = \int_0^\infty v^n f_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(v)\,dv. \tag{32}$$

By substituting (31) into (32) and applying [37, Equation (6.561.16)], we obtain

$$\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(n) = \left(\frac{m_{a_{\mathrm{SR}_t}} m_{a_{\mathrm{R}_t\mathrm{D}}}}{\Omega_{a_{\mathrm{SR}_t}}\Omega_{a_{\mathrm{R}_t\mathrm{D}}}}\right)^{-n/2} \times \frac{\Gamma\left(m_{a_{\mathrm{SR}_t}}+\frac{n}{2}\right)\Gamma\left(m_{a_{\mathrm{R}_t\mathrm{D}}}+\frac{n}{2}\right)}{\Gamma\left(m_{a_{\mathrm{SR}_t}}\right)\Gamma\left(m_{a_{\mathrm{R}_t\mathrm{D}}}\right)}. \tag{33}$$

Let $\Psi = \sum_{t=1}^{L} a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}$, its n^{th} moment is computed as [38]

$$\mu_\Psi(n) \triangleq \mathbb{E}\left\{\Psi^n\right\} = \sum_{n_1=0}^{n}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{L-1}=0}^{n_{L-2}}\binom{n}{n_1}\binom{n_1}{n_2}\cdots\binom{n_{L-2}}{n_{L-1}} \times \mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(n-n_1)\,\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(n_1-n_2)\cdots\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(n_{L-1}), \tag{34}$$

where $\binom{x}{y} = \frac{x!}{y!(x-y)!}$.

Using (33) and (34), the specific moments of Ψ are respectively expressed as [24]

$$\mu_\Psi(1) = \sum_{t=1}^{L}\mu_{a_{\mathrm{R}_t\mathrm{D}}}(1), \tag{35}$$

$$\mu_\Psi(2) = \sum_{t=1}^{L}\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(2) + 2\sum_{t=1}^{L}\sum_{t'=t+1}^{L}\left[\mu_{a_{\mathrm{SR}_t}a_{\mathrm{R}_t\mathrm{D}}}(1)\right]^2. \tag{36}$$

The n^{th} moment of $\mathcal{X}_1$ can now be represented as

$$\mu_{\mathcal{X}_1}(n) \triangleq \mathbb{E}\left\{(\Psi + a_{\mathrm{SD}})^n\right\} = \mathbb{E}\left\{\sum_{w=0}^{n}\binom{n}{w}\Psi^w\,(a_{\mathrm{SD}})^{n-w}\right\} = \sum_{w=0}^{n}\binom{n}{w}\mu_\Psi(w)\,\mu_{a_{\mathrm{SD}}}(n-w). \tag{37}$$

Based on (37), the specific moments of $\mathcal{X}_1$ are obtained as

$$\mu_{\mathcal{X}_1}(1) = \mu_\Psi(1) + \mu_{a_{\mathrm{SD}}}(1), \tag{38}$$

$$\mu_{\mathcal{X}_1}(2) = \mu_\Psi(2) + \mu_{a_{\mathrm{SD}}}(2) + 2\,\mu_\Psi(1)\,\mu_{a_{\mathrm{SD}}}(1). \tag{39}$$

From the moment expression, the CDF of $\mathcal{X}_1$ is given by [36]

$$F_{\mathcal{X}_1}(y) = \frac{1}{\Gamma\left(\frac{\left[\mu_{\mathcal{X}_1}(1)\right]^2}{\mu_{\mathcal{X}_1}(2)-\left[\mu_{\mathcal{X}_1}(1)\right]^2}\right)} \times \gamma\left(\frac{\left[\mu_{\mathcal{X}_1}(1)\right]^2}{\mu_{\mathcal{X}_1}(2)-\left[\mu_{\mathcal{X}_1}(1)\right]^2}, \frac{\mu_{\mathcal{X}_1}(1)y}{\mu_{\mathcal{X}_1}(2)-\left[\mu_{\mathcal{X}_1}(1)\right]^2}\right) = \frac{1}{\Gamma(\omega_1)}\gamma(\omega_1,\phi_1 y) = 1 - \frac{1}{\Gamma(\omega_i)}\Gamma(\omega_1,\phi_1 y). \tag{40}$$

From (10), we have

$$f_{\mathcal{Y}_i^2}(y) = \frac{m_{\mathcal{Y}_i}^{m_{\mathcal{Y}_i}}}{\Gamma(m_{\mathcal{Y}_i})\Omega_{\mathcal{Y}_i}^{m_{\mathcal{Y}_i}}} y^{m_{\mathcal{Y}_i}-1}\exp\left(-\frac{m_{\mathcal{Y}_i}y}{\Omega_{\mathcal{Y}_i}}\right), \quad y \geq 0 \tag{41}$$

where $\mathcal{Y}_i \in \{a_{\mathrm{JD}}, a_{\mathrm{JE}}\}$.

Applying (40) and (41) into (24), we have

$$F_{\gamma_{\mathrm{D}}}(x) = \int_0^\infty F_{\mathcal{X}_1}\left(\sqrt{\frac{x(\Delta P_{\mathrm{J}}\ y + \delta_{\mathrm{D}}^2)}{P_{\mathrm{S}}}}\right) f_{a_{\mathrm{JD}}{}^2}(y)dy = 1 - \frac{1}{\Gamma(\omega_1)}\frac{m_{\mathrm{JD}}^{m_{\mathrm{JD}}}}{\Gamma(m_{\mathrm{JD}})\Omega_{\mathrm{JD}}^{m_{\mathrm{JD}}}} \times \int_0^\infty \Gamma(\omega_1, \phi_1\sqrt{\frac{x(\Delta P_{\mathrm{J}}\ y + \delta_{\mathrm{D}}^2)}{P_{\mathrm{S}}}} y^{m_{\mathrm{JD}}-1}\exp(-\frac{m_{\mathrm{JD}}y}{\Omega_{\mathrm{JD}}})dy. \tag{42}$$

Deriving a closed-form expression for the CDF of γ_{D} in (42) is analytically intractable. However, an effective approximation of (42) can be achieved using the Chebyshev-Gauss quadrature method [39, Equation (25.4.30)], whose approximation formula is given by

$$\int_a^b f(x)dx \approx \frac{(b-a)\pi}{2N}\sum_{n=1}^{N}\sqrt{1-v_n^2 f(x_n)}, \tag{43}$$

where N denotes the Chebyshev parameter, which characterizes the trade-off between computational complexity and approximation accuracy, and

$$v_n = \cos\left(\frac{2n-1}{2N}\pi\right), x_n = \frac{b-a}{2}v_n + \frac{b+a}{2}.$$

By setting $\alpha_{\mathrm{JD}} = \frac{m_{\mathrm{JD}}}{\Omega_{\mathrm{JD}}}$ and $z = \exp(-\alpha_{\mathrm{JD}}y)$, we can transform (42) into the following form

$$F_{\gamma_{\mathrm{D}_1}^{\mathrm{e2e}}}(x) = 1 - \frac{1}{\Gamma(\omega_1)} \frac{\alpha_{\mathrm{JD}}^{m_{\mathrm{JD}}}}{\Gamma(m_{\mathrm{JD}})} \Big(\frac{1}{\alpha_{\mathrm{JD}}}\Big)^{m_{\mathrm{JD}}-1} \frac{1}{\alpha_{\mathrm{JD}}}$$
$$\int_0^1 \Big(\ln \frac{1}{z}\Big)^{m_{\mathrm{JD}}-1} \Gamma(\omega_1, \phi_1 \sqrt{\frac{x(\Delta P_{\mathrm{J}} \frac{1}{\alpha_{\mathrm{JD}}} \ln \frac{1}{z} + \delta_{\mathrm{D}}^2)}{P_{\mathrm{S}}}} dz. \tag{44}$$

Using the result in (43), the integral in (44) can be computed as follows

$$F_{\gamma_{\mathrm{D}}}(x) = 1 - \frac{1}{\Gamma(\omega_1)\Gamma(m_{\mathrm{JD}})} \Big(\ln \frac{2}{v_n + 1}\Big)^{m_{\mathrm{JD}}-1} \frac{\pi}{2N}$$
$$\times \sum_{n=1}^{N} \sqrt{1 - v_n^2}\, \Gamma\Big(\omega_1, \phi_1 \sqrt{\frac{x(\Delta P_{\mathrm{J}} \frac{1}{\alpha_{\mathrm{JD}}} \ln \frac{2}{v_n+1} + \delta_{\mathrm{D}}^2)}{P_{\mathrm{S}}}}\Big)$$
$$= 1 - \sum_{n=1}^{N} \xi_n \Gamma\Big(\omega_1, \phi_1 \sqrt{\frac{\mathrm{A_D} x}{P_{\mathrm{S}}}}\Big). \tag{45}$$

Following the same approach, the CDF of γ_{E} can be expressed as

$$F_{\gamma_{\mathrm{E}}}(x) = \Pr\{\gamma_{\mathrm{E}} < x\} = \Pr\{\frac{\mathcal{X}_2^2 P_{\mathrm{S}}}{P_{\mathrm{J}} a_{\mathrm{JE}}{}^2 + \delta_{\mathrm{E}}^2} < x\}$$
$$= \Pr\Big\{\mathcal{X}_2^2 P_{\mathrm{S}} < x(P_{\mathrm{J}}\ a_{\mathrm{JE}}{}^2 + \delta_{\mathrm{E}}^2)\Big\}$$
$$= \int_0^\infty F_{\mathcal{X}_2}\left(\sqrt{\frac{x(P_{\mathrm{J}}\ y + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}}\right) f_{a_{\mathrm{JE}}{}^2}(y)dy$$
$$= 1 - \frac{1}{\Gamma(\omega_2)} \frac{m_{\mathrm{JE}}^{m_{\mathrm{JE}}}}{\Gamma(m_{\mathrm{JE}})\Omega_{\mathrm{JE}}^{m_{\mathrm{JE}}}}$$
$$\times \int_0^\infty \Gamma(\omega_2, \phi_2 \sqrt{\frac{x(P_{\mathrm{J}}\ y + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}} y^{m_{\mathrm{JE}}-1} \exp\left(-\frac{m_{\mathrm{JE}} y}{\Omega_{\mathrm{JE}}}\right) dy. \tag{46}$$

Let $\alpha_{\mathrm{JE}} = \frac{m_{\mathrm{JE}}}{\Omega_{\mathrm{JE}}}$ and $z = \exp(-\alpha_{\mathrm{JE}} y)$, we can rewrite (46) as follows

$$F_{\gamma_{\mathrm{E}}}(x) = 1 - \frac{1}{\Gamma(\omega_2)} \frac{\alpha_{\mathrm{JE}}^{m_{\mathrm{JE}}}}{\Gamma(m_{\mathrm{JE}})} \Big(\frac{1}{\alpha_{\mathrm{JE}}}\Big)^{m_{\mathrm{JE}}-1} \frac{1}{\alpha_{\mathrm{JE}}}$$
$$\times \int_0^1 \Gamma(\omega_2, \phi_2 \sqrt{\frac{x(P_{\mathrm{J}} \frac{1}{\alpha_{\mathrm{JE}}} \ln \frac{1}{z} + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}} \Big(\ln \frac{1}{z}\Big)^{m_{\mathrm{JE}}-1} dz. \tag{47}$$

By applying (43) to evaluate the integral in (47), we obtain

$$F_{\gamma_{\mathrm{E}}}(x) = 1 - \frac{1}{\Gamma(\omega_2)\Gamma(m_{\mathrm{JE}})} \Big(\ln \frac{2}{v_w + 1}\Big)^{m_{\mathrm{JE}}-1} \frac{\pi}{2W}$$
$$\times \sum_{w=1}^{W} \sqrt{1 - v_w^2}\, \Gamma\Big(\omega_2, \phi_2 \sqrt{\frac{x(P_{\mathrm{J}} \frac{1}{\alpha_{\mathrm{JE}}} \ln \frac{2}{v_w+1} + \delta_{\mathrm{E}}^2)}{P_{\mathrm{S}}}}\Big)$$
$$= 1 - \sum_{w=1}^{W} \xi_w \Gamma\Big(\omega_2, \phi_2 \sqrt{\frac{\mathrm{A_E} x}{P_{\mathrm{S}}}}\Big). \tag{48}$$

By substituting (45) into (13), we obtain the expression of $\mathrm{C_D}$ as

$$\mathbb{E}\{\mathrm{C_D}\} = \frac{1}{\ln 2} \sum_{n=1}^{N} \xi_n \int_0^\infty \frac{1}{1+x} \Gamma\Big(\omega_1, \phi_1 \sqrt{\frac{\mathrm{A_D} x}{P_{\mathrm{S}}}}\Big) dx. \tag{49}$$

Let $z = 1/(1+x)$, formula (49) can be reformulated as

$$\mathbb{E}\{\mathrm{C_D}\} = \frac{1}{\ln 2} \sum_{n=1}^{N} \varepsilon_n \int_0^1 \frac{1}{z} \Gamma\Big(\omega_1, \phi_1 \sqrt{\frac{\mathrm{A_D}}{P_{\mathrm{S}}} \frac{1-z}{z}}\Big) dz. \tag{50}$$

Substituting (43) into the integral of (50), we derive

$$\mathbb{E}\{\mathrm{C_D}\} = \frac{1}{\ln 2} \sum_{n=1}^{N} \sum_{m=1}^{M} \varepsilon_n \varepsilon_m \Gamma\Big(\omega_1, \phi_1 \sqrt{\frac{\mathrm{A_D}}{P_{\mathrm{S}}} \frac{1-v_m}{1+v_m}}\Big). \tag{51}$$

Replacing into (14) the result from (48), we arrive at the expression for $\mathrm{C_E}$

$$\mathbb{E}\{\mathrm{C_E}\} = \frac{1}{\ln 2} \sum_{w=1}^{W} \xi_w \int_0^\infty \frac{1}{1+x} \Gamma\Big(\omega_2, \phi_2 \sqrt{\frac{\mathrm{A_E} x}{P_{\mathrm{S}}}}\Big) dx. \tag{52}$$

Using the variable change $z = 1/(1+x)$, formula (52) is rewritten in the form

$$\mathbb{E}\{\mathrm{C_E}\} = \frac{1}{\ln 2} \sum_{w=1}^{W} \varepsilon_w \int_0^1 \frac{1}{z} \Gamma\Big(\omega_2, \phi_2 \sqrt{\frac{\mathrm{A_E}}{P_{\mathrm{S}}} \frac{1-z}{z}}\Big) dz. \tag{53}$$

Using (43) in (53), the resulting expression for $\mathrm{C_E}$ is given by

$$\mathbb{E}\{\mathrm{C_E}\} = \frac{1}{\ln 2} \sum_{w=1}^{W} \sum_{q=1}^{Q} \varepsilon_w \varepsilon_q \Gamma\Big(\omega_2, \phi_2 \sqrt{\frac{\mathrm{A_E}}{P_{\mathrm{S}}} \frac{1-v_q}{1+v_q}}\Big). \tag{54}$$

Accordingly, inserting (51) and (54) into (12) leads to the expression of ASC in (15), concluding the proof.

Appendix B

This appendix outlines the complete derivation process for the ASC for the non-jammer system.

Following a similar method to that in (22) and (23), we derive the SINRs at D and E as follows

$$\gamma_{\mathrm{D}}^{\mathrm{NJ}} = \frac{\mathcal{X}_1^2 P_{\mathrm{S}}^{\mathrm{NJ}}}{\delta_{\mathrm{D}}^2}, \tag{55}$$

$$\gamma_{\mathrm{E}^{\mathrm{NJ}}} = \frac{\mathcal{X}_2^2 P_{\mathrm{S}}^{\mathrm{NJ}}}{\delta_{\mathrm{E}}^2}. \tag{56}$$

Using the result in (55), we obtain the CDF of $\gamma_{\mathrm{D}}^{\mathrm{NJ}}$ as

$$\begin{aligned} F_{\gamma_{\mathrm{D}}^{\mathrm{NJ}}}(x) &= \Pr\{\gamma_{\mathrm{D}}^{\mathrm{NJ}} < x\} = \Pr\{\frac{\mathcal{X}_1^2 P_{\mathrm{S}}^{\mathrm{NJ}}}{\delta_{\mathrm{D}}^2} < x\} \\ &= \Pr\Big\{\mathcal{X}_1^2 P_{\mathrm{S}}^{\mathrm{NJ}} < x\delta_{\mathrm{D}}^2\Big\} = F_{\mathcal{X}_1}\left(\sqrt{\frac{x\delta_{\mathrm{D}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}}\right) \\ &= 1 - \frac{1}{\Gamma(\omega_1)}\Gamma\big(\omega_1, \phi_1\sqrt{\frac{x\delta_{\mathrm{D}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}}\big). \end{aligned} \tag{57}$$

Following the same steps, the expression for $\gamma_{\mathrm{E}}^{\mathrm{NJ}}$ is given by

$$\begin{aligned} F_{\gamma_{\mathrm{E}}^{\mathrm{NJ}}}(x) &= \Pr\{\gamma_{\mathrm{E}}^{\mathrm{NJ}} < x\} = \Pr\{\frac{\mathcal{X}_2^2 P_{\mathrm{S}}^{\mathrm{NJ}}}{\delta_{\mathrm{E}}^2} < x\} \\ &= \Pr\Big\{\mathcal{X}_2^2 P_{\mathrm{S}}^{\mathrm{NJ}} < x\delta_{\mathrm{E}}^2\Big\} = F_{\mathcal{X}_2}\left(\sqrt{\frac{x\delta_{\mathrm{E}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}}\right) \\ &= 1 - \frac{1}{\Gamma(\omega_2)}\Gamma\big(\omega_2, \phi_2\sqrt{\frac{x\delta_{\mathrm{E}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}}\big). \end{aligned} \tag{58}$$

Substituting (57) into (13), we derive the following expression

$$\mathbb{E}\{C_{\mathrm{D}}^{\mathrm{NJ}}\} = \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_1)}\int_0^\infty \frac{1}{1+x}\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{x\delta_{\mathrm{D}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}}\Big)\, dx. \tag{59}$$

Using the same mathematical steps as in formula (49), the following expression is obtained

$$\mathbb{E}\{C_{\mathrm{D}}^{\mathrm{NJ}}\} = \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_1)}\varepsilon_{k_1}\Gamma\Big(\omega_1, \phi_1\sqrt{\frac{\delta_{\mathrm{D}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}\frac{1-v_{k_1}}{1+v_{k_1}}}\Big), \tag{60}$$

where $\varepsilon_{k_1} = \frac{\pi\sqrt{1-v_{k_1}^2}}{2K_1}\frac{2}{1+v_{k_1}}$.

Similar $\mathbb{E}\{C_{\mathrm{D}}^{\mathrm{NJ}}\}$, we obtain

$$\mathbb{E}\{C_{\mathrm{E}}^{\mathrm{NJ}}\} = \frac{1}{\ln 2}\frac{1}{\Gamma(\omega_2)}\varepsilon_{k_2}\Gamma\Big(\omega_2, \phi_2\sqrt{\frac{\delta_{\mathrm{D}}^2}{P_{\mathrm{S}}^{\mathrm{NJ}}}\frac{1-v_{k_2}}{1+v_{k_2}}}\Big), \tag{61}$$

where $\varepsilon_{k_2} = \frac{\pi\sqrt{1-v_{k_2}^2}}{2K_2}\frac{2}{1+v_{k_2}}$.

By inserting (60) and (61) into (12), we derive the closed-form expression of $\mathrm{ASC}^{\mathrm{NJ}}$ as shown in (16). This finalizes the proof.

References

[1] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] H. Sharma, N. Kumar, and R. Tekchandani, "Physical layer security using beamforming techniques for 5G and beyond networks: A systematic review," *Physical Communication*, vol. 54, p. 101791, 2022.

[4] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE communications magazine*, vol. 58, no. 1, pp. 106–112, 2019.

[5] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3480–3495, 2021.

[6] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, Jan. 2017.

[7] M. Lin, C. Liu, and W. Wang, "Relay-assisted uplink covert communication in the presence of multi-antenna warden and uninformed jamming," *IEEE Transactions on Communications*, vol. 72, no. 4, pp. 2124–2137, 2023.

[8] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 778–782, Jan. 2020.

[9] D.-T. Do, A.-T. Le, N.-D. X. Ha, and N.-N. Dao, "Physical layer security for internet of things via reconfigurable intelligent surface," *Future Generation Computer Systems*, vol. 126, pp. 330–339, 2022.

[10] B. C. Nguyen, Q.-N. Van, L. T. Dung, T. M. Hoang, N. V. Vinh, and G. T. Luu, "Secrecy performance of multi-RIS-assisted wireless systems," *Mobile Networks and Applications*, vol. 28, no. 3, pp. 1206–1219, 2023.

[11] P. Li, K. Guo, F. Zhou, X. Wang, and Y. Huang, "Average Secrecy Capacity of the Reconfigurable Intelligent Surface-Assisted Integrated Satellite Unmanned Aerial Vehicle Relay Networks." *CMES-Computer Modeling in Engineering and Sciences*, vol. 138, no. 2, 2024.

[12] X. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, and P.-H. Ho, "Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions," *IEEE Systems Journal*, vol. 17, no. 1, pp. 848–859, 2022.

[13] C. Jiang, C. Zhang, C. Huang, J. He, Z. Zhang, and J. Ge, "Secure performance comparison for NOMA: Reconfigurable intelligent surface or amplify-and-forward relay?" *Journal of Information and Intelligence*, vol. 2, no. 6, pp. 514–524, 2024.

[14] H. Liu, J. Luo, S. Wang, and H. Ding, "Effective Secrecy Capacity for RIS-Assisted NOMA Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 1, pp. 1379–1384, 2025.

[15] T. T. Nguyen, T. M. Hoang, and P. T. Tran, "Secrecy performance optimization for UAV-based relay NOMA systems with friendly jamming," *Computer Communications*, vol. 235, p. 108086, 2025.

[16] V. T. Ty, P. N. Son, and T. T. Duy, "Secrecy performance of RIS-assisted wireless-powered systems with artificial-jamming generation," *Physical Communication*, vol. 69, p. 102592, Apr. 2025.

[17] E. Illi, M. K. Qaraqe, F. E. Bouanani, and S. M. Al-Kuwari, "Can Artificial Noise Boost Further the Secrecy of Dual-hop RIS-aided Networks?" *arXiv preprint arXiv:2208.01726*, 2022.

[18] T.-L. Le, B. C. Nguyen, L. T. Dung, T. M. Hoang, T. Kim, and G. T. Luu, "Improving secrecy performance of NOMA networks with multiple non-colluding eavesdroppers employing multiple aerial reconfigurable intelligent surfaces," *Physical Communication*, vol. 63, p. 102314, 2024.

[19] A.-T. Le, T. D. Hieu, T. N. Nguyen, T.-L. Le, S. Q. Nguyen, and M. Voznak, "Physical layer security analysis for RIS-aided NOMA systems with non-colluding eavesdroppers," *Computer Communications*, vol. 219, pp. 194–203, Apr. 2024.

[20] X. Wei, D. Shen, and L. Dai, "Channel estimation for ris assisted wireless communications—part i: Fundamen-

tals, solutions, and future opportunities," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1398–1402, 2021.

[21] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis," *IEEE transactions on wireless communications*, vol. 19, no. 10, pp. 6607–6620, 2020.

[22] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless communications letters*, vol. 9, no. 2, pp. 240–243, 2019.

[23] X. N. Pham, B. C. Nguyen, T. D. Thi, V. V. Nguyen, B. V. Minh, T. Kim, T. N. Nguyen, and A. V. Le, "Enhancing data rate and energy efficiency of NOMA systems using reconfigurable intelligent surfaces for millimeter-wave communications," *Digital Signal Processing*, vol. 151, p. 104553, Aug. 2024.

[24] Q.-N. Van, B. C. Nguyen, T. M. Hoang, H. M. Nguyen, V. V. Nguyen, G. T. Luu *et al.*, "Multiple RISs for enhancing the secrecy performance of NOMA systems over realistic Nakagami-m fading channels," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 5, pp. 6584–6599, May 2023.

[25] Y. Ai, A. P. Felipe, L. Kong, M. Cheffena, S. Chatzinotas, and B. Ottersten, "Secure vehicular communications through reconfigurable intelligent surfaces," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7272–7276, 2021.

[26] M. H. Khoshafa, T. M. N. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1443–1447, 2020.

[27] B. Tahir, S. Schwarz, and M. Rupp, "Analysis of uplink IRS-assisted NOMA under Nakagami-m fading via moments matching," *IEEE Wireless Communications Letters*, vol. 10, no. 3, pp. 624–628, 2020.

[28] G. Alnwaimi and H. Boujemaa, "Non orthogonal multiple access using reconfigurable intelligent surfaces," *Wireless Personal Communications*, vol. 121, no. 3, pp. 1607–1625, 2021.

[29] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 296–12 300, 2020.

[30] A. Papoulis, *Random variables and stochastic processes*. McGraw Hill, 1965.

[31] T. M. Hoang, B. C. Nguyen, X. N. Tran, T. Kim *et al.*, "Secrecy performance analysis for mimo-df relay systems with mrt/mrc and tzf/mrc schemes," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 173–10 186, 2023.

[32] F. Zhao, W. Hao, H. Guo, G. Sun, Y. Wang, and H. Zhang, "Secure energy efficiency for mmWave-NOMA cognitive satellite terrestrial network," *IEEE Communications Letters*, vol. 27, no. 1, pp. 283–287, Apr. 2022.

[33] E. Björnson, Ö. Özdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE wireless communications letters*, vol. 9, no. 2, pp. 244–248, 2019.

[34] T. Q. Duong, T. T. Duy, M. Matthaiou, T. Tsiftsis, and G. K. Karagiannidis, "Cognitive cooperative networks in dual-hop asymmetric fading channels," in *Proceedings of the IEEE GLOBECOM*. IEEE, 2013, pp. 955–961.

[35] B. Li, Y. Zou, T. Wu, Z. Zhang, M. Chen, and Y. Jiang, "Security and Reliability Tradeoff of NOMA Based Hybrid Satellite-Terrestrial Network With a Friendly Jammer," *IEEE Transactions on Vehicular Technology*, pp. 3439–3444, 2025.

[36] T. N. Do, G. Kaddoum, T. L. Nguyen, D. B. Da Costa, and Z. J. Haas, "Multi-RIS-aided wireless systems: Statistical characterization and performance analysis," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8641–8658, 2021.

[37] A. Jeffrey and D. Zwillinger, "Table of integrals, series, and products by IS Gradshteyn and IM Ryzhik," 1994.

[38] D. B. da Costa, H. Ding, and J. Ge, "Interference-limited relaying transmissions in dual-hop cooperative networks over Nakagami-m fading," *IEEE Communications Letters*, vol. 15, no. 5, pp. 503–505, 2011.

[39] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, 1972.

Vo Ta Ty received the B.S. degree in electrical engineering from Telecommunication University, Khanh Hoa, Vietnam, from the Posts and Telecommunications Institute of Technology (VNPT), Ho Chi Minh City, Vietnam, in 2011. Now, he is working toward the Ph.D degree in the Faculty of Electrical and Electronics Engineering with Ho Chi Minh City University of Technology and Education (HCMUTE). His major research interests are physical layer security, cooperative communication, intelligent reflecting surfaces.

Tran Trung Duy received the PhD degree (2013) in electrical engineering from University of Ulsan, South Korea. From 2013 to the present, he joined the Posts and Telecommunications Institute of Technology (PTIT), Ho Chi Minh City campus. From 2017, he served as an associate editor of Transactions on Industrial Networks and Intelligent Systems. From 2021, he served as an associate editor of Hindawi Wireless Communications and Mobile Computing and Frontiers in Communications and Networks. His major research interests are cooperative communications, cooperative multi-hop, cognitive radio, physical-layer security, energy harvesting, hardware impairments, and Fountain codes.

Pham Ngoc Son received the BE degree (2005) and M. Eng. degree (2009) in Electronics and Telecommunications Engineering from the Post and Telecommunication Institute of Technology, Ho Chi Minh City and Ho Chi Minh City University of Technology, Vietnam, respectively. In 2015, he received the PhD degree in Electrical Engineering from University of Ulsan, South Korea. He is currently an associate Professor in the Faculty of Electrical and Electronics Engineering (FEEE) of Ho Chi Minh City University of Technology and Education (HCMUTE). His major research interests are cooperative communication, cognitive radio, physical layer security, energy harvesting, intelligent reflecting surfaces, short packet communications, and deep learning.

Tran Manh Hoang received the B.S. degree in communication command from Telecommunications University, Ministry of Defense, Nha Trang, Vietnam, in 2002, the B.Eng. degree in electrical engineering from Le Quy Don Technical University, Ha Noi, Vietnam, in 2006 the M.Eng. degree in electronics engineering from Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam, in 2013 and the Ph.D degree from Le Quy Don Technical University, Hanoi, Vietnam, in 2018. He is currently working as a Lecturer with Telecommunications University Khanh Hoa, Vietnam and a Visiting Professor the School of Information and Communication Engineering, Chungbuk National University, Cheongju 28644, South Korea from November 2021. He has more than 100 papers in referred international journals and conferences. His research interests include energy harvesting, UAV, short packet communication, non-orthogonal multiple access, and MIMO, RIS, signal processing for wireless cooperative communications. He was a recipient of the IEEE ATC-2022, REV-ECIT-2023, and IEEE ICCAIS-2023 Best Papers Award.