Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 12, No. 04, December 2026.

SECRECY PERFORMANCE ANALYSIS OF RIS-ASSISTED RSMA SYSTEMS UNDER IMPERFECT ARTIFICIAL JAMMING CANCELLATION AND IMPERFECT SIC

Le Huu Luyen[1], Le The Dung[1], Thanh Trung Nguyen[2] and Tran Manh Hoang[2]

(Received: 13-Aug.-2026, Revised: 29-Sep.-2026, Accepted: 4-Oct.-2026)

ABSTRACT

This work investigates a secrecy communication for a novel reconfigurable intelligent surface (RIS)-assisted rate-splitting multiple access (RSMA) downlink transmission system using the artificial jamming (AJ). To better reflect practical scenarios, this work considers the effects of imperfect successive interference cancellation (SIC) and residual artificial jamming (AJ) interference at legitimate users. The mathematical analysis is derived by using the statistical characteristics of the cascaded channel using the Gaussian-Chebyshev quadrature and the incomplete Gamma function. Closed-form expressions are derived for four key performance metrics: outage probability, intercept probability, secrecy reliability trade-off, and average secrecy capacity. Moreover, the Golden Section Search (GSS) is separately applied to determine the optimal values of individual system parameters through one-dimensional optimization. The analytical expressions are verified against Monte Carlo simulation, which verifies that the proposed jammer-assisted RIS-RSMA scheme achieves significantly better performance than RIS-assisted non-orthogonal multiple access (NOMA), and RIS-assisted Non-jammer benchmark schemes in terms of secrecy performance. The results further reveal that the proposed jammer-assisted RIS-RSMA scheme achieves the most favorable security-reliability trade-off among all considered schemes, outperforming both the RIS-assisted NOMA and non-AJ counterparts.

KEYWORDS

Physical layer security, Rate-splitting multiple access, Artificial jamming, Reconfigurable intelligent surface, Non-orthogonal multiple access, Imperfect AJ cancellation, Secrecy-reliability trade-off.

1. INTRODUCTION

Internet of Things (IoT) is regarded as a key enabler of sixth-generation (6G) wireless networks, supporting massive connectivity and intelligent services. However, the rapid growth of IoT devices introduces significant challenges, including spectrum scarcity, signaling overhead, and increased vulnerability because of the inherently broadcast characteristic of wireless networks [1]. Conventional encryption techniques and orthogonal multiple access (OMA) or non-orthogonal multiple access (NOMA) may become inefficient in large-scale IoT systems because of their high complexity and energy consumption [2]. To address these issues, physical-layer security (PLS) and advanced multiple-access techniques have emerged as promising solutions to achieve secure transmission without relying on complex cryptographic operations, while also improving spectral efficiency (SE) and interference management capabilities [3]. From the PLS perspective, secure wireless transmission has also been investigated by combining energy harvesting with multi-antenna diversity to improve communication security against eavesdropping [4]. Meanwhile, rate-splitting multiple access (RSMA) has been widely recognized for its high SE and flexible interference management capabilities [5]. In addition, reconfigurable intelligent surfaces (RISs) can intelligently reconfigure wireless propagation to enhance legitimate communications and suppress information leakage to eavesdroppers (Eve) [6, 7]. Furthermore, artificial jamming (AJ) can effectively impair the reception quality at the eavesdropper, thereby enhancing secrecy performance. Recent studies have further extended RSMA and RIS technologies to emerging integrated wireless networks. In particular, RSMA and advanced multiple-access techniques have been investigated to support massive access in satellite-aerial and space-air-ground integrated networks (SAGINs) [8, 9]. Meanwhile, RIS-assisted transmission has been explored in hybrid satellite-terrestrial relay networks and, more recently, in secure multi-RIS-assisted SAGINs to enhance transmission and secrecy performance [10]-[11].

1. L. H. Luyen and L. T. Dung are with Ho Chi Minh City University of Technology and Engineering, Vietnam, Emails: {luyenlh25.ncs, dunglt}@hcmute.edu.vn.
2. T. T. Nguyen and T. M. Hoang (Corresponding Author) are with Telecommunications University, Khanh Hoa, Vietnam, Emails: {thanhtrungsqtt, tranmanhhoang}@tcu.edu.vn

1.1 Related Works

Recently, the integration of RIS and RSMA for enhancing PLS has attracted increasing research attention. However, studies jointly exploiting the benefits of RIS, RSMA, and AJ to further improve secrecy performance remain relatively limited. Most studies focus on physical properties of the signal *via* RIS elements to enhance the energy quality experienced by legitimate users and confusing the received signals at eavesdroppers. Specially, the authors in [12, 13] employed the deep reinforcement learning to investigate the PLS of the RIS-assisted RSMA systems. The results revealed that RSMA, particularly in conjunction with a larger RIS, provides substantial gains in PLS over both NOMA and space division multiple access (SDMA). In [14], a secure transmission framework based on RIS-assisted cooperative RSMA was proposed, where cooperative relaying (CR-RISs) are employed to improve secrecy performance. The proposed scheme outperformed both the cooperative RSMA scheme without RIS deployment and the non-cooperative RIS-assisted RSMA scheme, highlighting the benefits of jointly exploiting cooperative relaying users and CR-RIS. A secure RIS-assisted RSMA scheme for multi-cluster high-altitude platforms (HAPs) systems was proposed by [15], where time allocation, precoding, and RIS beamforming were jointly optimized to maximize the sum-rate performance subject to secrecy constraints. Although the above works investigated PLS in RIS-assisted RSMA systems, secrecy performance was primarily assessed through simulations and algorithmic comparisons, without deriving analytical closed-form expressions to provide insights into the effects of system parameters. Furthermore, AJ, which can effectively improve secrecy performance by suppressing information interception at Eve, was not incorporated.

Other studies investigate the secrecy performance in integrated sensing and communication (ISAC) frameworks assisted by RIS systems employing RSMA [16, 17]. These works jointly optimized the communication, and radar precoders with RIS phase shifts, while utilizing the common stream as AJ to maximize the minimum secrecy rate. The results showed that adding or removing radar sequences balances system complexity and security; while keeping RSMA-ISAC performance close to the communication-only scheme. The authors in [18] use an active RIS to reduce eavesdropping and perform joint resource allocation for secure beamforming in the mmWave-RSMA system. This scheme enables the maximization of the sum secrecy rate of the considered system. In [19], the authors develop a novel secure transmission framework by combining the stream-splitting strategy of RSMA with RIS-assisted communications to mitigate security threats in satellite networks. Herein, the diagonal RIS (BD-RIS) is employed, and the results validate that the secrecy rate achieved by the BD-RIS outperforms those of the benchmark schemes. However, the works in [16, 17, 18] focus on beamforming design to enhance the secrecy rate and balance the rate between sensing and communication, whereas [19] investigates the stream-splitting strategy through iterative optimization. It is worth noting that most existing works employing AJ rely on the ideal assumption of perfect AJ cancellation at legitimate users. Due to hardware impairments, perfect cancellation may not be achievable in practice.

The secrecy performance of RIS-assisted original RSMA systems was investigated in [20, 21, 22]. In particular, [20] studied the max-min secrecy rate-optimization problem for the multiple-input single-output (MISO)-RSMA system. The work in [21] considered the secrecy rate in the novel RIS is mounted by an autonomous aerial vehicle (AAV) device. To further enhance the secrecy rate of conventional RIS systems, the simultaneously transmitting and reflecting (STAR-RIS)-assisted RSMA framework was proposed in [22]. These studies showed that RIS-assisted RSMA significantly outperforms conventional multiple-access schemes and benchmark systems without RIS in terms of secrecy rate. Unfortunately, these works did not employ the AJ to enhance the signal-to-noise ratio (SNR) of the legitimate channel and relied only on simulations to analyze secrecy performance. On the one hand, these works assume perfect successive interference cancellation (pSIC) at users, while in practical scenarios, due to hardware impairments and various types of noise, it is difficult to achieve pSIC.

In addition to optimization-oriented studies, recent works have investigated RSMA from a performance-analysis perspective. In [23], the outage performance of mmWave RSMA systems was analyzed using stochastic geometry, where closed-form expressions for the OP and asymptotic OP were derived. From a PLS perspective, [24] investigated secure mmWave RSMA systems in the presence of a passive eavesdropper and derived analytical expressions for the secrecy outage probability (SOP) using Gaussian-Chebyshev quadrature. More recently, [25] investigated the PLS of RSMA-aided integrated

sensing and communication systems and developed iterative optimization algorithms for secure beamforming under different eavesdropper CSI assumptions. In addition, the outage performance of RSMA over keyhole fading channels was analytically investigated under both perfect and imperfect SIC, providing further insights into the reliability of RSMA under challenging propagation conditions [26]. These studies provide important advances in RSMA performance analysis and secure transmission. However, the joint effects of RIS, AJ, ipSIC, and imperfect AJ cancellation on multiple secrecy and reliability metrics have not been analytically characterized.

Despite recent advances in RIS- and AJ-enabled PLS techniques, several important challenges remain unresolved in the literature. In particular, the joint impact of RIS, RSMA, AJ, imperfect AJ cancellation, and imperfect SIC (ipSIC) on secrecy performance has not yet been investigated within a unified analytical framework. Moreover, most existing studies primarily rely on simulation-based evaluations without deriving closed-form expressions to characterize the influence of system parameters on the secrecy behavior of the considered system. To address these limitations, our work investigates the PLS of RIS-assisted RSMA systems with AJ under Rayleigh fading channels. Table 1 summarizes the key characteristics of related studies and highlights the main distinctions of the proposed work.

Table 1. Comparison of the proposed work with existing RSMA performance-analysis and optimization studies.

Ref.	RIS	RSMA	AJ ipSIC	Imperfect AJ	Approach	Method/Tool Closed-form		Metrics
[12]	✓	✓			Optimization	HDRL		Secrecy rate
[13]	✓	✓			Optimization	DRL		Secrecy rate
[14]	✓	✓			Optimization	LPCR-RIS		Sum rate
[15]	✓	✓			Optimization	SCA		Secrecy-constrained sum rate
[16]	✓	✓	✓		Optimization	AO/SCA		Max-min secrecy rate
[17]	✓	✓			Optimization	BCD/WMMSE		Sum rate
[18]	✓	✓			Optimization	SCA/SDR		Sum secrecy rate
[19]	✓	✓			Optimization	PDD/SCA		Max-min secrecy rate
[20]	✓	✓	✓		Optimization	AO		Max-min secrecy rate
[21]	✓	✓	✓		Optimization	AO/DDPG		Sum secrecy rate
[22]	✓	✓			Optimization	AO/WMMSE		Max-min secrecy rate
23		✓			Performance analysis	Stochastic geometry	✓	OP, asymptotic OP
[24]		✓			Performance analysis	Gaussian-Chebyshev	✓	SOP
[25]		✓			Optimization	SCA/Penalty		Energy efficiency, secrecy capacity
[26]		✓		✓	Performance analysis	Gaussian-Chebyshev		OP, diversity order
Our work	✓	✓	✓	✓ ✓	Performance analysis/Optimization	Gaussian-Chebyshev	✓	OP, IP, SRT, ASC

1.2 Motivation and Contributions

The motivation of this work is to enhance PLS in RIS-assisted RSMA systems under practical deployment scenarios. Artificial jamming is adopted to impair information interception at Eve, while RIS is employed to improve propagation conditions without requiring multiple antennas at legitimate users. In addition, practical impairments, including imperfect SIC and imperfect AJ cancellation, are considered to better reflect realistic wireless environments. To provide further insights into the effects of system parameters on secrecy performance, mathematical expressions for the secrecy reliability trade-off (SRT), average secrecy capacity (ASC), outage probability (OP), and intercept probability (IP) are derived for the considered system. These metrics are rigorously derived by analyzing an approximated cumulative distribution function (CDF) *via* Gaussian-Chebyshev quadrature and the incomplete Gamma function. Compared with existing studies that mainly focus on optimization-based secrecy-rate enhancement, the analytical treatment of the considered system involves several additional technical

challenges. In particular, the simultaneous presence of the RIS-assisted cascaded channel, RSMA common and private streams, ipSIC, and residual AJ interference leads to coupled SINR expressions the distributions of which cannot be directly characterized using conventional channel models. Moreover, the secrecy analysis requires jointly characterizing the reliability of the legitimate links and the information interception capability of Eve under the same system parameters. To address these challenges, the statistical characteristics of the cascaded RIS channels are exploited together with Gaussian-Chebyshev quadrature and the incomplete Gamma function to obtain tractable analytical expressions for the OP, IP, SRT, and ASC. The analytical results further reveal several design insights. Increasing the transmit power or the number of RIS elements does not always improve secrecy performance, while the jamming power introduces a trade-off between suppressing Eve and increasing residual interference at legitimate users. Moreover, power allocation and imperfect interference cancellation significantly affect secrecy performance, indicating the existence of suitable operating points for key system parameters. The key contributions of this paper are summarized as follows:

- We propose an AJ-assisted secure transmission framework for RIS-assisted downlink RSMA systems under imperfect SIC (ipSIC). Specifically, the source node transmits superimposed RSMA signals to the users, while the jammer transmits an AJ signal that is imperfectly canceled at legitimate users, but remains unknown to Eve, thereby reducing interception capability and enhancing secrecy performance. This work closely reflects real-world scenarios of hardware impairment. Different from the RIS-AJ-assisted NOMA framework in [27], this work develops an RIS-AJ-assisted RSMA framework with common- and private-stream decoding.
- By employing Gaussian-Chebyshev quadrature and the incomplete Gamma function, closed-form expressions for the OP, IP, SRT, and ASC are derived for the RIS-assisted downlink RSMA system under the effects of ipSIC and imperfect AJ cancellation. Furthermore, separate one-dimensional optimization problems are formulated for the considered system parameters, and the Golden Section Search (GSS) algorithm is employed to determine their individual optimal values for SRT minimization or sum ASC maximization.
- Based on the derived analytical expressions, several insightful observations are obtained. Specifically, increasing the transmit power can reduce the OP of the main link, thereby improving reliability. However, it may simultaneously increase the risk of eavesdropping, leading to degraded secrecy performance. The results reveal the inherent reliability security trade-off in the considered system. Furthermore, the impacts of several key parameters, including the transmit power, jammer transmit power, number of RIS elements, and common stream coefficient, are systematically investigated to evaluate their effects on the overall reliability and security performance.
- Extensive numerical results are presented to validate the effectiveness of the considered scheme, and the results demonstrate that the proposed RIS-assisted RSMA scheme with AJ achieves superior secrecy performance compared with both the Non-jammer and NOMA benchmarks. Particularly, at a transmit power of $P_S = 30\text{dBm}$, the proposed scheme reduces the IP by about 98.5% compared with the Non-jammer scheme, while maintaining the OP below 10^{-2}. On the other hand, by optimizing the transmit power, the number of RIS elements, and the power allocation coefficient of the common stream, the system can minimize the SRT while maximizing the ASC.

The rest of the paper is structured as follows. Section 2 introduces the considered system model, while Section 3 develops the performance analysis and derives closed-form expressions for OP, IP, SRT, and ASC. Numerical results and corresponding discussions are provided in Section 4. Finally, Section 5 concludes the paper and summarizes the main contributions.

2. SYSTEM MODEL

The considered secure communication system employing RSMA-RIS-AJ is illustrated in Fig. 1. In this framework, a base station (S) employs the RSMA technique to transmit signals to two legitimate users, denoted by D_1 and D_2, in the presence of a passive eavesdropper (E). Due to the relatively long transmission distance between S and $D_i (i \in \{1,2\})$, together with the blockage of the direct links [28]-[29], an RIS equipped with L passive reflecting elements is utilized to facilitate signal propagation. To

enhance the PLS performance, an artificial jammer (J) is introduced to transmit jamming signals in order to confuse E and impair its decoding capability.

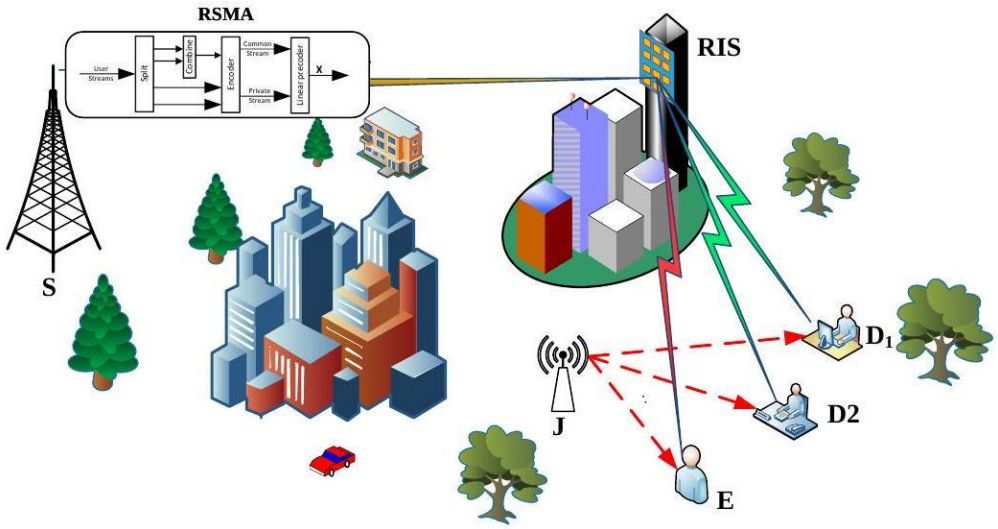


Figure 1. System model.

Furthermore, to better capture practical deployment scenarios, the impacts of residual AJ interference and ipSIC at D_i are also taken into account [27, 30]. For the analysis, the channel state information (CSI) of the legitimate links is considered available at the source node S, acquired through appropriate channel-estimation techniques or feedback-based approaches [31][1] All nodes are assumed to be equipped with a single antenna [29, 34][2], and the wireless propagation environment is modeled by Rayleigh fading channels [29, 35][3]. Since S employs RSMA, a common stream and two private streams are generated for transmission to D_1 and D_2. Specifically, the common signal x_c is designed for D_1 and D_2, whereas the private signals x_1 and x_2 are assigned to D_1 and D_2, respectively. Therefore, for each legitimate user D_i, both the common signal x_c and the corresponding private signal x_p contain useful information for signal detection.

At the receiver side, each user first decodes the common message x_c. After successfully removing this component, the corresponding private message is subsequently decoded, while the remaining private message $x_q (q \in \{1,2\}, q \neq p)$ is treated as interference [7]. Accordingly, the RSMA signal transmitted by S can be expressed as [7, 36]:

$$x_{\mathrm{S}} = x_c\sqrt{\alpha_c P_{\mathrm{S}}} + x_{p_1}\sqrt{\alpha_1 P_{\mathrm{S}}} + x_{p_2}\sqrt{\alpha_2 P_{\mathrm{S}}}, \tag{1}$$

where P_{S} denotes the transmit power of S, and $\alpha_c, \alpha_1, \alpha_2$ are the power allocation coefficients for messages x_c, x_{p_1} and x_{p_2}, respectively. These coefficients satisfy the constraint $\alpha_c + \alpha_1 + \alpha_2 = 1$.

The complex channel coefficients $h_{\mathrm{SR}_l} = a_{\mathrm{SR}_l} e^{-j\Psi_{\mathrm{SR}_l}}, h_{\mathrm{R}_l\mathrm{D}_i} = a_{\mathrm{R}_l\mathrm{D}_i} e^{-j\Psi_{\mathrm{R}_l\mathrm{D}_i}}$, and $h_{\mathrm{JD}_i} = a_{\mathrm{JD}_i} e^{-j\Psi_{\mathrm{JD}_i}}$ denote the channels between S and the l th RIS element, between the l th RIS element and D_i, and between J and D_i, respectively. Herein, $(a_{\mathrm{SR}_l}, \Psi_{\mathrm{SR}_l}), (a_{\mathrm{R}_l\mathrm{D}_i}, \Psi_{\mathrm{R}_l\mathrm{D}_i})$ and $(a_{\mathrm{JD}_i}, \Psi_{\mathrm{JD}_i})$ characterize the magnitude and phase of $h_{\mathrm{SR}_l}, h_{\mathrm{R}_l\mathrm{D}_i}$, and h_{JD_i}, respectively. As demonstrated in [27], the RIS can significantly enhance the received signal power through appropriate phase alignment Ψ_l, despite the fact

[1] In particular, advanced channel-estimation methods designed for RIS-assisted wireless systems can be employed to acquire CSI with relatively high accuracy [32, 33].
[2] The single-antenna SISO architecture considered in this work inherently provides limited spatial degrees of freedom compared with multi-antenna systems. Although the RIS can provide passive beamforming and coherent-combining gains through controllable reflections, it does not offer the full spatial multiplexing capabilities of a conventional MIMO system. The SISO setting is adopted to maintain analytical tractability and is also relevant to small-cell scenarios, where central access points are often equipped with only one transmit antenna.
[3] The analysis adopts a block-fading channel model, where the channel coefficients are assumed to remain constant within each transmission block. Therefore, temporal channel variations within a transmission block are not explicitly considered. Extending the proposed framework to time-varying channel conditions is left for future work.

that practical deployments are typically subjected to discrete and quantized phase constraints[4]. Nevertheless, to ensure analytical tractability and to establish a theoretical upper bound on the system performance, we adjust the phase shifts of the RIS elements to satisfy $\Psi_l = \Psi_{\mathrm{SR}_l} + \Psi_{\mathrm{R}_l\mathrm{D}_i}$ [30]. Therefore, the received signal at D_i aided by the RIS is represented as:

$$y_{\mathrm{D}_i} = \left(\sqrt{d_{\mathrm{SR}}^{-\beta} d_{\mathrm{RD}_i}^{-\beta}} \sum_{l=1}^{L} \alpha_{\mathrm{SR}_l} \alpha_{\mathrm{R}_l\mathrm{D}_i}\right) x_s + \sqrt{\eta_i P_{\mathrm{J}}} \sqrt{d_{\mathrm{JD}_i}^{-\beta}} h_{\mathrm{JD}_i} x_{\mathrm{J}} + z_{\mathrm{D}_i}, \tag{2}$$

where $d_{\mathrm{SR}}, d_{\mathrm{RD}_i}$, and d_{JD_i} represent the distances between S and the RIS, the RIS and D_i, and J and D_i, respectively. β denotes the path-loss factor, while $0 \le \eta_i \le 1$ denotes the residual AJ interference coefficient at D_i after imperfect AJ cancellation [27, 38][5] $\mathrm{z}_{\mathrm{D}_i} \sim \mathcal{CN}\left(0, \delta_{\mathrm{D}_i}^2\right)$ is the additive white Gaussian noise (AWGN) at D_i with zero mean and variance $\delta_{\mathrm{D}_i}^2$, and P_{J} is the power of the AJ.

Upon receiving the transmitted signal from source S reflected via the RIS to user D_i and based on (2), the signal-to-interference-plus-noise ratio (SINR) at D_i can be given as:

$$\gamma_{\mathrm{D}_i}^{x_c} = \frac{\mathcal{Z}_i^2 \alpha_c P_{\mathrm{S}}}{\mathcal{Z}_i^2 (\alpha_1 + \alpha_2) P_{\mathrm{S}} + \gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2}, \tag{3}$$

$$\gamma_{\mathrm{D}_i}^{x_p} = \frac{\mathcal{Z}_i^2 \alpha_p P_{\mathrm{S}}}{\mathcal{Z}_i^2 (\Delta\alpha_c + \alpha_q) P_{\mathrm{S}} + \gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2}, \tag{4}$$

where, $\mathcal{Z}_i = \sqrt{d_{\mathrm{SR}}^{-\beta} d_{\mathrm{RD}_i}^{-\beta}} \sum_{l=1}^{L} a_{\mathrm{SR}_l} a_{\mathrm{R}_l\mathrm{D}_i}, \bar{\gamma}_{\mathrm{JD}_i} = \eta_i P_{\mathrm{J}} d_{\mathrm{JD}_i}^{-\beta}, \gamma_{\mathrm{JD}_i} = \bar{\gamma}_{\mathrm{JD}_i} \left|h_{\mathrm{JD}_i}\right|^2; p, q \in \{1,2\}, p \ne q; \Delta$ denotes the residual interference remaining after imperfect SIC of the common stream [30].

The received signal at E *via* RIS is expressed as:

$$y_{\mathrm{E}} = \left(\sqrt{d_{\mathrm{SR}}^{-\beta} d_{\mathrm{RE}}^{-\beta}} \sum_{l=1}^{L} h_{\mathrm{SR}_l} h_{\mathrm{R}_l\mathrm{E}} e^{j\Psi_l}\right) x_{\mathrm{S}} + \sqrt{P_{\mathrm{J}}} \sqrt{d_{\mathrm{JE}}^{-\beta}} h_{\mathrm{JE}} x_{\mathrm{J}} + z_{\mathrm{E}}. \tag{5}$$

The location of E is assumed to be known and is treated as a predefined system parameter for determining the corresponding large-scale path loss. In practice, such location information may be obtained through preceding detection or rough estimation, as discussed in [40]. The CSI associated with E is assumed to be perfectly known for analytical tractability.[6] To evaluate the system under the worst-case security paradigm, we assume that an eavesdropper E with superior computational capabilities can perform pSIC [41]. In contrast, due to practical implementation impairments, ipSIC and imperfect AJ cancellation may result in residual interference at the legitimate users. Specifically, when decoding the common message x_c, E treats the private messages as interference. After extracting x_c, E completely removes it from the superimposed signal before decoding the private message x_p. Consequently, the corresponding SINRs at E for x_c and x_p are given by:

$$\gamma_{\mathrm{E}}^{x_c} = \frac{\mathcal{Z}_3^2 \alpha_c P_{\mathrm{S}}}{\mathcal{Z}_3^2 (\alpha_1 + \alpha_2) P_{\mathrm{S}} + \gamma_{\mathrm{JE}} + \delta_{\mathrm{E}}^2}, \tag{6}$$

$$\gamma_{\mathrm{E}}^{x_p} = \frac{\mathcal{Z}_3^2 \alpha_p P_{\mathrm{S}}}{\mathcal{Z}_3^2 \alpha_q P_{\mathrm{S}} + \gamma_{\mathrm{JE}} + \delta_{\mathrm{E}}^2}, \tag{7}$$

[4] As discussed in [37], practical finite-resolution RIS phase shifts can be characterized using an average phase-error approximation. For a b-bit RIS, the phase quantization error results in an average attenuation factor given by $\mathbb{E}\{e^{j\Delta\theta_l}\} = \frac{\sin(\pi/2^b)}{\pi/2^b}$, where $b \ge 4$ provides a close approximation to the continuous-phase case.

[5] In practice, the adverse effect of AJ on D_i can be mitigated through effective interference management techniques, such as cooperative cancellation mechanisms, advanced receiver architectures, and optimized system design. The parameter η_i denotes the residual AJ interference coefficient after imperfect AJ cancellation, typically ranging from 0.01 to 0.1 [27, 38]. As reported in [39], cooperative jamming cancellation can achieve approximately 51 dB interference suppression, although imperfect synchronization and channel estimation still introduce residual interference. Consequently, these techniques can effectively mitigate jamming effects and improve the overall system performance.

[6] To assess the robustness of the proposed system against CSI uncertainty, ipCSI is additionally considered in the numerical evaluation for the common S-RIS link, the estimation error of which consequently affects the RIS-assisted links toward both the legitimate user D_i and the eavesdropper E. Specifically, the correlation-based model $\bar{h} = \rho h + \sqrt{1-\rho^2}\tilde{h}$ is adopted, where $\tilde{h}$ denotes an independent channel-estimation error component and $0 < \rho \le 1$ is the CSI correlation coefficient. Thus, $\rho = 1$ corresponds to pCSI, whereas a smaller ρ represents a higher level of CSI uncertainty.

where $\mathcal{Z}_3 = \sqrt{d_{\mathrm{SR}}^{-\beta} d_{\mathrm{RE}}^{-\beta}} \sum_{l=1}^{L} a_{\mathrm{SR}} a_{\mathrm{R}_l\mathrm{E}}; \bar{\gamma}_{\mathrm{JE}} = P_{\mathrm{J}} d_{\mathrm{JE}}^{-\beta}, \gamma_{\mathrm{JE}} = \bar{\gamma}_{\mathrm{JE}} |h_{\mathrm{JE}}|^2$.

Theorem 1 Based on (3), (4), (6), (7) and using the Gaussian-Chebyshev quadrature technique, the cumulative distribution functions (CDFs) of $\gamma_{\mathrm{D}_i}^{x_c}, \gamma_{\mathrm{D}_i}^{x_p}, \gamma_{\mathrm{E}}^{x_c}$, and $\gamma_{\mathrm{E}}^{x_p}$ can be derived as presented in the following theorem.

$$F_{\gamma_{\mathrm{D}_i}^{x_c}}(x) = 1 - \sum_{n=1}^{N_k} \rho_{n_1} \Gamma\left(\theta, \upsilon_{\mathrm{D}_i} \sqrt{\frac{x}{P_{\mathrm{S}}(\alpha_c - (\alpha_1 + \alpha_2)x)}}\right), \tag{8}$$

$$F_{\gamma_{\mathrm{D}_i}^{x_p}}(x) = 1 - \sum_{n_2=1}^{N_k} \rho_{n_2} \Gamma\left(\theta, \upsilon_{\mathrm{D}_i} \sqrt{\frac{x}{P_{\mathrm{S}}(\alpha_p - (\Delta\alpha_c + \alpha_q)x)}}\right), \tag{9}$$

$$F_{\gamma_{\mathrm{E}}^{x_c}}(x) = 1 - \sum_{n_3=1}^{N_k} \rho_{n_3} \Gamma\left(\theta, \upsilon_{\mathrm{E}} \sqrt{\frac{x}{P_{\mathrm{S}}(\alpha_c - (\alpha_1 + \alpha_2)x)}}\right), \tag{10}$$

$$F_{\gamma_{\mathrm{E}}^{x_p}}(x) = 1 - \sum_{n_4=1}^{N_k} \rho_{n_4} \Gamma\left(\theta, \upsilon_{\mathrm{E}} \sqrt{\frac{x}{P_{\mathrm{S}}(\alpha_p - \alpha_q x)}}\right), \tag{11}$$

where $\upsilon_{\mathrm{D}_i} = \frac{1}{\phi_{\mathrm{D}_i}} \sqrt{\frac{1}{\lambda_{\mathrm{JD}_i}} \ln \frac{2}{V_{\mathrm{n}_i}+1} + \delta_{\mathrm{D}_i}^2}, \rho_{n_1} = \frac{\pi \sqrt{1 - V_{n_1}{}^2}}{2N_k \Gamma(\theta)}, \rho_{n_2} = \frac{\pi \sqrt{1 - V_{n_2}{}^2}}{2N_k \Gamma(\theta)}, \upsilon_{\mathrm{E}} = \frac{1}{\phi_{\mathrm{E}}} \sqrt{\frac{1}{\lambda_{\mathrm{JE}}} \ln \frac{2}{V_{n_3}+1} + \delta_{\mathrm{E}}^2}, \rho_{n_3} = \frac{\pi \sqrt{1 - V_{n_3}{}^2}}{2N\Gamma(\theta)}$, and $\rho_{n_4} = \frac{\pi \sqrt{1 - V_{n_4}{}^2}}{2N_k \Gamma(\theta)}, 0 \le x < \min\left\{\frac{\alpha_c}{\alpha_1 + \alpha_2}, \frac{\alpha_p}{\Delta\alpha_c + \alpha_q}, \frac{\alpha_p}{\alpha_q}\right\}$.

Proof. The proof is given in Appendix A.

3. PERFORMANCE ANALYSIS

3.1 Outage Probability (OP) and Intercept Probability (IP)

In this sub-section, the OP of the considered RIS-RSMA system with AJ is investigated. For legitimate user D_i, an outage event occurs when the common stream x_c or the corresponding private stream x_p cannot be successfully decoded. Accordingly, the outage event at D_i is formulated in terms of the joint successful decoding probability as [30, 42].

$$\begin{aligned} \mathrm{OP}^{\mathrm{D}_i} &= \Pr\left\{\gamma_{\mathrm{D}_i}^{x_c} < \gamma_{\mathrm{th}}^{x_c} \cup \gamma_{\mathrm{D}_i}^{x_p} < \gamma_{\mathrm{th}}^{x_p}\right\} = \Pr\{\mathcal{Z}_i < \Omega_1 \cup \mathcal{Z}_1 < \Omega_2\} \\ &= \Pr\{\mathcal{Z}_i < \max\{\Omega_1, \Omega_2\}\}, \end{aligned} \tag{12}$$

where $\gamma_{\mathrm{th}}^{x_c} = 2^{R_c} - 1$ and $\gamma_{\mathrm{th}}^{x_p} = 2^{R_p} - 1$ represent the target SINR thresholds required to successfully decode the common and private signals, respectively, with R_c and R_p being their corresponding target data rates, $\Omega_1 = \sqrt{\frac{(\gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2)\gamma_{\mathrm{th}}^{x_c}}{P_{\mathrm{S}}(\alpha_c - (\alpha_1 + \alpha_2)\gamma_{\mathrm{th}}^{x_c})}}, \Omega_2 = \sqrt{\frac{(\gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2)\gamma_{\mathrm{th}}^{x_p}}{P_{\mathrm{S}}(\alpha_p - (\Delta\alpha_c + \alpha_q)\gamma_{\mathrm{th}}^{x_p})}}, \gamma_{\mathrm{th}}^{x_c} < \frac{\alpha_c}{\alpha_1 + \alpha_2}$ and $\gamma_{\mathrm{th}}^{x_p} < \frac{\alpha_p}{\Delta\alpha_c + \alpha_q}$.

From (12), the OP is rewritten as:

$$\mathrm{OP}^{\mathrm{D}_i} = \begin{cases} \Pr\{\mathcal{Z}_1 < \Omega_1\}, \dfrac{\gamma_{\mathrm{th}}^{x_c}}{\alpha_c - (\alpha_1 + \alpha_2)\gamma_{\mathrm{th}}^{x_c}} > \dfrac{\gamma_{\mathrm{th}}^{x_p}}{(\alpha_p - (\Delta\alpha_c + \alpha_q)\gamma_{\mathrm{th}}^{x_p}}, \\ \Pr\{\mathcal{Z}_1 < \Omega_2\}, \dfrac{\gamma_{\mathrm{th}}^{x_c}}{\alpha_c - (\alpha_1 + \alpha_2)\gamma_{\mathrm{th}}^{x_c}} \le \dfrac{\gamma_{\mathrm{th}}}{(\alpha_p - (\Delta\alpha_c + \alpha_q)\gamma_{\mathrm{th}}^{x_p})}. \end{cases} \tag{13}$$

The OP expression can be obtained by substituting (8) and (9) into (13) as follows:

$$\mathrm{OP}^{\mathrm{D}_i} \approx \begin{cases} 1-\sum_{n=1}^{N_k} \rho_{n_1} \Gamma\left(\theta, \mho_{\mathrm{D}_i} \sqrt{\frac{\gamma_{\mathrm{th}}^{x_c}}{P_{\mathrm{S}}\left(\alpha_c-(\alpha_1+\alpha_2)\gamma_{\mathrm{th}}^{x_c}\right)}}\right), \frac{\gamma_{\mathrm{th}}^{x_c}\left(1+\gamma_{\mathrm{th}}^{x_p}\right)}{\gamma_{\mathrm{th}}^{x_p}\left(1+\Delta\gamma_{\mathrm{th}}^{x_c}\right)} > \frac{\alpha_c}{\alpha_p}, \\ 1-\sum_{n_2=1}^{N_k} \rho_{n_2} \Gamma\left(\theta, \mho_{\mathrm{D}_i} \sqrt{\frac{\gamma_{\mathrm{th}}^{x_p}}{P_{\mathrm{S}}\left(\alpha_p-\left(\Delta\alpha_c+\alpha_q\right)\gamma_{\mathrm{th}}^{x_p}\right)}}\right), \frac{\gamma_{\mathrm{th}}^{x_c}\left(1+\gamma_{\mathrm{th}}^{x_p}\right)}{\gamma_{\mathrm{th}}^{x_p}\left(1+\Delta\gamma_{\mathrm{th}}^{x_c}\right)} \leq \frac{\alpha_c}{\alpha_p}. \end{cases} \tag{14}$$

It follows from (12)-(14) that the decoding bottleneck is determined by the larger effective threshold between Ω_1 and Ω_2. Specifically, the common stream becomes the bottleneck when $\Omega_1 > \Omega_2$, whereas the corresponding private stream becomes the bottleneck when $\Omega_2 > \Omega_1$; when $\Omega_1 = \Omega_2$, both decoding requirements are equally restrictive. Hence, the bottleneck is not fixed to a particular stream, but depends on the target SINR thresholds, power allocation coefficients, and residual interference level.

The IP of the considered system is given by [27, 42].

$$\begin{aligned} \mathrm{IP}^{x_i} &= \Pr\left\{\gamma_{\mathrm{E}^{x_c}} \geq \gamma_{\mathrm{th}}^{x_c} \cap \gamma_{\mathrm{E}_{x_i}^{x_p} \geq \gamma_{\mathrm{th}}^{x_p}}\right\}, = \Pr\{\mathcal{Z}_3 \geq \Omega_3 \cap \mathcal{Z}_3 \geq \Omega_4\}, \\ &= \Pr\{\mathcal{Z}_3 \geq \max\{\Omega_3, \Omega_4\}\} \end{aligned} \tag{15}$$

where $\Omega_3 = \sqrt{\frac{\left(\gamma_{\mathrm{JE}}+\delta_{\mathrm{E}}^2\right)\gamma_{\mathrm{th}}^{x_c}}{P_{\mathrm{S}}\left(\alpha_c-(\alpha_1+\alpha_2)\gamma_{\mathrm{th}}^{x_c}\right)}}, \Omega_4 = \sqrt{\frac{\left(\gamma_{\mathrm{JE}}+\delta_{\mathrm{E}}^2\right)\gamma_{\mathrm{th}}^{x_p}}{P_{\mathrm{S}}\left(\alpha_p-\alpha_q\gamma_{\mathrm{th}}^{x_p}\right)}}, \gamma_{\mathrm{th}}^{x_c} < \frac{\alpha_c}{\alpha_1+\alpha_2}$ and $\gamma_{\mathrm{th}}^{x_p} < \frac{\alpha_p}{\alpha_q}$.

From (15), an IP is rewritten as:

$$\mathrm{IP}^{x_i} = \begin{cases} \Pr\{\mathcal{Z}_3 \geq \Omega_3\}, \frac{\gamma_{\mathrm{th}}^{x_c}}{\alpha_c-(\alpha_1+\alpha_2)\gamma_{\mathrm{th}}^{x_c}} > \frac{\gamma_{\mathrm{th}}^{x_p}}{\alpha_p-\alpha_q\gamma_{\mathrm{th}}^{x_p}}, \\ \Pr\{\mathcal{Z}_3 \geq \Omega_4\}, \frac{\gamma_{\mathrm{th}}^{x_c}}{\alpha_c-(\alpha_1+\alpha_2)\gamma_{\mathrm{th}}^{x_c}} \leq \frac{\gamma_{\mathrm{th}}^{x_p}}{\alpha_p-\alpha_q\gamma_{\mathrm{th}}^{x_p}}. \end{cases} \tag{16}$$

By exploiting the probability identity $\Pr(Z \geq z) = 1 - \Pr(Z < z) = 1 - F_Z(z)$, together with the results in (10) and (11), the IP expression in the presence of jamming can be derived.

$$\mathrm{IP}^{x_i} \approx \begin{cases} \sum_{n_3=1}^{N_k} \rho_{n_3} \Gamma\left(\theta, \mho_{\mathrm{E}} \sqrt{\frac{\gamma_{\mathrm{th}}^{x_c}}{P_{\mathrm{S}}\left(\alpha_c-(\alpha_1+\alpha_2)\gamma_{\mathrm{th}}^{x_c}\right)}}\right), & \frac{\gamma_{\mathrm{th}}^{x_c}}{\gamma_{\mathrm{th}}^{x_p}} + \gamma_{\mathrm{th}}^{x_c} > \frac{\alpha_c}{\alpha_p}, \\ \sum_{n_4=1}^{N_k} \rho_{n_4} \Gamma\left(\theta, \mho_{\mathrm{E}} \sqrt{\frac{\gamma_{\mathrm{th}}^{x_p}}{P_{\mathrm{S}}\left(\alpha_p-\alpha_q\right)\gamma_{\mathrm{th}}^{x_p}}}\right), & \frac{\gamma_{\mathrm{th}}^{x_c}}{\gamma_{\mathrm{th}}^{x_p}} + \gamma_{\mathrm{th}}^{x_c} \leq \frac{\alpha_c}{\alpha_p}. \end{cases} \tag{17}$$

3.2 SRT Analysis

To evaluate the secrecy-reliability trade-off (SRT) of the proposed system, the SRT metric is defined as the probability that either an outage event or an intercept event takes place. Therefore, the SRT at D_i is formulated as follows [43].

$$\begin{aligned} \mathrm{SRT}^{\mathrm{D}_i} &= 1 - \Pr\left\{\gamma_{\mathrm{D}_i}^{x_c} \geq \gamma_{\mathrm{th}}^{x_c} \cap \gamma_{\mathrm{D}_i}^{x_p} \geq \gamma_{\mathrm{th}}^{x_p}, \gamma_E^{x_c} < \gamma_{\mathrm{th}}^{x_c} \cup \gamma_{E_{x_i}}^{x_p} < \gamma_{\mathrm{th}}^{x_p}\right\} \\ &\overset{(a)}{\approx} 1 - \Pr\left\{\gamma_{\mathrm{D}_i}^{x_c} \geq \gamma_{\mathrm{th}}^{x_c} \cap \gamma_{\mathrm{D}_i}^{x_p} \geq \gamma_{\mathrm{th}}^{x_p}\right\} \Pr\left\{\gamma_E^{x_c} < \gamma_{\mathrm{th}}^{x_c} \cup \gamma_{E_{x_i}}^{x_p} < \gamma_{\mathrm{th}}^{x_p}\right\} \\ &= 1 - \left(1 - \mathrm{OP}^{\mathrm{D}_i}\right)\left(1 - \mathrm{IP}^{x_i}\right). \end{aligned} \tag{18}$$

with the OP defined in (14) and the IP defined in (17).

It is worth noting that the effective $S-$ RIS $-\mathrm{D}_i$ and $S-$ RIS-E cascaded channels are not strictly independent, since they share the common RVs $\{|h_{\mathrm{SR}_l}|\}$. Therefore, following [44, Eq. (45)], the two effective cascaded channel gains are treated as independent RVs for analytical tractability, leading to the independence-based approximation in (18), as indicated by (a).

Similarly, the overall system SRT can be approximated as [43]:

$$\mathrm{SRT}^{\mathrm{Sys}} \approx 1-\left(1-\mathrm{OP}^{\mathrm{Sys}}\right)\left(1-\mathrm{IP}^{\mathrm{Sys}}\right), \tag{19}$$

where $\mathrm{OP}^{\mathrm{Sys}} = 1-\left(1-\mathrm{OP}^{\mathrm{D}_1}\right)\left(1-\mathrm{OP}^{\mathrm{D}_2}\right), \mathrm{IP}^{\mathrm{Sys}} = 1-(1-\mathrm{IP}^{x_1})(1-\mathrm{IP}^{x_2})$.

Remark 1 From (14), (17), (18) and (19), it can be observed that an inherent trade-off always exists between OP and IP, which is also investigated in this work. Specifically, improving the OP performance generally requires increasing the transmit power at the source node S. However, such an increase in transmit power may simultaneously deteriorate the IP performance. Moreover, increasing the number of L enhances the RIS-assisted links of both the legitimate users and Eve, and hence does not necessarily improve the overall secrecy-reliability performance. Imperfect SIC and imperfect AJ cancellation further introduce residual interference at the legitimate users, thereby degrading their decoding reliability. Therefore, the SRT is governed by competing reliability and security effects, indicating that suitable operating points of P_{S}, L, and the power allocation coefficients are required rather than simply increasing these parameters.

3.3 Average Secrecy Capacity (ASC)

The ASC represents the mean instantaneous secrecy capacity over the channel fading realizations and is given by [27, 45]:

$$\mathrm{ASC}_{x_i} = \left[\mathbb{E}\{\log_2\left(1+\gamma_{\mathrm{D}_i}\right)\} - \mathbb{E}\{\log_2\left(1+\gamma_{\mathrm{E}^{x_i}}\right)\}\right]^+, = \left[\mathbb{E}\{\mathrm{C}_{\mathrm{D}_i}\} - \mathbb{E}\{\mathrm{C}_{\mathrm{E}^{x_i}}\}\right]^+, \tag{20}$$

where γ_{D_i} and $\gamma_{\mathrm{E}^{x_i}}$ are given in (6) and (7), respectively. Here, $[x]^+ = \max\{x, 0\}$, and $\mathbb{E}\{C_{\mathrm{D}_i}\}$ and $\mathbb{E}\{C_{\mathrm{E}_i}\}$ denote the average capacities of the legitimate users and the eavesdropper, respectively, given by:

$$\overline{\mathrm{C}}_{\mathrm{D}_i} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-F_{\gamma_{\mathrm{b}_i}}(x)}{1+x}\,dx, \tag{21}$$

$$\overline{\mathrm{C}}_{\mathrm{E}^{x_i}} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-F_{\gamma_{\mathrm{E}}^{x_i}}(x)}{1+x}\,dx, \tag{22}$$

where $F_{\gamma_{\mathrm{D}}}(x)$, and $F\gamma_{\mathrm{E}^{x_i}}(x)$ are the CDFs of SINR at D_i, and E, respectively.

By substituting (8) into (21), the average capacity associated with the common streams at D_i are obtained as follows:

$$\overline{\mathrm{C}}_{\mathrm{D}_i^c} = \frac{1}{\ln 2}\sum_{n_1=1}^{N_k} \rho_{n_1}\int_0^{\frac{\alpha_c}{\alpha_1+\alpha_2}} \frac{1}{1+x}\Gamma\left(\theta, \mho_{\mathrm{D}_i}\sqrt{\frac{x}{P_{\mathrm{S}}(\alpha_c-(\alpha_1+\alpha_2)x)}}\right)dx. \tag{23}$$

Using [36] to calculate (23), we have:

$$\overline{\mathrm{C}}_{\mathrm{D}_i^c} = \frac{1}{\ln 2}\sum_{n_1=1}^{N_k}\sum_{n_5=1}^{N_k} \frac{\rho_{n_1}\rho_{n_5}}{1+\varphi_{v_{n_5}}}\Gamma\left(\theta, \mho_{\mathrm{D}_i}\sqrt{\frac{\varphi_{v_{n_5}}}{P_{\mathrm{S}}\left(\alpha_c-(\alpha_1+\alpha_2)\varphi_{v_{n_5}}\right)}}\right), \tag{24}$$

where $\varphi_{v_{n_5}} = \frac{\alpha_c(v_{n_5}+1)}{2(\alpha_1+\alpha_2)}, \rho_{n_5} = \frac{\alpha_c\pi\sqrt{1-v_{n_5}{}^2}}{2(\alpha_1+\alpha_2)N_k}$.

Following the same procedure as that used for $\overline{\mathrm{C}}_{\mathrm{D}_i^c}$, the expressions of $\overline{\mathrm{C}}_{\mathrm{D}_i^p}, \overline{\mathrm{C}}_{\mathrm{E}^c}$, and $\overline{\mathrm{C}}_{\mathrm{E}_{x_i}^p}$ can be respectively obtained as follows:

$$\overline{\mathrm{C}}_{\mathrm{D}_i^p} = \frac{1}{\ln 2}\sum_{n_2=1}^{N_k}\sum_{n_6=1}^{N_k} \frac{\rho_{n_2}\rho_{n_6}}{1+\varphi_{v_{n_6}}}\Gamma\left(\theta, \mho_{\mathrm{D}_i}\sqrt{\frac{\varphi_{v_{n_6}}}{P_{\mathrm{S}}\left(\alpha_p-\left(\Delta\alpha_c+\alpha_q\right)\varphi_{v_{n_6}}\right)}}\right), \tag{25}$$

where $\varphi_{v_{n_6}} = \frac{\alpha_p(v_{n_6}+1)}{2(\alpha_q+\Delta\alpha_c)}, \rho_{n_6} = \frac{\alpha_p\pi\sqrt{1-v_{n_6}{}^2}}{2(\alpha_q+\Delta\alpha_c)N_k}$.

$$\overline{\mathrm{C}}_{\mathrm{E}^c} = \frac{1}{\ln 2}\sum_{n_3=1}^{N_k}\sum_{n_7=1}^{N_k}\frac{\rho_{n_3}\rho_{n_7}}{1+\varphi_{v_{n_7}}}\Gamma\left(\theta, \mho_{\mathrm{E}}\sqrt{\frac{\varphi_{v_{n_7}}}{P_{\mathrm{S}}\left(\alpha_c-(\alpha_1+\alpha_2)\varphi_{v_{n_7}}\right)}}\right), \tag{26}$$

where $\varphi_{v_{n_7}} = \frac{\alpha_c(v_{n_7}+1)}{2(\alpha_1+\alpha_2)}, \rho_{n_7} = \frac{\alpha_c\pi\sqrt{1-v_{n_7}{}^2}}{2(\alpha_1+\alpha_2)N_k}$.

$$\overline{\mathrm{C}}^{p}_{\mathrm{E}_{x_i}} = \frac{1}{\ln 2}\sum_{n_4=1}^{N_k}\sum_{n_8=1}^{N_k}\frac{\rho_{n_4}\rho_{n_8}}{1+\varphi_{v_{n_8}}}\Gamma\left(\theta, \mho_{\mathrm{E}}\sqrt{\frac{\varphi_{v_{n_8}}}{P_{\mathrm{S}}\left(\alpha_p-\alpha_q\varphi_{v_{n_8}}\right)}}\right), \tag{27}$$

where $\varphi_{v_{n_8}} = \frac{\alpha_p(v_{n_8}+1)}{2\alpha_q}, \rho_{n_8} = \frac{\alpha_p\pi\sqrt{1-v_{n_8}{}^2}}{2\alpha_q N_k}$.

To enable correct decoding of x_c at both D_i, the transmit rate is required to contain the following condition [46]:

$$\overline{\mathrm{C}}_{\mathrm{D}^c} = \min\{\overline{\mathrm{C}}_{\mathrm{D}_1^c}, \overline{\mathrm{C}}_{\mathrm{D}_2^c}\}, \tag{28}$$

Based on the ASC definition in [46], the ASC at D_i can be formulated as follows:

$$\mathrm{ASC}_{\mathrm{D}_1} = \varepsilon\overline{\mathrm{C}}_{\mathrm{D}^c} + \overline{\mathrm{C}}_{\mathrm{D}^p_{x_1}} - \varepsilon\overline{\mathrm{C}}_{\mathrm{E}^c} - \overline{\mathrm{C}}_{\mathrm{E}^p_{x_1}} \tag{29}$$

$$\mathrm{ASC}_{\mathrm{D}_2} = (1-\varepsilon)\overline{\mathrm{C}}_{\mathrm{D}^c} + \overline{\mathrm{C}}_{\mathrm{D}^p_{x_2}} - (1-\varepsilon)\overline{\mathrm{C}}_{\mathrm{E}^c} - \overline{\mathrm{C}}_{\mathrm{E}^p_{x_2}}, \tag{30}$$

where ε denotes the shared rate allocation coefficient satisfying $0 \le \varepsilon \le 1$ [46].

Remark 2 According to (29) and (30), the ASC achieved by D_1 and D_2 is significantly affected by a variety of system parameters, including $P_{\mathrm{S}}, P_{\mathrm{J}}$, the power allocation factors, L, the SIC imperfection level, and the imperfect AJ cancellation level at the legitimate users. Specifically, increasing P_{S} or L can improve the legitimate-link rates, but the corresponding secrecy gain may diminish when Eve's received signal is also enhanced. Increasing P_{J} initially improves the ASC by suppressing Eve; however, excessive jamming increases the residual AJ interference at the legitimate users and may consequently degrade the ASC. Moreover, the power allocation coefficients directly control the rates of the common and private streams, whereas imperfect SIC and AJ cancellation reduces the achievable rates of the legitimate users through residual interference. These competing effects indicate that suitable values of $P_{\mathrm{S}}, P_{\mathrm{J}}, L$, and the power allocation coefficients are required to improve the secrecy performance.

4. NUMERICAL RESULTS

In this section, the numerical results are presented to characterize the secrecy performance of the proposed system and to demonstrate the correctness of the analytical results. The simulation experiments are conducted based on 10^6 independently generated Rayleigh fading channel realizations. Unless otherwise specified, the system parameters are adopted from commonly used settings in the literature and are summarized in Table 2. The jammer transmit power is defined as $P_{\mathrm{J}} = \tau P_{\mathrm{S}}$, where $0 < \tau < 1$.

Table 2. System parameter setting.

Notations	Values
P_{S},	0 ~ 40 dBm [30, 45]
$\alpha_c, \mathcal{R}_c$	0.5 ~ 0.9, 0.2 ~ 1.0 bpcu [7]
$\alpha_1, \alpha_2, \mathcal{R}_1, \mathcal{R}_2$	0.5 ~ 0.9, 0.2 ~ 1.0 bpcu [36]
L, η, τ	10 ~ 90 REs, $0.01{,}5 \times 10^{-4}$ [27, 38, 47
$PL_0, \beta_i, \beta_j, \delta^2_{\mathrm{D}_i}, \delta^2_{\mathrm{E}}$	10^{-3}, 2.2,2.5, -90dBm [48, 49]
$d_{\mathrm{S-RIS}}, d_{\mathrm{S-D}_1}, d_{\mathrm{S-D}_2}$	50 m, 90 m, 85 m [27]

$d_{\mathrm{S-E}}, d_{\mathrm{J-D}_1}, d_{\mathrm{J-D}_2}, d_{\mathrm{J-E}}$	$5\sqrt{362}$ m, $5\sqrt{17}$ m, $5\sqrt{26}$ m, 15 m [27]
ε	0.5 [46]
Δ, N_k	0.02, 100 [27, 30

For fair comparison, the transmit power of the non-jammer benchmark is set to $P_{\mathrm{S}}^{\mathrm{NJ}} = (1+\tau)P_{\mathrm{S}}$, ensuring the same total transmit power budget. Unless otherwise stated, $\tau = 5 \times 10^{-4}$ is considered throughout the simulations. Furthermore, the impacts of several key system parameters, including the source transmit power, jammer transmit power, the number of RIS reflecting elements L, RSMA power allocation coefficients, SIC imperfection level, and residual interference caused by imperfect AJ cancellation at the legitimate users, are comprehensively investigated. For ease of presentation, the proposed RIS-assisted RSMA scheme with AJ, the corresponding scheme without AJ, and the RIS-assisted NOMA scheme with AJ are denoted as RSMA, Non-Jammer, and NOMA, respectively. For numerical evaluation, the same residual AJ interference coefficient is assumed for both legitimate users; i.e., $\eta_1 = \eta_2 = \eta$. Unless otherwise specified, the target rates of the common and private streams are set to $\mathcal{R}_c = 0.5$bpcu and $\mathcal{R}_1 = \mathcal{R}_2 = 0.25$ bpcu, respectively. Accordingly, the corresponding target SINR thresholds are $\gamma_{\mathrm{th}}^{x_c} = 2^{\mathcal{R}_c} - 1$ and $\gamma_{\mathrm{th}}^{x_i} = 2^{\mathcal{R}_i} - 1$. Thus, different target SINR thresholds are considered for the common and private streams[7].

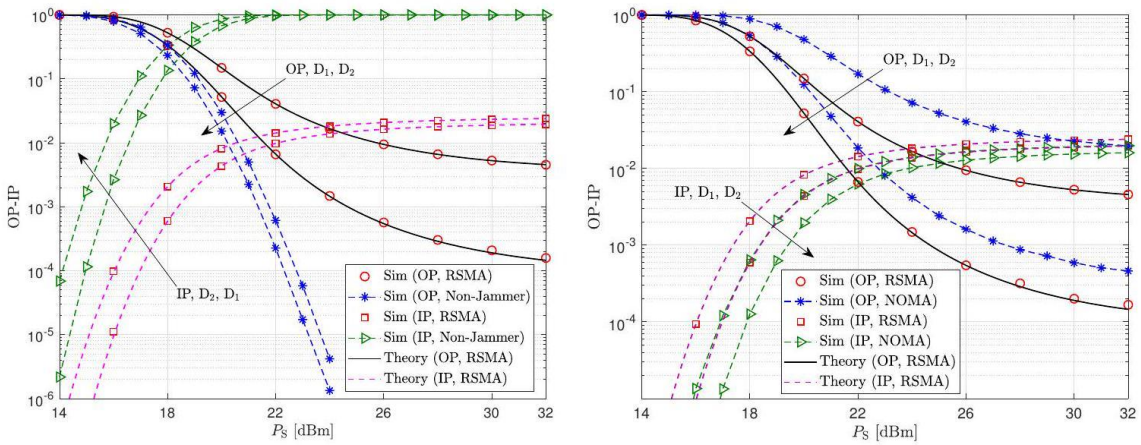


Figure 2. OP and IP *versus* P_{S} with $L = 28$.

Fig. 2 illustrates the OP-IP trade-off of the proposed system *versus* P_{S} with $L = 28$, considering two benchmark cases: (a) the scheme without artificial jamming and (b) the NOMA benchmark. The analytical OP and IP curves corresponding to D_1 and D_2 are plotted based on (14) and (17), respectively. As observed in Fig. 2, the analytical results are in excellent agreement with the simulation results, thereby validating the accuracy of the derived expressions. It can be observed that as P_{S} increases, the OP decreases in both cases, whereas the IP increases. This behavior is attributed to the fact that higher transmit power enhances the channel capacity of both the legitimate and eavesdropping links, thereby leading to an inherent OP-IP trade-off with respect to P_{S}. Moreover, when $P_{\mathrm{S}} > 30$dBm, both the OP performance and IP performance of the proposed system approach saturation. This phenomenon arises because, in the high transmit power regime, the SINRs corresponding to the common and private signal at D_i and E mainly depend on the qualities of the $\mathrm{S} \rightarrow \mathrm{RIS} \rightarrow \{\mathrm{D}_i, \mathrm{E}\}$ and $\mathrm{J} \rightarrow \{\mathrm{D}_i, \mathrm{E}\}$ links, rather than on P_{S}. For the non-jammer case in Fig. 2(a), when $P_{\mathrm{S}} \geq 20$dBm, a lower OP is achieved compared to the proposed system, while the IP approaches unity, indicating a complete loss of secrecy. From Fig. 2 (b), we see that the proposed system achieves superior OP performance compared with the NOMA-based model. In terms of IP, NOMA provides only marginal improvement over RSMA. Overall, the results in Fig. 2 demonstrate that the proposed scheme attains a more favorable OP-IP trade-off than both benchmark schemes.

[7] Code Availability: The MATLAB codes used to generate the numerical and Monte Carlo simulation results are available from the corresponding author upon reasonable request and will be made publicly available if required by the journal's publication policy.

"Secrecy Performance Analysis of RIS-assisted RSMA Systems under Imperfect Artificial Jamming Cancellation and Imperfect SIC," L. H. Luyen, L. T. Dung, T. T. Nguyen and T. M. Hoang.

Fig. 3 presents the impact of the number of L on the OP-IP trade-off of the proposed system for (a) the non-Jammer configuration and (b) the NOMA scheme, with $P_S = 22$dBm. It is observed that as L increases, the OP decreases for both schemes, while the IP tends to increase. This behavior arises, because a larger number of reflecting elements enhances the channel conditions for both legitimate users and the eavesdropper, thereby inducing an inherent trade-off between reliability and secrecy with respect to L. For the non-jammer scheme in Fig. 3(a), a lower OP is achieved compared to the proposed system, while the IP rapidly approaches unity, indicating severe secrecy degradation. However, Fig. 3(b) shows that the proposed system provides superior OP performance relative to the NOMA scheme, while the IP of NOMA is only marginally better. Overall, the results in Fig. 3 demonstrate that the proposed scheme achieves a more favorable OP-IP trade-off than the benchmark schemes.

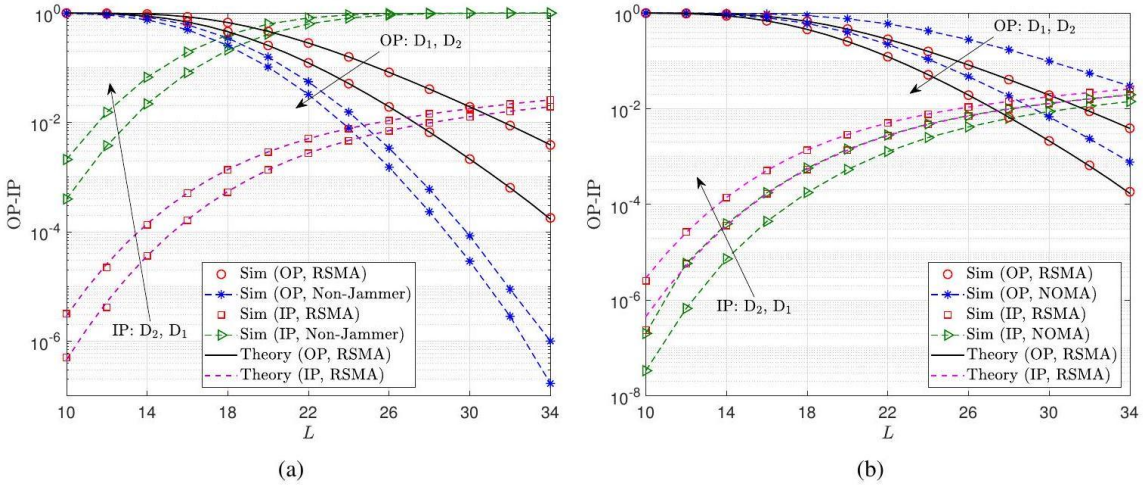


Figure 3. OP and IP *versus* L with $P_S = 22$dBm.

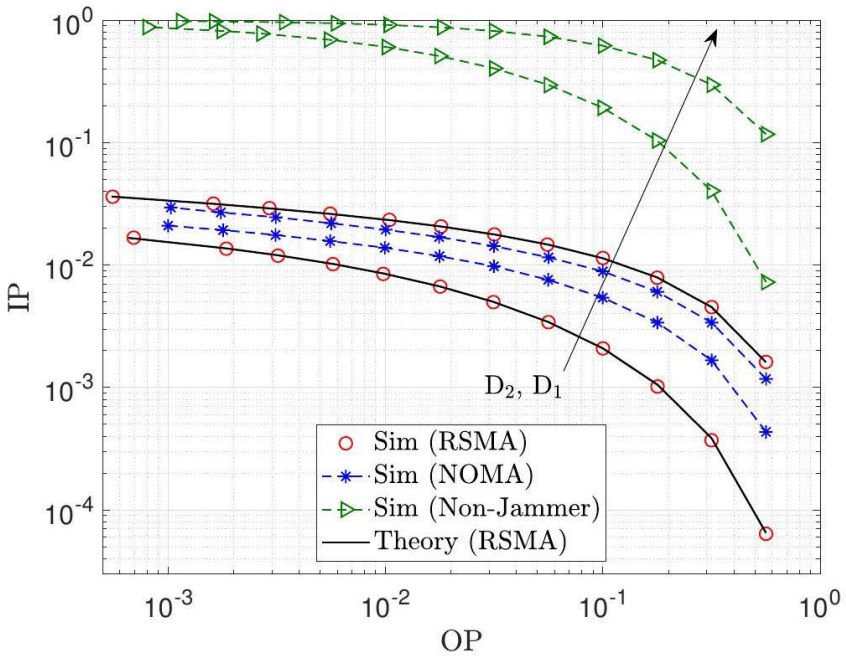


Figure 4. The OP-IP trade-off with $L = 40$.

Fig. 4 shows the OP-IP trade-off achieved by the proposed system with $L = 40$ and compares its performance against the non-jammer and NOMA benchmark schemes. It can be observed that as OP decreases, the IP values of all schemes increase, clearly reflecting the inherent trade-off between reliability and secrecy. Furthermore, for a given OP level, the proposed system consistently achieves lower IP than the non-jammer benchmark, indicating a notable enhancement in secrecy performance. For the NOMA scheme, the OP-IP trade-off for user D_1 shows only marginal improvement over RSMA, whereas RSMA provides a more favorable trade-off for user D_2. Overall, the results in Fig. 4 further

confirm that the proposed scheme attains a more efficient OP-IP trade-off compared with both the Non-jammer and NOMA schemes.

Fig. 5 shows the impact of the transmit power P_S on the SRT of the proposed system, in comparison with the non-jammer and NOMA schemes for $L = 40$. The analytical curves of the SRT of D_1, D_2, and system (Sys) for the proposed system are plotted from (18) and (19). As illustrated in Fig. 5, the analytical results closely match the simulation results, confirming the accuracy of the derived expressions. The results indicate that the proposed scheme consistently achieves superior SRT performance over the benchmark models across the entire range considered. Moreover, each curve exhibits a distinct minimum point, implying the existence of an optimal P_S that minimizes the SRT. However, this optimal value cannot be expressed in a closed form. Therefore, the Golden Section Search (GSS) method [43, 50, 51] is employed to determine the optimal solution through an iterative procedure, with the results summarized in Algorithm 1[8]. The obtained optimal values are in close agreement with the theoretical analysis. It should be emphasized that the GSS is applied separately to each scalar design parameter rather than jointly optimizing multiple parameters. For each optimization, the remaining system parameters are fixed according to the corresponding simulation setting. Hence, each considered optimization reduces to a one-dimensional search problem. These findings provide useful guidelines for selecting an appropriate P_S in practical system design and deployment.

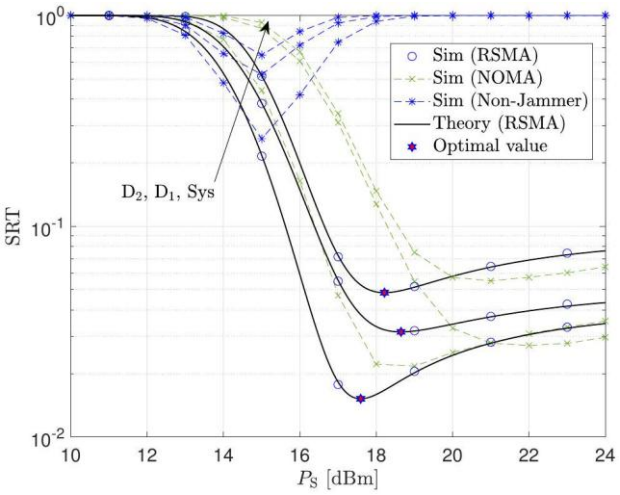


Figure 5. SRT as a function of P_S with $L = 40$.

Fig. 6 illustrates the SRT performance *versus* α_c for the proposed and non-jammer schemes under $L = 55,60,65$, and 70, with $P_S = 14$dBm and $\tau = 3 \times 10^{-4}$. The remaining power allocation coefficients are set as $\alpha_1 = 0.6(1 - \alpha_c)$ and $\alpha_2 = 0.4(1 - \alpha_c)$. The results indicate that the proposed system consistently achieves lower SRT than the non-jammer scheme over the entire range considered. Consistent with the trend observed in Fig. 5, each curve exhibits a distinct minimum, indicating the existence of an optimal α_c that minimizes the SRT. To determine the optimal α_c, the same one-dimensional GSS procedure is applied by using α_c as the search variable while keeping the remaining system parameters fixed. Furthermore, as the number of RIS reflecting elements increases, the corresponding optimal α_c gradually approaches unity. This behavior suggests that, as L becomes large, the optimal power allocation coefficient α_c^* gradually shifts toward higher values. The enhanced beamforming gain provided by the RIS significantly improves the reliability of common-stream decoding at the legitimate users, making a higher common-stream power allocation more favorable. Meanwhile, the secrecy advantage provided by the private streams gradually diminishes, since the eavesdropping channel quality at E is also enhanced as L increases. Consequently, the minimum SRT is achieved at progressively larger values of α_c.

[8] To simplify the optimization process and maintain manageable computational complexity, the considered optimization problems are formulated in a reduced one-dimensional form, where GSS is applied separately to each scalar design parameter while the remaining parameters are fixed. This approach also enables the individual impact of each design parameter on the secrecy performance to be clearly identified. However, the resulting one-dimensional optima do not necessarily coincide with the joint optimum over all design parameters. Joint multi-parameter optimization is therefore left for future work.

Fig. 7 shows the SRT performance *versus* L for the proposed, non-jammer, and NOMA schemes with $P_S = 15$ dBm. Consistent with the previous results, the proposed system consistently achieves lower SRT than the benchmark approaches over the entire range considered. Furthermore, each curve exhibits a distinct minimum point, indicating the existence of an optimal L that minimizes the SRT. This behavior suggests that increasing the number of RIS reflecting elements does not always improve secrecy performance, since both the legitimate and eavesdropping links are simultaneously enhanced as L increases. Therefore, an appropriate value of L should be selected to achieve an effective balance between reliability and secrecy. The optimal L is determined using the same one-dimensional GSS framework, while keeping the remaining system parameters fixed. Since the number of RIS reflecting elements must be integer-valued in practice, the continuous GSS solution is used to identify the optimal region, after which the neighboring integer values are evaluated to determine the final optimal L.

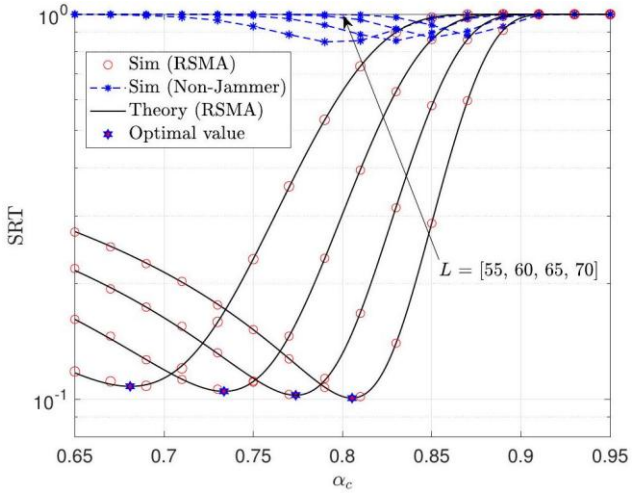


Figure 6. Impact of α_c on SRT for $L = 55,60,65,70$.

Algorithm 1. Golden section search for SRT minimization

Input: Establish $P_{S_{min}} = 10$dBm, $P_{S_{max}} = 24$dBm, the golden section search $\kappa = \frac{\sqrt{5}-1}{2}$, and a stopping threshold $v = 10^{-3}$.
Output: Optimal transmit power $P_S{}^*$ minimizing the SRT.
Begin:
1. Initialize: $\vartheta_1 = P_{S_{max}} - (P_{Smax} - P_{Smin})\kappa$
   $\vartheta_2 = P_{S_{min}} + (P_{S_{max}} - P_{S_{min}})\kappa$
2. **While** $P_{Smax^-} - P_{S_{min}} \geq v$ **do**
   Compute: SRT(ϑ_1) and SRT(ϑ_2).
   If SRT(ϑ_1) < SRT(ϑ_2) **then**
   Update: $P_{S_{max}} \leftarrow \vartheta_2$.
   Else
   Update: $P_{S_{min}} \leftarrow \vartheta_1$.
   End If.
3. **End While**.
4. Return $P_S{}^* = \frac{P_{S_{max}} + P_{S_{min}}}{2}$.

End.

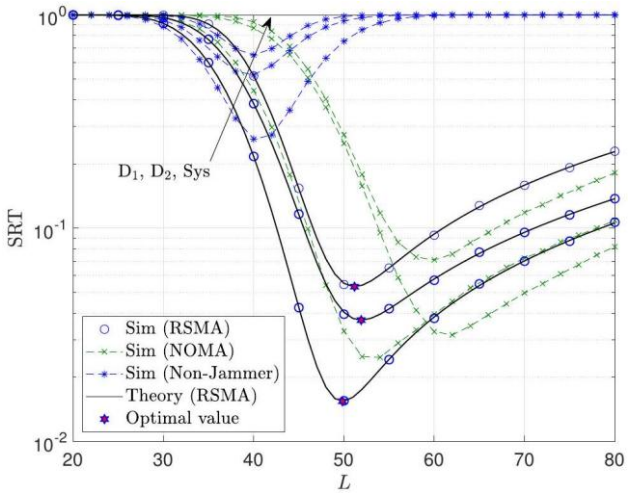


Figure 7. Impact of L on SRT for $P_S = 15$dBm.

Fig. 8 presents the ASC_{Sum} of the proposed system *versus* P_J for $P_S = 30,35$, and 40 dBm, with $L = 80$. The results show that, for each transmit power level P_S, there exists an optimal value of P_J that maximizes the ASC_{Sum}. This behavior can be explained as follows: As P_J increases, the eavesdropping capability at E is gradually suppressed, thereby improving the secrecy performance of the system. However, when the jamming power exceeds the optimal region, the signal quality at the legitimate users becomes significantly degraded, resulting in a reduction in the ASC. This phenomenon reflects the trade-off between suppressing the eavesdropping link and preserving the transmission quality of the legitimate links when selecting the jamming power. For each fixed value of P_S, the optimal P_J is independently determined by applying the one-dimensional GSS procedure in Algorithm 2. while keeping the remaining system parameters fixed. Furthermore, the obtained optimal solutions are in close agreement with the theoretical analysis. Specifically, when P_S is set to 30, 35 and 40 dBm, the maximum ASC_{Sum} values achieved are 2.9, 2.93, and 2.94, corresponding to the optimal P_J values of 1.9, 6.9, and 11.91 dBm, respectively.

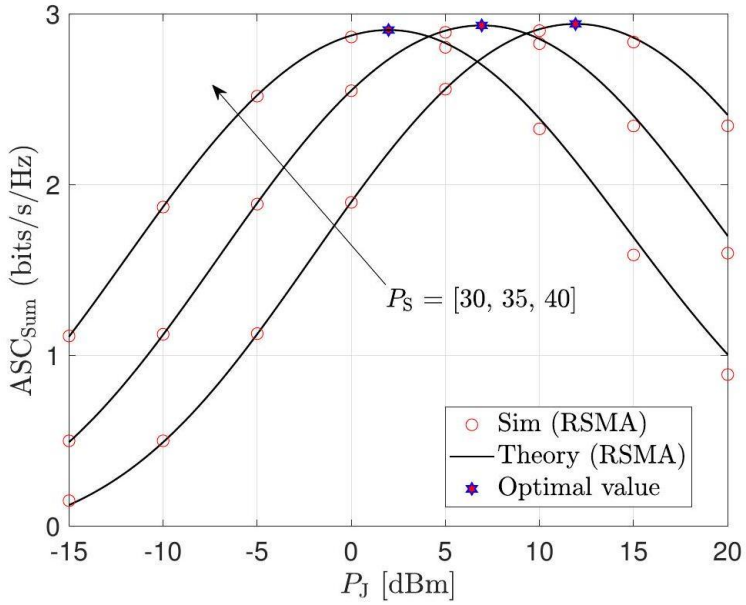


Figure 8. Impact of P_J on ASC_{Sum} for $L = 80$ and $P_{PB} = 30,35,40$dBm.

Algorithm 2. GSS-based optimization for ASC_{Sum} maximization

Input: Establish $P_{\mathrm{J}_{\min}} = -15\mathrm{dBm}, P_{\mathrm{J}_{\max}} = 20\mathrm{dBm}$, the golden section search $\kappa = \frac{\sqrt{5}-1}{2}$, and a stopping threshold $v = 10^{-3}$.
Output: Optimal jammer transmit power P_{J}^{*} maximizing the $\mathrm{ASC}_{\mathrm{sum}}$.
Begin:
1. Initialize: $\vartheta_1 = P_{\mathrm{J}_{\max}} - (P_{\mathrm{J}_{\max}} - P_{\mathrm{J}_{\min}})\kappa$
$\vartheta_2 = P_{\mathrm{J}_{\min}} + (P_{\mathrm{J}_{\max}} - P_{\mathrm{J}_{\min}})\kappa$
2. **While** $P_{\mathrm{J}_{\max}} - P_{\mathrm{J}_{\min}} \geq v$ **do**
Compute: $\mathrm{ASC}_{\mathrm{sum}}(\vartheta_1)$ and $\mathrm{ASC}_{\mathrm{sum}}(\vartheta_2)$.
If $\mathrm{ASC}_{\mathrm{sum}}(\vartheta_1) > \mathrm{ASC}_{\mathrm{sum}}(\vartheta_2)$ then
Update: $P_{\mathrm{J}_{\max}} \leftarrow \vartheta_2$.
Else
Update: $P_{\mathrm{J}_{\min}} \leftarrow \vartheta_1$.
End If.
3. **End While**.
4. Return $P_{\mathrm{J}}{}^{*} = \frac{P_{\max} + P_{\min}}{2}$.
End.

Fig. 9 illustrates the $\mathrm{ASC}_{\mathrm{Sum}}$ of the proposed system for $L = 35$ and $L = 55$. The analytical curves of $\mathrm{ASC}_{\mathrm{Sum}}$ are obtained from (29) and (30). As shown in Fig. 9, the analytical results are in excellent agreement with the simulation results, thereby confirming the accuracy of the derived expressions. The results further demonstrate that the proposed system consistently achieves significantly higher ASC than that of the non-jammer scheme over the entire range considered. Compared with the NOMA scheme, NOMA provides higher ASC than RSMA in the low transmit power region (0-15 dBm). However, when $P_{\mathrm{S}} > 15\mathrm{dBm}$, the RSMA-based system begins to exhibit clear superiority and achieves better secrecy performance than NOMA. Furthermore, increasing the number of L substantially improves the ASC performance of the system, thereby highlighting the effectiveness of RIS in enhancing the secrecy performance of the proposed framework.

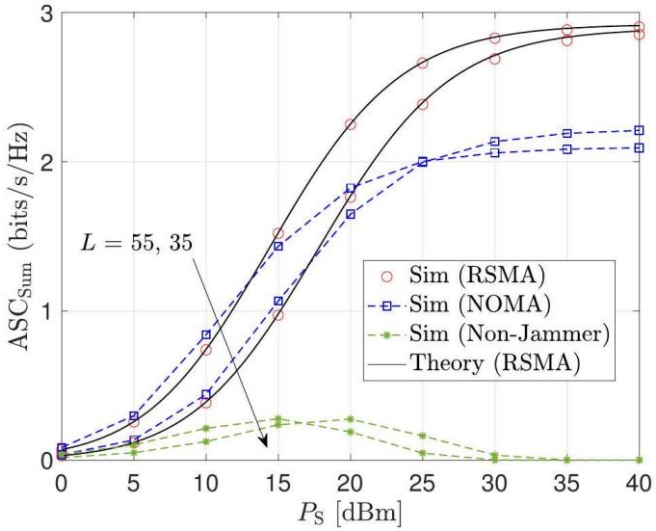


Figure 9. $\mathrm{ASC}_{\mathrm{Sum}}$ as a function of P_{S} for $L = 35{,}55$.

Fig. 10 presents the $\mathrm{ASC}_{\mathrm{Sum}}$ performance of the proposed, NOMA, and non-jammer schemes under different AJ cancellation and SIC conditions. Specifically, Fig. 10(a) considers $\eta = 0$ and $\eta = 0.01$ with $L = 10$ and $L = 30$, whereas Fig. 10(b) examines pSIC and ipSIC scenarios ($\Delta = 0$ and 0.02) for $L = 15{,}20$, and 30. As shown in Fig. 10(a), perfect AJ cancellation achieves higher ASC than the imperfect AJ cancellation case ($\eta = 0.01$). This performance gap is particularly pronounced when $L = 10$. However, when L increases to 30, the difference between the two cases becomes negligible. This observation indicates that increasing L can effectively mitigate the impact of residual interference and further enhance the secrecy performance of the system. In addition, consistent with the trend observed in Fig. 9, the proposed scheme achieves significantly higher ASC than the NOMA scheme in the high

transmit power region ($P_S > 20$dBm). For Fig. 10(b), the pSIC case consistently provides better ASC performance than the ipSIC scenario, especially in the high transmit power region. This behavior is attributed to the impact of residual interference arising from the common-stream separation process during private-stream decoding. Moreover, the considered system consistently achieves better ASC performance than the non-jammer scheme. Overall, the results in Fig. 10 confirm that effective AJ cancellation at the legitimate users, together with efficient SIC processing, are essential for fully exploiting the secrecy advantages of RSMA-RIS-AJ systems.

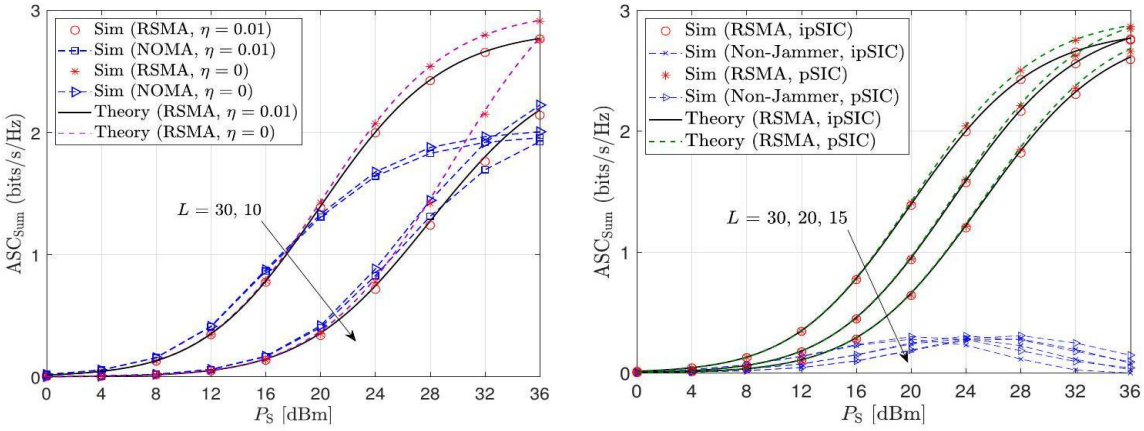


Figure 10. Impact of practical imperfections on $\mathrm{ASC}_{\mathrm{Sum}}$: (a) residual AJ interference coefficient η; (b) SIC imperfection coefficient Δ for ipSIC and pSIC.

Fig. 11 illustrates the effect of the RIS phase resolution b on $\mathrm{ASC_{Sum}}$ for $L = 40,50$, and 60. A significant increase in $\mathrm{ASC_{Sum}}$ is observed as b increases from 1 to 3 , whereas further increasing b yields only marginal gains for all considered values of L. This behavior results from the progressive reduction in the phase mismatch among the reflected components, which improves their coherent combination at the legitimate users. In particular, the curves become nearly flat from approximately $b = 4$ onward, showing that additional phase levels provide only a limited secrecy-capacity benefit. Fig. 11 further demonstrates that a larger L yields a higher $\mathrm{ASC_{Sum}}$ throughout the considered range of b, while the three curves exhibit a similar convergence trend with respect to the phase resolution. Therefore, a relatively small number of quantization bits can capture most of the ASC improvement observed with increasing phase resolution, whereas further increasing b offers diminishing returns.

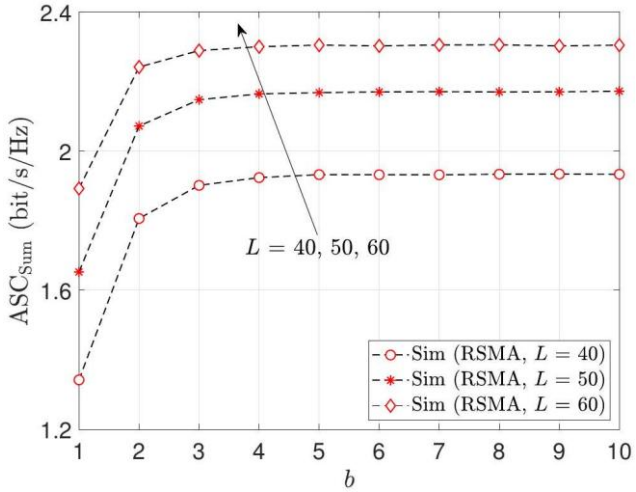


Figure 11. $\mathrm{ASC_{Sum}}$ *versus* the RIS phase resolution b for $L = 40,50,60$ and $P_S = 20$dBm.

To further investigate the impact of the system geometry, Fig. 12 illustrates $\mathrm{ASC_{Sum}}$ versus the jammer position x_J for $L = 30,50,70$, and $P_S = 20$dBm. The results show that $\mathrm{ASC_{Sum}}$ varies noticeably with x_J and exhibits an optimal region the location of which depends on L. This behavior results from the trade-off between suppressing the eavesdropping link and limiting the residual AJ interference at the

legitimate users. In particular, moving the jammer closer to E strengthens the jamming effect on the eavesdropper, whereas the corresponding change in the J-D_i links may also increase the residual AJ interference at the legitimate users. Therefore, the originally considered jammer position $(x_J = 110\ \text{m})$ is not necessarily optimal for all considered system configurations, and the secrecy performance depends on the overall system geometry. In addition, RSMA consistently achieves a higher ASC $_{\text{Sum}}$ than NOMA for the same L, while increasing L generally improves the secrecy performance, consistent with the preceding results. These results demonstrate that the secrecy benefit of AJ is maintained over a range of jammer locations rather than being restricted to a single fixed geometric configuration.

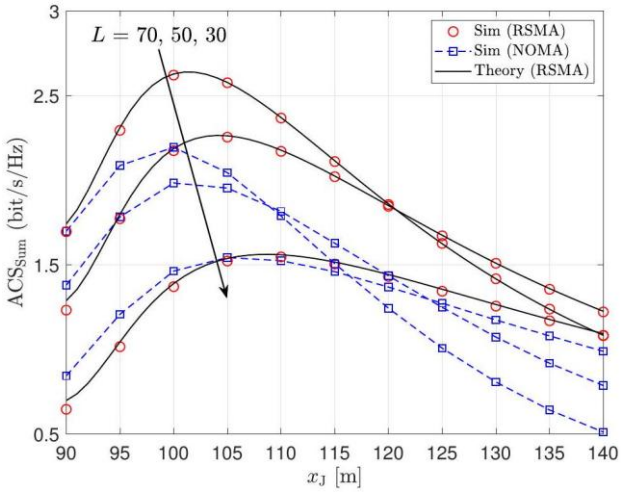


Figure 12. ASC_{Sum} *versus* x_J for different L at $P_S = 20\text{dBm}$.

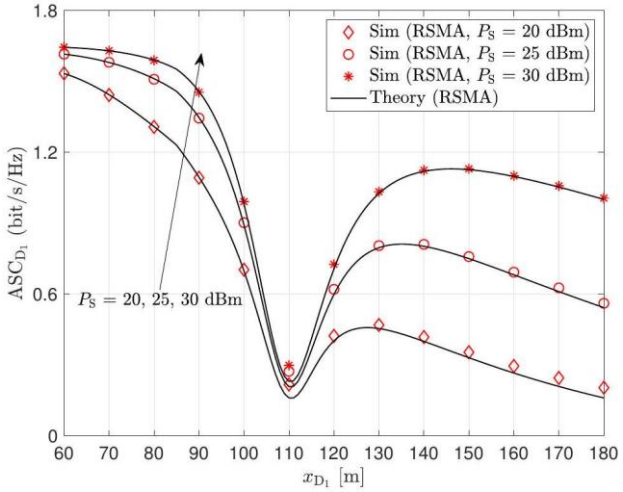


Figure 13. ASC_{D_1} *versus* x_{D_1} for different P_S at $L = 50$.

To further investigate the impact of user location, Fig. 13 illustrates ASC_{D_1} *versus* the horizontal position x_{D_1} for different transmit powers. The secrecy performance varies noticeably with the location of D_1. In particular, ASC_{D_1} decreases significantly when D_1 approaches the jammer located at (110, -5) m and reaches its lowest region around $x_{\text{D}_1} = 110$ m. This behavior is mainly attributed to the reduced $\text{J} - \text{D}_1$ distance, which strengthens the residual AJ interference at D_1 under imperfect AJ cancellation. As D_1 moves away from the jammer, the residual jamming interference is reduced, leading to an initial recovery in the secrecy performance. However, when D_1 moves farther away, the increased RIS- D_1 distance causes higher path loss over the reflected link, thereby reducing the received signal strength and the corresponding SINR at D_1. Consequently, ASC $_{\text{D}_1}$ may decrease again at larger x_{D_1}. Therefore, the variation of ASC_{D_1} with the user location results from the combined effects of the residual AJ interference and the distance-dependent attenuation of the RIS-assisted link. These results highlight the

sensitivity of the proposed system to the user location. A full mobility model incorporating time-varying trajectories and Doppler effects, however, is beyond the scope of this work.

To investigate the convergence and numerical accuracy of the Gaussian-Chebyshev quadrature, Fig. 14 illustrates the analytical $\mathrm{ASC}_{\mathrm{Sum}}$ *versus* the number of quadrature nodes N for $L = 30{,}50$, and 70 , with $P_{\mathrm{S}} = 10\mathrm{dBm}$, together with the corresponding Monte Carlo results. For small values of N, the analytical results exhibit noticeable variations due to insufficient quadrature resolution. However, the results rapidly converge as N increases and become nearly unchanged beyond a moderate number of quadrature nodes. The relative errors between the analytical and Monte Carlo results are negligible. These results demonstrate the numerical convergence and accuracy of the adopted quadrature over different numbers of RIS reflecting elements. Therefore, $N = 100$ is adopted throughout this work as a conservative choice to ensure sufficient numerical accuracy and stable convergence.

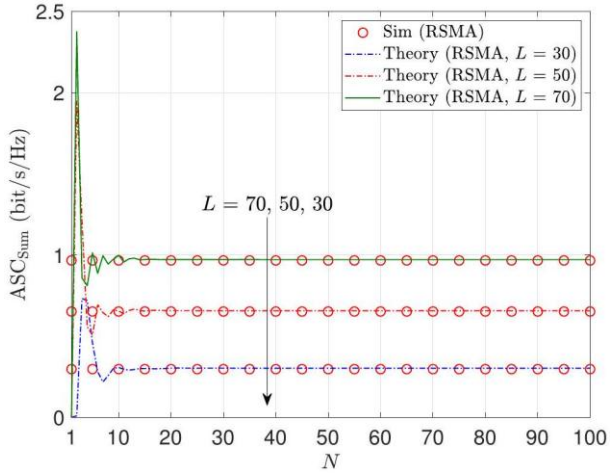


Figure 14. Convergence of the analytical $\mathrm{ASC}_{\mathrm{Sum}}$ *versus* N for different L at $P_{\mathrm{S}} = 10\mathrm{dBm}$.

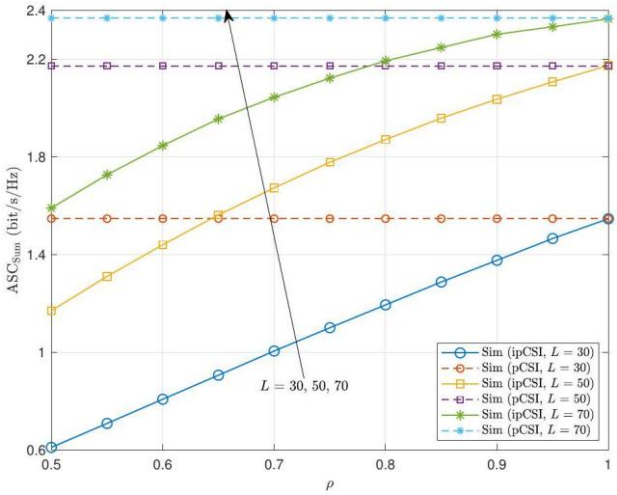


Figure 15. Impact of the ρ on $\mathrm{ASC}_{\mathrm{Sum}}$ for different numbers of L with $P_{\mathrm{S}} = 20\mathrm{dBm}$.

To evaluate the robustness of the proposed system against imperfect CSI, Fig. 15 illustrates $\mathrm{ASC}_{\mathrm{Sum}}$ *versus* the CSI correlation coefficient ρ for different numbers of L, where $\rho = 1$ corresponds to the perfect-CSI (pCSI) case. The corresponding pCSI results are also included as reference benchmarks for the analytical framework. As ρ increases, $\mathrm{ASC}_{\mathrm{Sum}}$ under ipCSI consistently improves and gradually approaches the corresponding pCSI benchmark. In particular, when ρ increases from 0.5 to $1, \mathrm{ASC}_{\mathrm{Sum}}$ increases from approximately 0.61 to 1.55, 1.17 to 2.17, and 1.59 to 2.37 bit/s/Hz for $L = 30$, 50, and 70, respectively. Moreover, increasing L improves the secrecy performance over the considered range of CSI correlation coefficients. These results demonstrate that CSI uncertainty can noticeably degrade the secrecy performance relative to the pCSI-based analytical benchmark, while the performance loss gradually diminishes as the CSI quality improves.

"Secrecy Performance Analysis of RIS-assisted RSMA Systems under Imperfect Artificial Jamming Cancellation and Imperfect SIC," L. H. Luyen, L. T. Dung, T. T. Nguyen and T. M. Hoang.

5. CONCLUSION

This paper investigated the secrecy performance of an RSMA system assisted by RIS and AJ in the presence of an eavesdropper. To better capture practical deployment scenarios, the effects of residual AJ interference at legitimate users as well as ipSIC were taken into account. Analytical expressions for the OP, IP, SRT, and ASC of the proposed system were derived. The performance of the proposed scheme was compared with that of the non-jammer and NOMA benchmark systems, thereby highlighting the advantages of integrating RSMA, RIS, and AJ for enhancing PLS. Numerical results demonstrated that the proposed system achieved superior secrecy performance compared with the benchmark schemes across various performance metrics. In addition, the GSS method was separately applied to the considered design parameters, including P_S, P_J, L, and α_c, through one-dimensional optimization to determine their individual optimal values for SRT minimization or ASC maximization. Moreover, the effects of residual AJ interference at legitimate users and ipSIC on the overall system performance were comprehensively analyzed. The present analysis considers a passive RIS with ideal hardware operation, while practical hardware impairments, such as component aging and reflecting-element failures, are not explicitly modeled. In addition, active RIS architectures, which introduce different hardware characteristics and power-consumption requirements, are beyond the scope of this work. Incorporating RIS hardware impairments and extending the proposed framework to active RIS architectures constitute interesting directions for future work. Furthermore, the present study considers a single eavesdropper to maintain analytical tractability. In practical scenarios, multiple eavesdroppers may further degrade the secrecy performance, depending on their number, spatial distribution, and potential cooperation. Extending the proposed analytical framework to multi-eavesdropper scenarios, including both non-colluding and colluding eavesdroppers, is therefore an important direction for future work. Based on these findings, several practical design insights were provided to further improve the secrecy performance of RSMA-RIS-AJ systems in future wireless networks.

APPENDIX

Using (3), the CDF of $\gamma_{\mathrm{D}_i^{x_c}}$ can be derived as follows:

$$F_{\mathrm{D}_i^{x_i}}(x) = \Pr\{\gamma_{\mathrm{D}_i}{}^{x_c} < x\} = \Pr\left\{\frac{\mathcal{Z}_i^2 \alpha_c P_S}{\mathcal{Z}_i^2(\alpha_1+\alpha_2)P_S + \gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2} < x\right\},$$
$$= \Pr\{\mathcal{Z}_i^2 P_S(\alpha_c - (\alpha_1+\alpha_2)x) < x(\gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2)\}. \quad (31)$$

From (31), the evaluation of $F_{\gamma_D}^{x_c}(x)$ can be divided into two cases, i.e., $\alpha_c - (\alpha_1+\alpha_2)x \le 0$ and $\alpha_c - (\alpha_1+\alpha_2)x > 0$. In the first case, namely $\alpha_c - (\alpha_1+\alpha_2)x \le 0$ or equivalently $x \ge \frac{\alpha_c}{\alpha_1+\alpha_2}$, the outage event always occurs. This is because the left-hand side of the inequality becomes negative or zero, whereas the right-hand side remains strictly positive. Therefore, it follows that $F_{\gamma_D}^{x_c}(x) = 1$ when $x \ge \frac{\alpha_c}{\alpha_1+\alpha_2}$. In the second case, i.e., $\alpha_c - (\alpha_1+\alpha_2)x > 0$ or equivalently $x < \frac{\alpha_c}{\alpha_1+\alpha_2}$, (31) can be rewritten as follows:

$$F_{\gamma_{\mathrm{D}_i}^{x_c}}(x) = \Pr\left\{\mathcal{Z}_i^2 < \frac{x(\gamma_{\mathrm{JD}_i} + \delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c - (\alpha_1+\alpha_2)x)}\right\} = \int_0^\infty F_{\mathcal{Z}_i}\left(\sqrt{\frac{x(y+\delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c-(\alpha_1+\alpha_2)x)}}\right) f_{\gamma_{\mathrm{D}_i}}(y)dy. \quad (32)$$

Based on the result given in [27, Eq. (A4)], we obtain:

$$F_{\mathcal{Z}_i}\left(\sqrt{\frac{x(y+\delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c-(\alpha_1+\alpha_2)x)}}\right) = 1 - \frac{1}{\Gamma(\theta)}\Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}_i}}\sqrt{\frac{x(y+\delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c-(\alpha_1+\alpha_2)x)}}\right), \quad (33)$$

where $\theta = \frac{L\pi^2}{16-\pi^2}$; $\phi_{\mathrm{D}_i} = \frac{(16-\pi^2)\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}}}{4\pi}$ with $\lambda_j = d_j^{-\beta}, j \in (\mathrm{SR}, \mathrm{RD}_i, \mathrm{RE})$.

As the channel between J and D_1 follows a Rayleigh fading distribution, the corresponding random variable γ_{JD_i} is exponentially distributed. Accordingly, the PDF of γ_{JD_i} can be expressed as follows:

$$f_{\gamma_{\mathrm{J}_i}}(y) = \lambda_{\mathrm{JD}_i} e^{-\lambda_{\mathrm{JD}_i} y}, \quad (34)$$

where, $\lambda_{\mathrm{JD}_i} = \frac{1}{\gamma_{\mathrm{JD}_i}}$.

Combining (33) and (34), we can be calculated as:

$$F_{\gamma_{\mathrm{D}_i}^{x_c}}(x) = \int_0^\infty \left(1 - \frac{1}{\Gamma(\theta)}\Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}_i}}\sqrt{\frac{x(y+\delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c-(\alpha_1+\alpha_2)x)}}\right)\right) f_{\gamma_{\mathrm{JD}_i}}(y)dy$$

$$= 1 - \frac{\lambda_{\mathrm{JD}_i}}{\Gamma(\theta)}\int_0^\infty \Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}_i}}\sqrt{\frac{x(y+\delta_{\mathrm{D}_i}^2)}{P_S(\alpha_c-(\alpha_1+\alpha_2)x)}}\right) e^{-\lambda_{\mathrm{JD}_i} y} dy \quad (35)$$

The CDF of $\gamma_{\mathrm{D}_i}^{x_c}$ in (35) is mathematically intractable for deriving an exact closed-form expression. To address this issue, the Chebyshev-Gauss quadrature technique [52, Eq. (25.4.30)[9] is employed to obtain an accurate approximation of (35).
Let $t = e^{-\lambda_{\mathrm{JD}_i} y}$, (35) can be reformulated as follows:

$$F_{\gamma_{\mathrm{D}_i}^{x_c}}(x) = 1 - \frac{1}{\Gamma(\theta)} \int_0^1 \Gamma\left(\theta, \frac{1}{\phi_{\mathrm{D}_i}} \sqrt{\frac{x\left(\frac{\ln(1/t)}{\lambda_{\mathrm{JD}_i}} + \delta_{\mathrm{D}_i}^2\right)}{P_{\mathrm{S}}(\alpha_c - (\alpha_1 + \alpha_2)x)}}\right) dt \tag{37}$$

Finally, by applying (36), the corresponding CDF of $\gamma_{\mathrm{D}_i}^{x_c}$ can be obtained as (8).

By following the same derivation procedure used for obtaining the CDF of $\gamma_{\mathrm{D}i}^{x_c}$, the CDFs of $\gamma_{\mathrm{D}i}^{x_p}$, $\gamma_{\mathrm{E}}^{x_c}$, and $\gamma_{\mathrm{E}}^{x_p}$ can be derived as given in (9), (10), and (11), respectively. This completes the proof.

REFERENCES

[1] M. H. Khoshafa, T. Ngatched, M. H. Ahmed, Y. Gadallah and D. Niyato, "RIS-empowered Rate-splitting Multiple Access Toward 6G and Beyond Wireless Communication Networks: A Comprehensive Survey," IEEE Internet Things J., vol. 13, no. 3, pp. 3913-3937, 2026.

[2] H. Niu, Y. Xiao, X. Lei, J. Chen, Z. Xiao, M. Li and C. Yuen, "A Survey on Artificial Noise for Physical Layer Security: Opportunities, Technologies, Guidelines, Advances and Trends," IEEE Commun. Surv. Tutor., vol. 28, pp. 341-381, 2026.

[3] L. Cai et al., "Secure Physical Layer Communications for Low-altitude Economy Networking: A Survey," IEEE Commun. Surv. Tutor., vol. 28, pp. 2497-2530, 2025.

[4] N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and B. S. Kim, "Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 11, no. 2, pp. 197-210, 2025.

[5] B. Clerckx et al., "A Primer on Rate-splitting Multiple Access: Tutorial, Myths and Frequently Asked Questions," IEEE J. Sel. Areas Commun., vol. 41, no. 5, pp. 1265-1308, 2023.

[6] Q.-N. Van, "Multiple RISs for Enhancing the Secrecy Performance of NOMA Systems over Realistic Nakagami- m Fading Channels," IEEE Trans. Veh. Technol., vol. 73, no. 5, pp. 6584-6599, 2024.

[7] P. T. Tran et al., "Enhancing secrecy performance of full-duplex relaying systems using IRS and RSMA," IEEE Trans. Mobile Comput., vol. 25, no. 1, pp. 878-891, 2026.

[8] Z. Lin et al., "Supporting IoT with rate-splitting multiple access in satellite and aerial-integrated networks," IEEE Internet Things J., vol. 8, no. 14, pp. 11123-11134, 2021.

[9] Z. Lin, Z. Feng, K. Guo, A. Nauman, D. Niyato, J. Wang, "AI-driven Seamless and Massive Access in Space-air-ground Integrated Networks," IEEE Wireless Commun., vol. 32, no. 3, pp. 72-79, 2025.

[10] Z. Lin et al., "Refracting RIS-aided Hybrid Satellite-terrestrial Relay Networks: Joint Beamforming Design and Optimization," IEEE Trans. Aerosp. Electron. Syst., vol. 58, no. 4, pp. 3717-3724, 2022.

[11] Z. Feng, Z. Lin, H. Wang, R. Ma, K. An and Y. He, "Toward Secure and Reliable SAGIN: Learning-Driven Multi-dimensional Resource Scheduling for Multi-RIS-assisted OTFS Transmission," IEEE J. Sel. Areas Commun., vol. 44, pp. 4848-4860, 2026.

[12] T. Bao and M. Erol-Kantarci, "Heuristic Deep Reinforcement Learning for Phase Shift Optimization in RIS-assisted Secure Satellite Communication Systems with RSMA," Proc. of the IEEE Int. Conf. on Communications (ICC), pp. 3900-3905, 2025.

[13] P. Huang, S. Pala, K. Singh and C.-P. Li, "RIS-assisted Multiple Access for Secure Multiuser MISO Non-terrestrial Networks: A Deep Reinforcement Learning Approach," Proc. of the IEEE Conf. on Computer Communications Workshops (IN-FOCOM WKSHPS), pp. 1-6, London, UK, 2025.

[14] B. Wang et al., "Secure Beamforming Design for RIS-aided Rate-splitting Systems with Untrusted User Cooperative Relay," IEEE Trans. Veh. Technol., vol. 75, pp. 1557-1562, 2026.

[15] Z. Ali et al., "Secure Sum-rate Optimization in RIS-assisted RSMA HAP Systems with Untrusted Users," IEEE Trans. Aerosp. Electron. Syst., vol. 62, pp. 5167-5182, 2026.

[16] C. Zhang et al., "Robust Secure Beamforming Design for Downlink RIS-ISAC Systems Enhanced by RSMA," IEEE Wireless Commun. Lett., vol. 14, pp. 1271-1275, 2025.

[17] H. Ke et al., "Rate Splitting and Beamforming Design for RIS-assisted RSMA-enhanced ISAC Networks," IEEE Wireless Commun. Lett., vol. 14, pp. 1738-1742, 2025.

[18] H. Liu et al., "Joint Resource Allocation and Secure Beamforming for Active RIS-aided mmWave-RSMA with Dual-identity User," IEEE Internet Things J., vol. 13, no. 4, pp. 6626-6639, 2026.

---

9 The approximate expression based on the Chebyshev-Gauss quadrature can be formulated as:

$$\int_a^b f(x)dx \approx \frac{(b-a)\pi}{2N_k} \sum_{n=1}^{N_k} \sqrt{1 - V_n^2} f(x_n), \tag{36}$$

where N serves as a critical parameter determining the trade-off between approximation accuracy and computational complexity. Furthermore, the variables V_n and x_n are defined as $V_n = \cos\left(\frac{2n-1}{2N_k}\pi\right); x_n = \frac{b-a}{2} V_n + \frac{b+a}{2}$.

[19] M. Guo et al., "RIS-empowered Secure and Reliable Satellite Communications with RSMA," Proc. of the IEEE/CIC Int. Conf. on Communications in China (ICCC), pp. 1-6, 2025.

[20] Y. Gao, Q. Wu, W. Chen and D. W. K. Ng, "Rate-splitting Multiple Access for Intelligent Reflecting Surface-aided Secure Transmission," IEEE Commun. Lett., vol. 27, no. 2, pp. 482-486, 2023.

[21] D. Wang, J. Li, Q. Lv, Y. He, L. Li, Q. Hua, O. Alfarraj and J. Zhang, "Integrating Reconfigurable Intelligent Surface and AAV for Enhanced Secure Transmissions in IoT-enabled RSMA Networks," IEEE Internet Things J., vol. 12, no. 8, pp. 9405-9419, 2025.

[22] X. Guo, R. Yuan, J. Zhang, Y. Song and S. Chen, "RSMA-enhanced Secure Transmission Scheme for Active STAR-RIS-aided Networks," IEEE Wireless Commun. Lett., vol. 15, pp. 2699-2703, 2026.

[23] H. Lei, S. Zhou, K.-H. Park, I. S. Ansari, H. Tang and M.-S. Alouini, "Outage Analysis of Millimeter Wave RSMA Systems," IEEE Trans. Commun., vol. 71, no. 3, pp. 1504-1520, 2023.

[24] H. Lei, S. Zhou, X. Chen, I. S. Ansari, Y. Li, G. Pan and M.-S. Alouini, "On secure mmWave RSMA Systems," IEEE Internet Things J., vol. 11, no. 10, pp. 18917-18929, 2024.

[25] Q. Dan, H. Lei, K.-H. Park and G. Pan, "Beamforming for Secure RSMA-aided ISAC Systems," IEEE Trans. Cogn. Commun. Netw., vol. 11, no. 5, pp. 2970-2983, 2025.

[26] H.-N. Nguyen and P.-C. Ngo, "On the Effect of Keyhole Channel in RSMA Networks: A Theoretical Outage Analysis," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 12, no. 2, pp. 201-211, 2026.

[27] V. Ta Ty, T. Trung Duy and P. Ngoc Son, "Enhancing the Secrecy Performance and Secure Energy Efficiency of NOMA Systems Using RIS with Artificial Jamming," Int. J. Commun. Syst., vol. 39, no. 7, p. e70474, 2026.

[28] M. H. Khoshafa, T. M. N. Ngatched and M. H. Ahmed, "Reconfigurable Intelligent Surfaces-aided Physical Layer Security Enhancement in D2D Underlay Communications," IEEE Commun. Lett., vol. 25, no. 5, pp. 1443-1447, 2020.

[29] Y. Pei et al., "Secrecy Outage Probability Analysis for Downlink RIS-NOMA Networks with on-off Control," IEEE Trans. Veh. Technol., vol. 72, no. 9, pp. 11772-11786, 2023.

[30] N. H. Kiem et al., "Outage Probability and Ergodic Capacity of RIS-assisted RSMA Communication System," Digit. Signal Process., vol. 172, Article no. 105900, 2026.

[31] C. Ruan, Z. Zhang, H. Jiang, J. Dang, L. Wu and H. Zhang, "Approximate Message Passing for Channel Estimation in Reconfigurable Intelligent Surface Aided MIMO Multiuser Systems," IEEE Trans. Commun., vol. 70, no. 8, pp. 5469-5481, 2022.

[32] Z. Wang, L. Liu and S. Cui, "Channel Estimation for Intelligent Reflecting Surface Assisted Multiuser Communications: Framework, Algorithms and Analysis," IEEE Trans. Wireless Commun., vol. 19, no. 10, pp. 6607-6620, 2020.

[33] X. Wei, D. Shen and L. Dai, "Channel Estimation for RIS Assisted Wireless Communications Part I: Fundamentals, Solutions and Future Opportunities," IEEE Commun. Lett., vol. 25, no. 5, pp. 1398-1402, 2021.

[34] I. Trigui, W. Ajib, W. P. Zhu and M. Di Renzo, "Performance Evaluation and Diversity Analysis of RIS-assisted Communications over Generalized Fading Channels in the Presence of Phase Noise," IEEE Open J. Commun. Soc., vol. 3, pp. 593-607, 2022.

[35] C. Gong et al., "Intelligent Reflecting Surface Aided Secure Communications for NOMA Networks," IEEE Trans. Veh. Technol., vol. 71, no. 3, pp. 2761-2773, 2021.

[36] C. Hung Dinh et al., "Transmit Antenna Selection for Full-duplex Relay Millimeter-wave Communications Employing Rate-splitting Multiple Access," Int. J. Commun. Syst., vol. 38, no. 3, p. e6113, 2025.

[37] Z. Mo, Y. Ni, Y. Liu, H. Zhao, L. Li and Y. Cai, "Active RIS-assisted Communication Systems with Discrete Phase Shifts," IEEE Commun. Lett., vol. 29, no. 4, pp. 674-678, 2025.

[38] T. T. Nguyen, T. M. Hoang and P. T. Tran, "Secrecy Performance Optimization for UAV-based Relay NOMA Systems with Friendly Jamming," Comput. Commun., vol. 235, p. 108086, 2025.

[39] W. Guo, H. Zhao and Y. Tang, "Testbed for Cooperative Jamming Cancellation in Physical Layer Security," IEEE Wireless Commun. Lett., vol. 9, no. 2, pp. 240-243, 2020.

[40] Q. Dan, H. Lei, K.-H. Park, G. Pan and M.-S. Alouini, "Two Birds with One Stone: Beamforming Design for Target Sensing and Proactive Eavesdropping," IEEE Trans. Veh. Technol., vol. 75, no. 8, pp. 17590-17603, 2026.

[41] S. N. Quoc et al., "Enhancing Secrecy Performance in Multi-user Multi-antenna Systems Using Rate-splitting Multiple Access," Digit. Signal Process., vol. 173, Article no. 105943, 2026.

[42] Y. Zou, X. Wang, W. Shen and L. Hanzo, "Security *versus* Reliability Analysis of Opportunistic Relaying," IEEE Trans. Veh. Technol., vol. 63, no. 6, pp. 2653-2661, 2014.

[43] B. Li, Y. Zou, T. Wu, Z. Zhang, M. Chen and Y. Jiang, "Security and Reliability Trade-off of NOMA Based Hybrid Satellite-terrestrial Network with a Friendly Jammer," IEEE Trans. Veh. Technol., vol. 74, no. 2, pp. 3439-3444, 2025.

[44] V. T. Ty, P. N. Son and T. T. Duy, "Secrecy Performance of RIS-assisted Wireless-powered Systems with Artificial Jamming Generation," Phys. Commun., vol. 69, Article no. 102592, 2025.
[45] B. C. Nguyen et al., "Secrecy Performance of Multi-RIS-assisted Wireless Systems," Mob. Netw. Appl., vol. 28, no. 3, pp. 1206-1219, 2023.
[46] F. Xiao, P. Chen, S. Xu, X. Pang and H. Liu, "Physical Layer Security of STAR-RIS-aided RSMA Systems," Phys. Commun., vol. 61, p. 102192, 2023.
[47] M. V. Katwe, R. Deshpande, K. Singh, M.-L. Ku and B. Clerckx, "RSMA-enabled Aerial RIS-aided MU-MIMO System for Improved Spectral-efficient URLLC," IEEE Trans. Veh. Technol., vol. 74, no. 2, pp. 3110-3127, 2025.
[48] C. Pan et al., "Intelligent Reflecting Surface Aided MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," IEEE J. Sel. Areas Commun., vol. 38, no. 8, pp. 1719-1734, 2020.
[49] H. Chang, H. Yang, S. Xu, X. Pang and H. Liu, "Covert Communications in STAR-RIS-aided Rate-Splitting Multiple Access Systems," Phys. Commun., vol. 64, p. 102342, 2024.
[50] B. Li et al., "Securing Multiuser Communications *via* an Energy Harvesting Node: Jammer or Relay?," IEEE Trans. Veh. Technol., vol. 72, no. 7, pp. 8755-8769, 2023.
[51] T. Q. Duong, T. T. Duy, M. Matthaiou, T. Tsiftsis and G. K. Karagiannidis, "Cognitive Cooperative Networks in Dual-hop Asymmetric Fading Channels," Proc. of the 2013 IEEE Global Communications Conference (GLOBECOM), pp. 955-961, Atlanta, USA, 2014.
[52] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables, US Government Printing Office, 1968.

ملخص البحث:

يبحث هذا العمل في اتّصالات السّرّية لنظام إرسال هابط جديد يعتمد تقنية الوصول المتعدّد بتقسيم المعدّل المدعومة بأسطح ذكية قابلة لإعادة التّشكيل مع استخدام التّشويش الاصطناعي. ولكي تعكس الدّراسة السّيناريوهات العملية بشكلٍ أفضل، تمّ أخذ تأثيرات كلّ من عملية إلغاء التّداخل المتتابع غير المثالية وتداخل التّشويش الاصطناعي المتبقّي لدى المستخدمين الشّرعيين بعين الاعتبار. وقد تمّ اشتقاق التّحليل الرّياضي باستخدام الخصائص الإحصائية للقناة المتسلسلة بالاستعانة بطريقة "غاوس-تشيبيشف" للتّربيع العددي ودالّة غاما غير المكتملة. كذلك تمّ اشتقاق صيغ رياضية مغلقة لأربعة مقاييس رئيسية: احتمالية الانقطاع، واحتمالية الاعتراض، والمفاضلة بين الموثوقية والسّرّية، ومتوسط سعة السّرّية.

علاوة على ذلك، تمّ تطبيق خوارزمية البحث بالقسمة الذّهبية بشكل منفصل لتجديد القيم المثلى لمعاملات النّظام الفردية من خلال التّحسين أحادي البعد. تمّ التّحقق من صحّة الصّيغ التّحليلية باستخدام محاكاة مونت كارلو، الّتي أثبتت أنّ المخطّط المدعّم بتقنية التّشويش يحقّق أداءً أفضل بكثيرٍ من مخطّط الوصول المتعدّد غير المتعامد المدعّم بتقنية الأسطح الذّكية القابلة لإعادة التّشكيل والمخطّطات المعيارية غير المدعّمة بتقنية التّشويش، وذلك من حيث أداء السّرّية.

وكشفت النّتائج أنّ مخطّط الوصول النتعدّد المدعّم بأسطح ذكية قابلةٍ لإعادة التّشكيل في ظلّ ظروف إلغاء التّشويش الاصطناعي غير المثالي وإلغاء التّداخل المتتابع غير المثالي يحقّق أفضل توازنٍ بين الأمان والموثوقية من بين جميع المخطّطات المدروسة، متفوقاً بذلك على كلٍّ من مخطّط الوصول المتعدّد غير المتعامد المدعّم بتقنية الأسطح الذّكية القابلة لإعادة التّشكيل والمخطّطات غير المدعّمة بتقنية التّشويش الاصطناعي.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).