On Secrecy Performance of RIS-Assisted MISO Systems Over Rician Channels With Spatially Random Eavesdroppers

Wei Shi, *Graduate Student Member, IEEE*, Jindan Xu, *Member, IEEE*, Wei Xu, *Senior Member, IEEE*, Chau Yuen, *Fellow, IEEE*, A. Lee Swindlehurst, *Fellow, IEEE*, and Chunming Zhao, *Member, IEEE*

***Abstract*— Reconfigurable intelligent surface (RIS) technology is emerging as a promising technique for performance enhancement for next-generation wireless networks. This paper investigates the physical layer security of an RIS-assisted multiple-antenna communication system in the presence of random spatially distributed eavesdroppers. The RIS-to-ground channels are assumed to experience Rician fading. Using stochastic geometry, exact distributions of the received signal-to-noise-ratios (SNRs) at the legitimate user and the eavesdroppers located according to a Poisson point process (PPP) are derived, and closed-form expressions for the secrecy outage probability (SOP) and the ergodic secrecy capacity (ESC) are obtained to provide insightful guidelines for system design. First, the secrecy diversity order is obtained as $\frac{2}{\alpha_2}$, where α_2 denotes the path loss exponent of the RIS-to-ground links. Then, it is revealed that the secrecy performance is mainly affected by the number of RIS reflecting elements, N, and the impact of the number of transmit antennas and transmit power at the base station is marginal. In addition, when the locations of the randomly located eavesdroppers are unknown, deploying the RIS closer to the legitimate user rather than to the base station is shown to be more efficient. Moreover, it is also found that the density of randomly located eavesdroppers, λ_e, has an additive effect on the asymptotic ESC performance given by $\log_2(1/\lambda_e)$. Finally, numerical simulations are conducted to verify the accuracy of these theoretical observations.**

Manuscript received 31 July 2023; revised 19 November 2023; accepted 27 December 2023. Date of publication 9 January 2024; date of current version 14 August 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62271137, Grant 62022026, and Grant 62211530108; and in part by the Fundamental Research Funds for the Central Universities under Grant 2242022k60002 and Grant 2242023K5003. The work of Chau Yuen was supported by the Ministry of Education (MOE), Singapore, under its MOE Tier 2 under Award MOE-T2EP50220-0019. The work of A. Lee Swindlehurst was supported by the U.S. National Science Foundation under Grant CNS-2107182 and Grant EECS-2030029. An earlier version of this paper was presented in part at the IEEE GLOBECOM 2023 Workshops (GC Wkshps) [1]. The associate editor coordinating the review of this article and approving it for publication was Y. Shi. *(Corresponding authors: Wei Xu; Jindan Xu.)*

Wei Shi, Wei Xu, and Chunming Zhao are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with Purple Mountain Laboratories, Nanjing 211111, China (e-mail: wshi@seu.edu.cn; wxu@seu.edu.cn; cmzhao@seu.edu.cn).

Jindan Xu and Chau Yuen are with the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore 639798 (e-mail: jindan.xu@ntu.edu.sg; chau.yuen@ntu.edu.sg).

A. Lee Swindlehurst is with the Center for Pervasive Communications and Computing, Henry Samueli School of Engineering, University of California at Irvine, Irvine, CA 92697 USA (e-mail: swindle@uci.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2023.3348591.

Digital Object Identifier 10.1109/TWC.2023.3348591

***Index Terms*— Reconfigurable intelligent surface (RIS), physical layer security, secrecy outage probability (SOP), ergodic secrecy capacity (ESC), stochastic geometry.**

I. Introduction

RECONFIGURABLE intelligent surface (RIS) technology has recently been recognized as a promising approach for realizing both spectral and energy efficient communications in future wireless networks [2], [3], [4], [5]. An RIS comprises a large number of low-cost passive reflecting elements that are able to independently control the phase shifts and/or amplitudes of their reflection coefficients. In this way, the RIS can realize accurate beamforming for adjusting the propagation environments and thus improving the signal quality at desired receivers. In addition, unlike traditional relay transmission, an RIS with miniaturized circuits does not generate new signals or thermal noise. Hence, RISs can be flexibly installed on outdoor buildings, signage, street lamps, and indoor ceilings to help provide additional high-quality links [5]. Due to these advantages, RISs have been widely studied to support a broad range of communication requirements, including data rate enhancement [6], [7], [8], coverage extension [9], [10], [11], and interference mitigation [12], [13], [14].

In recent years, with the fast-growing number of wireless devices, security for wireless communication has become a critical issue. As a complement to conventional complicated cryptographic methods, physical layer security (PLS) approach leverages the physical characteristics of the propagation environment for enhancing cellular network security against eavesdropping attacks. The capability of an RIS to create a smart controllable wireless propagation environment makes it a promising approach for providing PLS [15]. For example, the authors of [16] and [17] investigated the joint optimization of the active and nearly passive beamforming at the transmitter and the RIS to maximize the theoretical secrecy rate. Furthermore, the design of artificial noise (AN) was also considered in [18] for maximizing the system sum-rate while limiting information leakage to potential eavesdroppers.

On the other hand, there are multiple works that investigate the theoretical secrecy performance for RIS-enhanced PLS systems in terms of secrecy outage probability (SOP) and ergodic secrecy capacity (ESC) [19], [20], [21], [22],

1536-1276 © 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

[23], [24], [25]. In particular, the SOP of an RIS-aided single-antenna system was first studied in the presence of an eavesdropper [19]. An SOP and ESC analysis that considered implementation issues was conducted in [20] and [21], respectively, under the assumption of discrete RIS phase shifts. RIS-aided secure communications were also studied in emerging applications, such as Device-to-Device (D2D) [22], vehicular networks [23], unmanned aerial vehicle (UAV) [24], and non-terrestrial networks [25]. However, for analytical simplicity and mathematical tractability, most works have considered single-antenna nodes and Rayleigh fading channels, and overlooked randomly distributed eavesdroppers. In order to investigate a more practical RIS-aided secure system, the randomness of the eavesdropper locations has to be taken into account when analyzing the system performance.

Stochastic geometry is an efficient mathematical tool for capturing the topological randomness of networks [26]. In this approach, the wireless network is conveniently abstracted to a point process that can capture the essential network properties. A homogeneous Poisson point process (PPP) is the most popular and tractable point process used to model the locations of the mobile devices in wireless networks [27]. However, there have been few works studying the secrecy performance of an RIS-aided communication system with spatially random eavesdroppers, which leaves the impact of key system parameters under the stochastic geometry framework still unclear.

A. Motivation and Contribution

PLS has been studied in diverse RIS-assisted communication scenarios, but rarely considered in the general case of randomly located eavesdroppers. Although the authors of [28] and [29] considered random eavesdropper locations, there are still several research gaps left to be filled. In [28], a single-antenna setting was adopted at the base station to analyze the ESC performance, but the Rician fading assumption and RIS phase shifts optimization were not taken into consideration for the multiple-antenna setting. In [29], a study was developed based on a simplified transmit beamforming design and the analyses of secrecy diversity order and capacity were not conducted. In addition, the works in [28] and [29] both need to be further explored to quantify the impact of the key parameters, e.g., the number of RIS reflecting elements, on the attainable secrecy performance in order to provide insightful guidelines for system design. Table I provides a summary of current studies related to the RIS-assisted secure communication systems and compares our work with them. In this paper, we investigate the SOP and ESC performance of an RIS-assisted multiple-input single-output (MISO) system over Rician fading channels with spatially random eavesdroppers. The main contributions of our work are summarized as follows.

- Assuming maximum ratio transmission (MRT) for the transmit beamforming, the optimal reflect beamforming at the RIS is designed. Using tools from stochastic geometry, we derive accurate closed-form expressions for the distributions of the received signal-to-noise-ratios (SNRs) at the legitimate user and randomly located eavesdroppers located according to a homogeneous PPP.
- We propose a new analytical PLS framework for the RIS-aided MISO secure communication system over Rician fading channels. Novel closed-form expressions are derived to characterize the SOP and ESC of the system. The derived results show that both the SOP and ESC are mainly affected by the number of RIS reflecting elements, and are not strong functions of the number of transmit antennas nor the transmit power at the base station, which means that increasing either of these latter resources will not significantly improve the secrecy performance.
- To obtain more insightful observations, the asymptotic secrecy performance in the high SNR regime is also analyzed to characterize the SOP and ESC. The asymptotic SOP demonstrates that the secrecy diversity order of RIS-aided MISO secure communication systems depends on the path loss exponent of the RIS-to-ground links. In addition, when the locations of spatially random eavesdroppers are unknown, it is more efficient to deploy the RIS closer to the legitimate user than to the base station. Moreover, the impact of the randomly located eavesdropper density, λ_e, on the asymptotic ESC performance is quantitatively evaluated to be additive and proportional to $\log_2(1/\lambda_e)$.

B. Organization

The rest of this paper is organized as follows. We introduce the system model in Section II, and in Section III, we derive the exact distributions of the received SNRs for the legitimate user and randomly located eavesdroppers. In Section IV, we provide a closed-form expression for the SOP, and we study the secrecy diversity order at high SNR. The ergodic secrecy capacity is investigated in Section V and simulation results are discussed in Section VI. Finally, we draw our conclusions in Section VII.

Notation: Boldface lowercase (uppercase) letters represent vectors (matrices). The set of all complex numbers is denoted by $\mathbb{C}$. The set of all positive real numbers is denoted by $\mathbb{Z}^+$. The superscripts $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ stand for the transpose, conjugate, and conjugate-transpose operations, respectively. A circularly symmetric complex Gaussian distribution is denoted by $\mathcal{CN}$. A Rician distribution is denoted by $Rice$. $\mathbb{E}\{\cdot\}$ denotes the expectation of a random variable (RV). $\mathrm{diag}\{\cdot\}$ indicates a diagonal matrix. The operators $|\cdot|$ and $\|\cdot\|$ take the norm of a complex number and a vector, respectively. $\angle$ returns the phase of a complex value. The symbol $\Gamma(\cdot)$ is the Gamma function. The symbols $\gamma(\cdot,\cdot)$ and $\Gamma(\cdot,\cdot)$ denote the lower and upper incomplete Gamma functions, respectively. $[x]^+ = \max\{0, x\}$ returns the maximum between 0 and x.

II. System Model

As illustrated in Fig. 1, an RIS-assisted secure communication system is considered, where a base station (S) is equipped with K antennas and an RIS is composed of N reflecting elements. The reflection matrix of the RIS is denoted by $\mathbf{\Theta} \triangleq \mathrm{diag}\left\{\eta_1 e^{j\theta_1}, \ldots, \eta_n e^{j\theta_n}, \ldots, \eta_N e^{j\theta_N}\right\}$, where $\eta_n \in [0,1]$ and $\theta_n \in [0, 2\pi)$ for $n = 1, 2, \ldots, N$ are, respectively,

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

TABLE I
COMPARISON BETWEEN OUR WORK WITH THE STATE-OF-THE-ART

	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[28]	[29]	Our work
MISO								✓	✓	✓
Rician channel									✓	✓
Eves with PPP distribution								✓	✓	✓
SOP analysis	✓	✓		✓	✓	✓			✓	✓
ESC analysis			✓				✓	✓		✓
High-SNR analysis		✓		✓		✓				✓

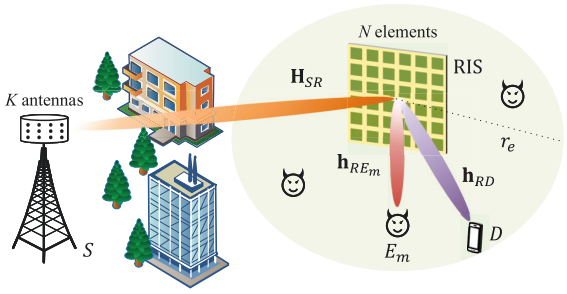

Fig. 1. System model of an RIS-assisted MISO communication system in the presence of spatially random eavesdroppers.

the amplitude coefficient and the phase shift introduced by the n-th reflecting element. In order to exploit the maximum reflection capability of the RIS, the amplitude coefficients in this paper are set to 1, i.e., $\eta_n = 1$ for all n. The eavesdroppers (E) are randomly located within a disk of radius r_e centered at the RIS, and their spatial distribution is modeled using a homogeneous PPP Φ_e with a density λ_e [27], [28], [29]. In contrast, the legitimate user is located without any spatial restrictions.

We assume that the direct link between S and the legitimate user (D) is blocked by obstacles, which is a common occurrence in high frequency bands. To address this issue, the data transmission between S and D is facilitated by the RIS. Since the base station and the RIS are typically deployed at an elevated height with few scatterers, the channel between S and the RIS is assumed to obey a line-of-sight (LoS) model [30], [31], [32], denoted by $\mathbf{H}_{SR} \in \mathbb{C}^{N\times K}$. While the legitimate user and eavesdroppers are usually located on the ground, the RIS-related channels with these terminals undergo both direct LoS and rich scattering, which can be modeled using Rician fading. Here, $\mathbf{h}_{Ri} \in \mathbb{C}^{N\times 1}$ is the channel vector of the RIS-i links, where $i \in \{D, E_m\}$ and E_m represents the m-th eavesdropper. Specifically, the expressions for $\mathbf{H}_{SR}$ and $\mathbf{h}_{Ri}$ are given by

$$\mathbf{H}_{SR} = \sqrt{\nu}\overline{\mathbf{H}}_{SR}, \tag{1}$$

$$\mathbf{h}_{Ri} = \sqrt{\mu_i}\left(\sqrt{\frac{\epsilon}{\epsilon+1}}\overline{\mathbf{h}}_{Ri} + \sqrt{\frac{1}{\epsilon+1}}\widetilde{\mathbf{h}}_{Ri}\right), \tag{2}$$

where $\nu = \beta_0 d_{SR}^{-\alpha_1}$ and $\mu_i = \beta_0 d_{Ri}^{-\alpha_2}$ denote the large-scale fading coefficients, β_0 is the path loss at a reference distance of 1m, d_{SR} and d_{Ri} are the distances of the S-RIS and RIS-i links respectively, $\alpha_1 \geq 2$ and $\alpha_2 \geq 2$ are the path loss exponents for the S-RIS and RIS-i links respectively, and ϵ denotes the Rician factor. [1] The vector $\widetilde{\mathbf{h}}_{Ri}$ represents the non-line-of-sight (NLoS) component, whose entries are standard independent and identically distributed (i.i.d.) Gaussian RVs, i.e., $\mathcal{CN}(0,1)$. The LoS components $\overline{\mathbf{H}}_{SR}$ and $\overline{\mathbf{h}}_{Ri}$ are expressed as

$$\overline{\mathbf{H}}_{SR} = \mathbf{a}_N\left(\phi_{SR}^a, \phi_{SR}^e\right)\mathbf{a}_K^H\left(\psi_{SR}^a, \psi_{SR}^e\right) = \mathbf{a}_{N,SR}\mathbf{a}_{K,SR}^H, \tag{3}$$

$$\overline{\mathbf{h}}_{Ri} = \mathbf{a}_N\left(\psi_{Ri}^a, \psi_{Ri}^e\right) = \mathbf{a}_{N,Ri}, \tag{4}$$

where ϕ_{SR}^a (ϕ_{SR}^e) is the azimuth (elevation) angle of arrival (AoA) at the RIS, ψ_{SR}^a (ψ_{SR}^e) and ψ_{Ri}^a (ψ_{Ri}^e) are the azimuth (elevation) angles of departure (AoD) at the base station and RIS, respectively, and $\mathbf{a}_Z\left(\vartheta^a, \vartheta^e\right)$ is the array response vector. We consider a uniform square planar array (USPA) deployed at both the base station and the RIS. Thus, the array response vector can be written as [35]

$$\mathbf{a}_Z\left(\vartheta^a, \vartheta^e\right) = \Big[1, \ldots, \mathrm{e}^{j2\pi\frac{d}{\lambda}\left(x\sin\vartheta^a\sin\vartheta^e + y\cos\vartheta^e\right)}, \ldots, \mathrm{e}^{j2\pi\frac{d}{\lambda}\left(\left(\sqrt{Z}-1\right)\sin\vartheta^a\sin\vartheta^e + \left(\sqrt{Z}-1\right)\cos\vartheta^e\right)}\Big]^T, \tag{5}$$

where d and λ are the element spacing and signal wavelength, respectively, and $0 \leq x, y < \sqrt{Z}$ are the element indices in the plane. We assume that the channel coefficients of $\mathbf{H}_{SR}$ and $\mathbf{h}_{RD}$ are perfectly known to S and extensive approaches have been proposed in literature for the channel estimation of RIS-aided links [36], [37], [38]. However, the channel coefficient $\mathbf{h}_{RE_m}$ is typically not available to S, since eavesdroppers are usually passive devices that do not emit signals.

III. DISTRIBUTIONS OF THE RECEIVED SNRS

In order to analyze the secrecy performance of the system, we need to first characterize the distributions of the received SNRs at the legitimate user and the eavesdroppers.

A. Distribution of the Received SNR at D

Assuming quasi-static flat fading channels, the signal received at D is expressed as

$$r_D = \mathbf{g}_D^H\mathbf{f}s + n_D, \tag{6}$$

where the cascaded channel $\mathbf{g}_D^H \triangleq \mathbf{h}_{RD}^H\mathbf{\Theta}\mathbf{H}_{SR} \in \mathbb{C}^{1\times K}$, $\mathbf{f} \in \mathbb{C}^{K\times 1}$ is the normalized beamforming vector, s denotes the transmit signal that satisfies the power constraint $\mathbb{E}\{|s|^2\} = P_T$, and $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ is additive white Gaussian noise

[1] The Rician factors/path loss exponents for the RIS-D and RIS-E channels are assumed to be identical, as shown in [29], [33], and [34], since the propagation environments around the legitimate user and eavesdroppers are similar.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

(AWGN) at D with variance σ_D^2. Therefore, the received SNR at D is calculated as

$$\gamma_D = \frac{P_T \left|\mathbf{g}_D^H \mathbf{f}\right|^2}{\sigma_D^2} = \rho_d \left|\mathrm{A}\right|^2, \tag{7}$$

where the RV $|\mathrm{A}| \triangleq \left|\mathbf{g}_D^H \mathbf{f}\right|$, and $\rho_d \triangleq \frac{P_T}{\sigma_D^2}$ denotes the transmit SNR from S to D.

Due to passive eavesdropping, the channel state information of the eavesdropper is not known to the RIS, thus we determine the transmit beamforming at S and the reflect beamforming at the RIS by maximizing the received signal power at D.

Theorem 1: When MRT beamforming is adopted, i.e., $\mathbf{f} = \frac{\mathbf{g}_D}{\|\mathbf{g}_D^H\|}$, the optimal reflection matrix of the RIS is given as

$$\mathbf{\Theta}^{\mathrm{opt}} = \mathrm{diag}\left\{ \mathrm{e}^{-j\angle\left(\mathrm{diag}\left\{\mathbf{h}_{RD}^H\right\}\mathbf{a}_{N,SR}\right)} \right\}. \tag{8}$$

Proof: See Appendix A. ∎

With the optimized RIS phase shifts in *Theorem 1*, the RV $|\mathrm{A}|$ is expressed as $|\mathrm{A}| = \sqrt{K\nu}\sum_{n=1}^{N} |h_{RD}(n)|$ which follows the distribution characterized in the following lemma.

Lemma 1: The cumulative distribution function (CDF) of $|\mathrm{A}|$ is well approximated by

$$F_{|\mathrm{A}|}(x) = \frac{1}{\Gamma(k)} \gamma\left(k, \frac{x}{\theta}\right), \tag{9}$$

with shape parameter $k = N\frac{\frac{\pi}{4}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}{1+\epsilon-\frac{\pi}{4}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}$ and scale parameter $\theta = \sqrt{K}\sqrt{\frac{\mu_D \nu}{\epsilon+1}}\frac{1+\epsilon-\frac{\pi}{4}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}{\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)}$, in which $L_q(x)$ is the Laguerre polynomial defined in [39, Eq. (2.66)].

Proof: See Appendix B. ∎

By applying *Lemma 1*, we can obtain the CDF and probability density function (PDF) of γ_D in (7), respectively, as

$$F_{\gamma_D}(x) = F_{|\mathrm{A}|}\left(\sqrt{x/\rho_d}\right) = \frac{1}{\Gamma(k)}\gamma\left(k, \frac{\sqrt{x/\rho_d}}{\theta}\right), \tag{10}$$

$$f_{\gamma_D}(x) = \frac{dF_{\gamma_D}(x)}{dx} = \frac{\mathrm{e}^{-\frac{\sqrt{x/\rho_d}}{\theta}}\left(\frac{\sqrt{x/\rho_d}}{\theta}\right)^k}{2\Gamma(k)\,x}. \tag{11}$$

Corollary 1 (Asymptotic Analysis): For large N, the average received SNR at the legitimate user D is obtained as

$$\mathbb{E}\{\gamma_D\} = \frac{\pi\left(L_{1/2}(-\epsilon)\right)^2}{4(\epsilon+1)}\rho_d \mu_D \nu K N^2. \tag{12}$$

Proof: We can infer from (7) and *Lemma 1* that $\mathbb{E}\{\gamma_D\} = \rho_d \mathbb{E}\{|\mathrm{A}|^2\} = \rho_d k(1+k)\theta^2$ [40]. By substituting the shape and scale parameters, the proof is completed. ∎

Remark 1: From *Corollary 1*, we see that $\mathbb{E}\{\gamma_D\}$ scales with K and N^2, which implies that deploying more transmit antennas and RIS reflecting elements both increase the average received SNR at the legitimate user, while the impact of N is more dominant. Such a "squared improvement" in terms of N is due to the fact that the optimal reflect beamforming attained in *Theorem 1* not only enables the system to achieve a beamforming gain of KN in the S-RIS link, but also acquires an additional gain of N by coherently collecting signals in the RIS-D link.

Remark 2: From *Corollary 1*, it is also found that $\mathbb{E}\{\gamma_D\}$ is increasing with respect to (w.r.t.) the Rician factor $\epsilon > 0$. In other words, the average received SNR at the legitimate user is greater when the proportion of the LoS component in the RIS-D link is higher. It is worth noting that the average SNR in (12) can be upper bounded as $\mathbb{E}\{\gamma_D\} \leq \mathbb{E}\{\gamma_D\}^{\mathrm{U}} = \rho_d \mu_D \nu K N^2$ which holds for large N and ϵ since $\lim_{\epsilon\to\infty}\frac{\left(L_{1/2}(-\epsilon)\right)^2}{\epsilon+1} = \frac{4}{\pi}$.

B. Distribution of the Received SNR at E

Before calculating the effective SNR of the independent and homogeneous PPP distributed eavesdroppers, we first derive the SNR of the m-th eavesdropper E_m. The signal received at E_m is formulated as

$$r_{E_m} = \mathbf{h}_{RE_m}^H \mathbf{\Theta} \mathbf{H}_{SR} \mathbf{f} s + n_{E_m}, \tag{13}$$

where $n_{E_m} \sim \mathcal{CN}(0, \sigma_E^2)$ is AWGN at E_m with variance σ_E^2. The received SNR at E_m is given in the following proposition.

Proposition 1: The received SNR at E_m is expressed as

$$\gamma_{E_m} = \rho_e K \nu \left|Z_{E_m}\right|^2, \tag{14}$$

where $\rho_e \triangleq \frac{P_T}{\sigma_E^2}$ denotes the transmit SNR and we define the RV $Z_{E_m} \triangleq \sum_{n=1}^{N} h_{RE_m}^*(n)\,\mathrm{e}^{-j\angle h_{RD}^*(n)}$.

Proof: See Appendix C. ∎

According to *Proposition 1*, we present *Lemma 2* before deriving the distribution of γ_{E_m}.

Lemma 2: The RV Z_{E_m} follows a complex Gaussian distribution with mean M_{E_m} and variance V_{E_m}, given by

$$M_{E_m} = \sqrt{\frac{\mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\mathrm{e}^{j\pi\frac{d}{\lambda}\left(\sqrt{N}-1\right)(\delta_1+\delta_2)} \times \frac{\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_2\right)}{\sin\left(\pi\frac{d}{\lambda}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\delta_2\right)}, \tag{15}$$

$$V_{E_m} = N\mu_{E_m}\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right], \tag{16}$$

where $\delta_1 = \sin\psi_{RD}^a \sin\psi_{RD}^e - \sin\psi_{RE_m}^a \sin\psi_{RE_m}^e$ and $\delta_2 = \cos\psi_{RD}^e - \cos\psi_{RE_m}^e$.

Proof: See Appendix D. ∎

As disclosed in *Lemma 2*, we conclude that γ_{E_m} is a non-central Chi-squared RV with two degrees of freedom. Then, the CDF of γ_{E_m} is given by

$$F_{\gamma_{E_m}}(x) = 1 - Q_1\left(\frac{s}{\sigma}, \frac{\sqrt{x}}{\sigma}\right), \tag{17}$$

where $Q_1(\cdot,\cdot)$ is the first-order Marcum Q-function [41], and

$$s = \sqrt{\frac{\rho_e K \nu \mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\left|\frac{\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_2\right)}{\sin\left(\pi\frac{d}{\lambda}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\delta_2\right)}\right|, \tag{18}$$

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

$$\sigma^2=\frac{1}{2}\rho_e K N \nu \mu_{E_m}\left[1-\frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]. \quad (19)$$

In the case of non-colluding eavesdroppers, the eavesdropper with the strongest channel dominates the secrecy performance. Thus, the corresponding CDF of the eavesdropper SNR is derived as

$$\begin{aligned}F_{\gamma_E}(x)&=\Pr\left\{\max_{m\in\Phi_e}\gamma_{E_m}\le x\right\}\\&\overset{(a)}{=}\mathbb{E}_{\Phi_e}\left\{\prod_{m\in\Phi_e, r_m\le r_e}F_{\gamma_{E_m}}(x)\right\}\\&\overset{(b)}{=}\exp\left[-2\pi\lambda_e\int_0^{r_e}\left(1-F_{\gamma_{E_m}}(x)\right)r\,\mathrm{d}r\right]\\&\overset{(c)}{=}\exp\left[-2\pi\lambda_e\int_0^{r_e}Q_1\left(\varpi,\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)r\,\mathrm{d}r\right], \quad (20)\end{aligned}$$

where (a) follows from the i.i.d. characteristic of the eavesdroppers' SNRs and their independence from the point process Φ_e, (b) follows from the probability generating functional (PGFL) of the PPP [26, Eq. (4.55)], and (c) is obtained by using $\mu_{E_m}=\beta_0 r^{-\alpha_2}$ and defining the parameters

$$\begin{aligned}\varpi\triangleq\sqrt{2}&\left|\frac{\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_2\right)}{\sin\left(\pi\frac{d}{\lambda}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\delta_2\right)}\right|\\&\times\left[N\left(\frac{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}{\epsilon^2}-1\right)\right]^{-\frac{1}{2}}, \quad (21)\end{aligned}$$

$$\Xi\triangleq\sqrt{2}\left[NK\nu\beta_0\rho_e\left(1-\frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right)\right]^{-\frac{1}{2}}. \quad (22)$$

From the characterization in [41, Eq. (2)], we have the following approximation for the Marcum Q-function in (20): $Q_1\left(\varpi,\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)\simeq\exp\left[-\mathrm{e}^{v(\varpi)}\left(\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)^{\mu(\varpi)}\right]$, where $v(\varpi)$ and $\mu(\varpi)$ are polynomial functions of ϖ defined as $v(\varpi)=-0.840+0.327\varpi-0.740\varpi^2+0.083\varpi^3-0.004\varpi^4$ and $\mu(\varpi)=2.174-0.592\varpi+0.593\varpi^2-0.092\varpi^3+0.005\varpi^4$. Then, (20) is further calculated as

$$\begin{aligned}F_{\gamma_E}(x)&=\exp\left[-2\pi\lambda_e\int_0^{r_e}\exp\left[-\mathrm{e}^{v(\varpi)}\left(\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)^{\mu(\varpi)}\right]r\mathrm{d}r\right]\\&=\exp\left[-t_0\frac{\Gamma(t_1)-\Gamma(t_1,t_2x^{t_3})}{x^{t_4}}\right], \quad (23)\end{aligned}$$

where the last equality is obtained from [44, Eq. (3.326)] with the definitions $t_0=\frac{2\pi\lambda_e}{\frac{\alpha_2}{2}\mu(\varpi)\mathrm{e}^{\frac{4v(\varpi)}{\alpha_2\mu(\varpi)}}\Xi^{\frac{4}{\alpha_2}}}$, $t_1=\frac{2}{\frac{\alpha_2}{2}\mu(\varpi)}$, $t_2=\mathrm{e}^{v(\varpi)}\Xi^{\mu(\varpi)}r_e^{\frac{\alpha_2}{2}\mu(\varpi)}$, $t_3=\frac{\mu(\varpi)}{2}$, and $t_4=\frac{2}{\alpha_2}$.

Therefore, the PDF of the overall eavesdropper SNR can be further derived from (23) as

$$\begin{aligned}f_{\gamma_E}(x)=\frac{dF_{\gamma_E}(x)}{dx}&=t_0x^{-t_4-1}\left(t_4\gamma\left(t_1,t_2x^{t_3}\right)\right.\\&\left.-t_3\left(t_2x^{t_3}\right)^{t_1}\mathrm{e}^{-t_2x^{t_3}}\right)\mathrm{e}^{-t_0x^{-t_4}\gamma\left(t_1,t_2x^{t_3}\right)}. \quad (24)\end{aligned}$$

IV. Secrecy Outage Analysis

In this section, we apply the derived statistical properties of γ_D and γ_E in the above section to conduct the secrecy outage analysis of the RIS-aided MISO system.

A. Theoretical SOP Analysis

A popular metric for quantifying PLS is the SOP, which is defined as the probability that the instantaneous secrecy capacity falls below a target secrecy rate C_{th}. Mathematically, the SOP is evaluated by

$$\begin{aligned}\mathrm{SOP}&=\Pr\left(\ln(1+\gamma_D)-\ln(1+\gamma_E)<C_{\mathrm{th}}\right)\\&=\int_0^{\infty}F_{\gamma_D}\left((1+x)\varphi-1\right)f_{\gamma_E}(x)\,\mathrm{d}x, \quad (25)\end{aligned}$$

where $\varphi\triangleq\mathrm{e}^{C_{\mathrm{th}}}$. By substituting (10) and (24) into (25), the SOP can be easily expressed as follows

$$\mathrm{SOP}=\frac{1}{\Gamma(k)}t_0\left(t_4I_1-t_3t_2^{t_1}I_2\right), \quad (26)$$

where I_1 and I_2 are defined as

$$\begin{aligned}I_1=\int_0^{+\infty}&\gamma\left(k,\frac{\sqrt{\frac{((1+x)\varphi-1)}{\rho_d}}}{\theta}\right)x^{-t_4-1}\\&\times\gamma\left(t_1,t_2x^{t_3}\right)\mathrm{e}^{-t_0x^{-t_4}\gamma\left(t_1,t_2x^{t_3}\right)}\mathrm{d}x, \quad (27)\\I_2=\int_0^{+\infty}&\gamma\left(k,\frac{\sqrt{\frac{((1+x)\varphi-1)}{\rho_d}}}{\theta}\right)x^{-t_4-1}x^{t_1t_3}\\&\times\mathrm{e}^{-t_2x^{t_3}}\mathrm{e}^{-t_0x^{-t_4}\gamma\left(t_1,t_2x^{t_3}\right)}\mathrm{d}x. \quad (28)\end{aligned}$$

However, it is difficult to directly compute an accurate closed-form expression for (26), because (27) and (28) both involve an intractable integral. In order to analyze the secrecy performance, an approximate closed-form expression for the SOP is presented in *Proposition 2*.

Proposition 2: When $r_e\to\infty$, the SOP can be approximated as[2]

$$\begin{aligned}\mathrm{SOP}\simeq\ &1-\frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}\\&\times G_{0,p+4q}^{p+4q,0}\left(\frac{\left(t_0\Gamma(t_1)\varphi^{t_4}\right)^p}{p^p\left(4q\sqrt{\rho_d}\theta\right)^{4q}}\middle|\begin{matrix}-\\\Delta\end{matrix}\right), \quad (29)\end{aligned}$$

where $G_{s,t}^{m,n}(z)$ is Meijer's G function [44], $p,q\in\mathbb{Z}^+$, $p/q=\alpha_2$, and $\Delta=\left[0,\frac{1}{p},\ldots,\frac{p-1}{p},\frac{k}{4q},\frac{k+1}{4q},\ldots,\frac{k+4q-1}{4q}\right]$.

Proof: See Appendix E. ■

Proposition 2 provides an explicit relation between the secrecy outage probability and various system parameters. A number of interesting points can be made based on this expression.

[2]The assumption of a large r_e, similar to [42] and [43], only denotes an upper limit of distance and does not mean that the eavesdroppers must be far away from the RIS. Also, we will illustrate that the insights we obtained under this assumption are still applicable when r_e is relatively small in the simulations.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

Remark 3: The SOP in (29) is not a function of the transmit power P_T at the base station, which implies that increasing P_T does not enhance the system's secrecy performance. This is intuitive since an increase in P_T would yield a proportional increase in the transmit SNRs at both the legitimate user and eavesdroppers.

Proof: According to *Proposition 2*, we see that the transmit power P_T affects only the term $\frac{t_0^p}{\rho_d^{2q}}$ in (29), which is given by

$$\frac{t_0^p}{\rho_d^{2q}} = \left(\frac{2\pi\lambda_e}{\frac{\alpha_2}{2}\mu\left(\varpi\right)e^{\frac{4v(\varpi)}{\alpha_2\mu(\varpi)}}}\right)^p \frac{1}{\left(\Xi^2\rho_d\right)^{2q}} \propto \left(\frac{\rho_e}{\rho_d}\right)^{2q}. \quad (30)$$

This equality shows that the SOP depends on the ratio of the transmit SNRs at the legitimate user and the eavesdroppers, i.e., $\frac{\rho_e}{\rho_d}$, regardless of the specific values of P_T. ■

Remark 4: The SOP in (29) is mainly affected by the number of RIS reflecting elements, N, while the impact of the number of transmit antennas, K, is marginal. This is readily checked by calculating $\frac{t_0^p}{\theta^{4q}}$ in (29) because the other terms are obviously irrelevant to K. We obtain $\frac{t_0^p}{\theta^{4q}} = \left(\frac{2\pi\lambda_e}{\frac{\alpha_2}{2}\mu(\varpi)e^{\frac{4v(\varpi)}{\alpha_2\mu(\varpi)}}}\right)^p \frac{1}{(\Xi\theta)^{4q}}$, where $\Xi\theta = \frac{\chi}{\sqrt{N}}$ depends only on N, since the coefficient χ is independent of N and K.

In addition, *Proposition 2* is a general analysis of the SOP for any path loss exponent α_2. Some specific case studies are reported below. Note that other values of α_2 also admit closed-form expressions using (29).

Corollary 2: For the special case of $\alpha_2 = 2$, i.e., $p = 2$ and $q = 1$, which corresponds to free space propagation [45], the SOP in (29) reduces to

$$\mathrm{SOP} \simeq 1 - \frac{2^{k-1}}{\sqrt{\pi}\Gamma\left(k\right)} G_{0,3}^{3,0}\left(\frac{t_0\Gamma\left(t_1\right)\varphi}{4\rho_d\theta^2}\middle|_{0,\frac{k}{2},\frac{k+1}{2}}^{-}\right). \quad (31)$$

Corollary 3: For the special case of $\alpha_2 = 4$, i.e., $p = 4$ and $q = 1$, which is a common practical value for the path-loss exponent in outdoor urban environments [45], the SOP in (29) simplifies to the following expression

$$\mathrm{SOP} \simeq 1 - \frac{2}{\Gamma\left(k\right)}\left(\frac{t_0\Gamma\left(t_1\right)\sqrt{\varphi}}{\sqrt{\rho_d}\theta}\right)^{\frac{k}{2}} K_k\left(2\left(\frac{t_0\Gamma\left(t_1\right)\sqrt{\varphi}}{\sqrt{\rho_d}\theta}\right)^{\frac{1}{2}}\right), \quad (32)$$

where $K_\nu\left(\cdot\right)$ denotes the ν-th-order modified Bessel function of the second kind [44, Eq. (8.407)].

From (32), it is obvious that the SOP is a monotonically increasing function w.r.t. $\frac{t_0}{\sqrt{\rho_d}\theta} = \sqrt{\frac{\rho_e}{\rho_d}}\lambda_e d_{RD}^2\beta\left(N,\epsilon\right)$ with fixed k, where $\beta\left(N,\epsilon\right)$ consists of the parameters N, ϵ, and constant terms. Some new observations can thus be obtained in addition to the results presented in *Remark 3* and *Remark 4*. We evince that the SOP increases with the density parameter λ_e, which implies that a larger density of randomly located eavesdroppers leads to a negative effect on the secrecy performance. Moreover, we can also see that the SOP is only related to the distance of the RIS-D link, i.e., d_{RD}. Therefore, when the locations of the eavesdroppers are unknown, this suggests that the RIS should be deployed closer to the legitimate user than to the base station.

B. Secrecy Diversity Order Analysis

In order to derive the secrecy diversity order and gain further insights, we adopt the analytical framework proposed in [46] where the secrecy diversity order is defined as follows

$$d_s = -\lim_{\rho_d\to\infty}\frac{\log \mathrm{SOP}^\infty}{\log\rho_d}, \quad (33)$$

where SOP^∞ represents the asymptotic value of the SOP in (29) for $\rho_d \to \infty$, and the transmit SNR ρ_e is fixed.

According to [47, Eq. (07.34.06.0006.01)], the SOP in (29) can be expanded as

$$\begin{aligned}\mathrm{SOP} \simeq& 1 - \frac{1}{\Gamma\left(k\right)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}} \times G_{0,p+4q}^{p+4q,0}\left(x\middle|_{\Delta}^{-}\right)\\ =& 1 - \frac{1}{\Gamma\left(k\right)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}\times\\ &\sum_{l=1}^{p+4q}\prod_{j=1,j\neq l}^{p+4q}\Gamma\left(\Delta\left(j\right)-\Delta\left(l\right)\right)x^{\Delta(l)}\left(1+\mathcal{O}\left(x\right)\right), \quad (34)\end{aligned}$$

where $x = \frac{\left(t_0\Gamma(t_1)\varphi^{t_4}\right)^p}{p^p\left(4q\sqrt{\rho_d}\theta\right)^{4q}} \to 0$, and $\mathcal{O}$ denotes higher order terms.

When the transmit SNR from S to D is sufficiently large, i.e., $\rho_d \to \infty$, only the dominant terms $l = 0$ and $l = 1$ in the summation of (34) are retained, which yields the asymptotic SOP as expressed in (35), shown at the bottom of the next page, where the last step is calculated by applying Gauss' multiplication formula [48, Eq. (6.1.20)].

Remark 5: By substituting (35) into (33), the secrecy diversity order is obtained as $\frac{2}{\alpha_2}$, which only depends on the path loss exponent of the RIS-to-ground links. This implies that the secrecy diversity order of this system improves when the RIS is deployed to provide better LoS links to the terminals.

V. Ergodic Secrecy Capacity Analysis

In this section, we obtain closed-form expressions for both the theoretical and asymptotic ESC. We also characterize the impact of various parameters, including N, K, P_T, and λ_e, on the ESC performance of the system.

A. Theoretical ESC Analysis

The ESC is an alternative fundamental metric that denotes the statistical average of the secrecy rate over fading channels, which is mathematically expressed as

$$C_s = \mathbb{E}\left\{\left[\log_2\left(1+\gamma_D\right) - \log_2\left(1+\gamma_E\right)\right]^+\right\}. \quad (36)$$

Given the received SNRs at both the legitimate user and eavesdroppers in Section III, we first derive an approximate expression for the ESC in the following proposition.

Proposition 3: The ESC for the RIS-assisted system is evaluated as

$$\bar{C}_s = \left[R_D - R_E\right]^+, \quad (37)$$

where R_D and R_E are the ergodic rates of the legitimate user D and the eavesdroppers E, respectively, and are expressed as

$$R_D = \frac{1}{\ln 2}\frac{1}{\Gamma\left(k\right)}\frac{2^{k-\frac{1}{2}}}{\sqrt{2\pi}}G_{2,4}^{4,1}\left(\frac{1}{4\rho_d\theta^2}\middle|_{0,0,\frac{k}{2},\frac{k+1}{2}}^{0,1}\right), \quad (38)$$

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

$$R_E = \frac{1}{\ln 2}\int_0^{+\infty} \frac{1-\exp\left[-t_0\frac{\Gamma(t_1)-\Gamma\left(t_1,t_2x^{t_3}\right)}{x^{t_4}}\right]}{1+x}\mathrm{d}x. \quad (39)$$

Proof: Using Jensen's inequality, an effective approximation of the ESC can be written as [49] and [50]

$$\bar{C}_s = \left[\mathbb{E}\{\log_2(1+\gamma_D)-\log_2(1+\gamma_E)\}\right]^+ = \left[R_D - R_E\right]^+, \quad (40)$$

where R_D and R_E are respectively calculated as follows

$$\begin{aligned} R_D &= \mathbb{E}\{\log_2(1+\gamma_D)\} = \frac{1}{\ln 2}\int_0^{+\infty}\frac{\bar{F}_{\gamma_D}(x)}{1+x}dx \\ &= \frac{1}{\ln 2}\int_0^{+\infty}\frac{\Gamma\left(k,\frac{\sqrt{x/\rho_d}}{\theta}\right)}{\Gamma(k)(1+x)}\mathrm{d}x, \quad (41) \\ R_E &= \mathbb{E}\{\log_2(1+\gamma_E)\} = \frac{1}{\ln 2}\int_0^{+\infty}\frac{\bar{F}_{\gamma_E}(x)}{1+x}dx \\ &= \frac{1}{\ln 2}\int_0^{+\infty}\frac{1-\exp\left[-t_0\frac{\Gamma(t_1)-\Gamma\left(t_1,t_2x^{t_3}\right)}{x^{t_4}}\right]}{1+x}\mathrm{d}x. \quad (42) \end{aligned}$$

Using [47, Eq. (07.34.03.0613.01)] and [44, Eq. (9.31.5)], (41) is equivalently given by

$$\begin{aligned} R_D &= \frac{1}{\ln 2}\frac{1}{\Gamma(k)}\int_0^{+\infty}\frac{1}{1+x}G_{1,2}^{2,0}\left(\frac{\sqrt{x}}{\sqrt{\rho_d}\theta}\middle|\begin{matrix}1\\k,0\end{matrix}\right)\mathrm{d}x \\ &= \frac{1}{\ln 2}\frac{1}{\Gamma(k)}\frac{2^{k-\frac{1}{2}}}{\sqrt{2\pi}}G_{3,5}^{5,1}\left(\frac{1}{4\rho_d\theta^2}\middle|\begin{matrix}0,\frac{1}{2},1\\0,0,\frac{1}{2},\frac{k}{2},\frac{k+1}{2}\end{matrix}\right), \quad (43) \end{aligned}$$

where the integral of (43) is evaluated through [47, Eq. (07.34.21.0086.01)].

By further applying the identity given in [44, Eq. (9.31.1)], a simplified expression for the ergodic rate of the legitimate user D is obtained in (38). The proof is thus complete. ■

As a general analysis, the ergodic rate R_E given by (39) involves an intractable integral that is difficult to compute. So in the sequel we focus on a few relevant cases for widely-used values of path loss exponents where significant simplification is possible and intuitive ergodic secrecy rate expressions can be obtained.

Corollary 4: For $r_e \to \infty$ and $\alpha_2 = 2$, which corresponds to the free space model [45], the ESC in (37) reduces to the closed-form expression as

$$\bar{C}_s = \left[R_D - R_{E,1}\right]^+, \quad (44)$$

where R_D is given in closed-form by (38) and

$$\begin{aligned} R_{E,1} &= \frac{1}{\ln 2}\int_0^{+\infty}\frac{1-\exp\left[-t_0\Gamma(t_1)x^{-1}\right]}{1+x}\mathrm{d}x \\ &= \frac{1}{\ln 2}\{\gamma + \ln(t_0\Gamma(t_1)) + \exp[t_0\Gamma(t_1)] \\ &\quad \times (\mathrm{Shi}(t_0\Gamma(t_1)) - \mathrm{Chi}(t_0\Gamma(t_1)))\}, \quad (45) \end{aligned}$$

where γ denotes Euler's constant, and $\mathrm{Shi}(\cdot)$ and $\mathrm{Chi}(\cdot)$ are the hyperbolic sine and cosine integral functions, respectively [44, Eq. (8.221)].

Corollary 5: For $r_e \to \infty$ and $\alpha_2 = 4$, which is a common value for the path-loss exponent in outdoor urban environments [45], the ESC in (37) reduces to the closed-form expression

$$\bar{C}_s = \left[R_D - R_{E,2}\right]^+, \quad (46)$$

where R_D is the same as (38), and

$$\begin{aligned} R_{E,2} &= \frac{1}{\ln 2}\int_0^{+\infty}\frac{1-\exp\left[-t_0\Gamma(t_1)x^{-\frac{1}{2}}\right]}{1+x}\mathrm{d}x \\ &= \frac{1}{\ln 2}\frac{1}{\sqrt{\pi}}G_{2,4}^{3,2}\left(\frac{t_0^2\Gamma(t_1)^2}{4}\middle|\begin{matrix}1,1\\\frac{1}{2},1,1,0\end{matrix}\right). \quad (47) \end{aligned}$$

B. Asymptotic ESC Analysis

In order to obtain useful insights for system design, we analyze the asymptotic ESC at high SNR in this subsection. For the sake of tractability, we first derive new expressions for bounding the ergodic rate R_D in the following lemma.

Lemma 3: The ergodic rate R_D can be upper bounded by

$$R_D^{\mathrm{U}} = \log_2\left(1+\rho_d K N \nu \mu_D\left(1+\frac{\pi}{4}(N-1)\frac{\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}{\epsilon+1}\right)\right). \quad (48)$$

Proof: See Appendix F. ■

By applying *Lemma 3*, we are ready to give the following corollary quantitatively analyzing the asymptotic ESC in the high SNR region.

Corollary 6: In the high SNR regime, the ESC in (44) is further simplified as follows

$$\bar{C}_s \to \left\{\log_2\left(\frac{\sigma_E^2}{\sigma_D^2}\right) + \log_2\left(\frac{d_{RD}^{-2}}{\pi\lambda_e}\right) - \frac{\gamma}{\ln 2} + C\right.$$

$$\begin{aligned} \mathrm{SOP}^{\infty} &= 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}\left[\prod_{j=2}^{p+4q}\Gamma(\Delta(j))x^0 + \prod_{j=1,j\neq 2}^{p+4q}\Gamma\left(\Delta(j)-\frac{1}{p}\right)x^{\frac{1}{p}}\right] \\ &= 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}\left[\prod_{j=0}^{p-1}\Gamma\left(\frac{1}{p}+\frac{j}{p}\right)\prod_{j=0}^{4q-1}\Gamma\left(\frac{k}{4q}+\frac{j}{4q}\right) - p\prod_{j=0}^{p-1}\Gamma\left(\frac{1}{p}+\frac{j}{p}\right)\right. \\ &\quad \left.\times\prod_{j=0}^{4q-1}\Gamma\left(\frac{k}{4q}-\frac{1}{p}+\frac{j}{4q}\right)x^{\frac{1}{p}}\right] = \frac{t_0\Gamma(t_1)\varphi^{\frac{2}{\alpha_2}}\Gamma\left(k-\frac{4}{\alpha_2}\right)}{\theta^{\frac{4}{\alpha_2}}\Gamma(k)}(\rho_d)^{-\frac{2}{\alpha_2}}, \quad (35) \end{aligned}$$

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

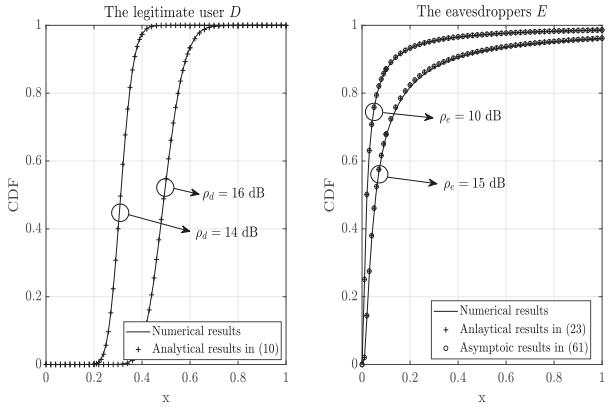

Fig. 2. The CDF of the received SNRs at the legitimate user D and the eavesdroppers E, respectively.

$$+\log_2\left(\frac{1+(N-1)\frac{\pi}{4}\frac{1}{\epsilon+1}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}{1-\frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\right)\Bigg\}^+, \quad (49)$$

where $C=\log_2\frac{\mu(\varpi)\mathrm{e}^{\frac{2\upsilon(\varpi)}{\mu(\varpi)}}}{\Gamma\left(\frac{2}{\mu(\varpi)}\right)}$ is a constant.

Proof: See Appendix G. ■

From *Corollary 6*, we have the following remarks on the impact of key system parameters, including N, K, P_T, and λ_e, on the secrecy performance.

Remark 6: By direct inspection of (49), it is evident that the asymptotic ESC does not depend on the number of transmit antennas, K, but it increases with the number of RIS reflecting elements, N. This suggests that deploying more RIS reflecting elements rather than transmit antennas achieves better secrecy performance. Moreover, for large N, the asymptotic ESC scales logarithmically with N.

Remark 7: Corollary 6 also indicates that the asymptotic ESC is not a function of d_{SR} whereas it increases with decreasing d_{RD}. This result might seem a bit counterintuitive at first, but it actually makes sense and can be explained as follows. When the distance from the base station to the RIS decreases, the received SNRs at both the legitimate user and the eavesdroppers increase by the same amount, and they offset each other. Therefore, if the locations of the eavesdroppers are unknown, this suggests that the RIS should be deployed closer to the legitimate user than to the base station.

Remark 8: In agreement with *Remark 3*, the asymptotic ESC in (49) is only related to the ratio of the noise power at the legitimate user and the eavesdroppers $\frac{\sigma_D^2}{\sigma_E^2}$, and is independent of the transmit power P_T. In addition, in line with intuition, the asymptotic ESC decreases when the density of the homogeneous PPP λ_e increases. We see that the effect of λ_e on the ESC is additive, and is proportional to $\log_2(1/\lambda_e)$.

VI. Numerical Results

In this section, Monte-Carlo simulations are presented to validate the analytical results. All the simulation results are obtained by averaging over 10^5 independent channel realizations. We first verify the approximations of the received SNR distributions at the legitimate user and the eavesdroppers in Fig. 2. The simulation parameters are set to $K=16$, $N=36$, $\alpha_1=\alpha_2=2$, $\epsilon=2$, $d_{SR}=30$ m, $d_{RD}=40$ m, $r_e=200$ m, and $\lambda_e=10^{-3}$. We see from Fig. 2 that both the analytical CDF of the received SNRs at the legitimate user D and the eavesdroppers E characterized by (10) and (23), respectively, match well with the numerical curves. In addition, the asymptotic CDF of the received SNR at the eavesdroppers E calculated from (61) for large r_e is also verified to be quite accurate.

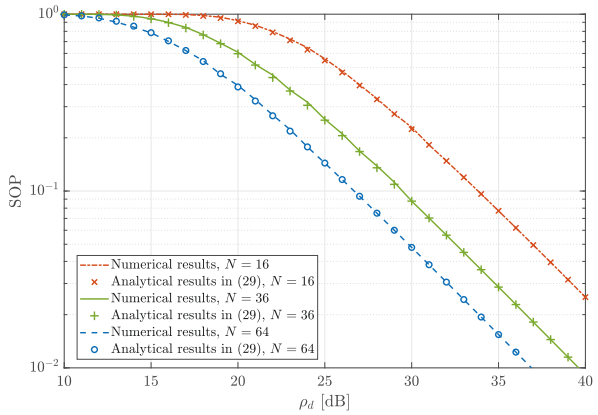

Fig. 3. The SOP versus ρ_d, with $K=16$, $\alpha_1=\alpha_2=2$, $\epsilon=2$, $d_{SR}=30$ m, $d_{RD}=40$ m, $r_e=200$ m, $\lambda_e=10^{-3}$, $C_{\text{th}}=0.05$, and $\rho_e=30$ dB.

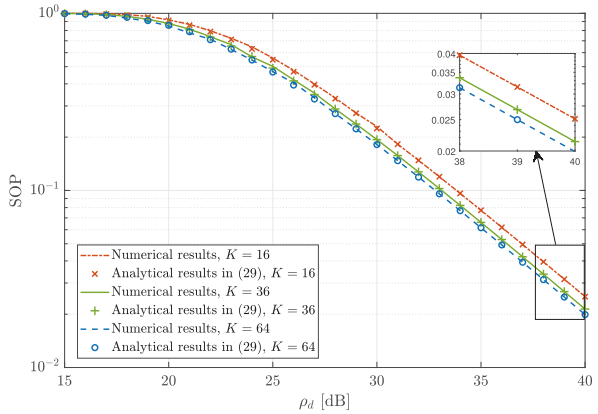

Fig. 4. The SOP versus ρ_d, with $N=16$, $\alpha_1=\alpha_2=2$, $\epsilon=2$, $d_{SR}=30$ m, $d_{RD}=40$ m, $r_e=200$ m, $\lambda_e=10^{-3}$, $C_{\text{th}}=0.05$, and $\rho_e=30$ dB.

A. Secrecy Outage Probability

In this subsection, we compare the SOP obtained from Monte-Carlo simulations and the analytical results calculated from (29). Fig. 3 and Fig. 4 plot the SOP versus the transmit SNR ρ_d for different values of N and K, respectively. Again, the analytical expressions in (29) match very well with the numerical results, and the SOP always decreases as the transmit SNR ρ_d increases. Furthermore, as expected from *Remark 4*, the SOP obviously decreases as N increases. However, the SOP remains almost the same when K increases with fixed N, which means that the impact of the number of transmit antennas on the secrecy outage performance is negligible.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

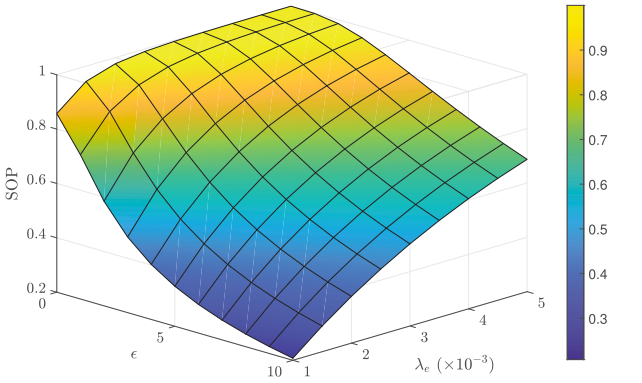

Fig. 5. The SOP versus ϵ and λ_e, with $K = 16$, $N = 36$, $\alpha_1 = \alpha_2 = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $C_{\text{th}} = 0.05$, $\rho_d = 20$ dB, and $\rho_e = 30$ dB.

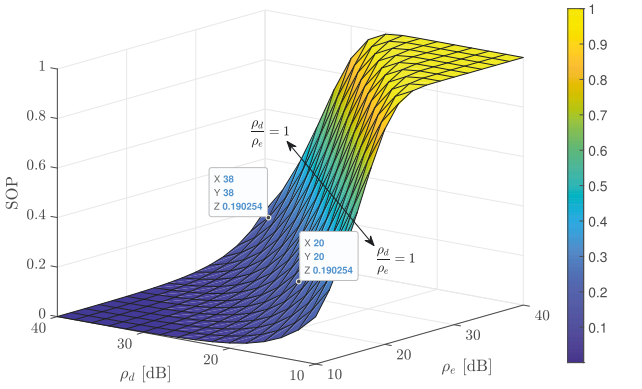

Fig. 6. The SOP versus ρ_d and ρ_e, with $K = 16$, $N = 16$, $\alpha_1 = \alpha_2 = 2$, $\epsilon = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $\lambda_e = 10^{-3}$, and $C_{\text{th}} = 0.05$.

Fig. 5 depicts the SOP as a function of the Rician factor ϵ and the eavesdropper density λ_e. It is observed that the SOP improves as ϵ increases. This is because with a large Rician factor, the channels are dominated by the LoS component with better link quality than NLoS. Additionally, it is noteworthy that the SOP increases with λ_e, since a larger λ_e leads to more eavesdroppers which increases the likelihood that the worst-case eavesdropper obtains higher quality information.

Fig. 6 illustrates the SOP as a function of the transmit SNRs ρ_d and ρ_e. It is clearly shown that increasing ρ_d and decreasing ρ_e improve the SOP performance. We can further observe that the SOP remains the same when the ratio of the transmit SNRs at the legitimate user and the eavesdroppers, i.e., $\frac{\rho_d}{\rho_e}$, is kept fixed. This implies that increasing the transmit power P_T will not help improve the secrecy outage performance of the system, which is consistent with *Remark 3*.

Fig. 7 shows the SOP versus the transmit SNR ρ_d for various values of the path loss exponents α_1 and α_2. It can be seen that the slope of the secrecy outage curves is determined by α_2, which becomes less steep as α_2 increases. Besides, according to the definition in (33), the secrecy diversity order presented in *Remark 5* can be demonstrated by calculating the negative slope of the SOP curves on a log-log scale.

B. Ergodic Secrecy Capacity

In this subsection, we compare the ESC obtained from Monte-Carlo simulations with the analytical and asymptotic

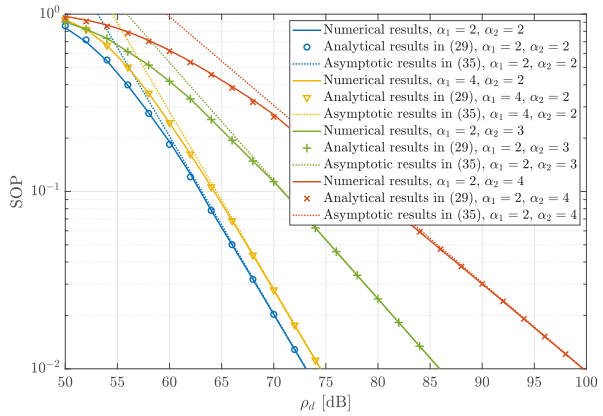

Fig. 7. The SOP versus ρ_d, with $K = 16$, $N = 16$, $\epsilon = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $\lambda_e = 10^{-3}$, $C_{\text{th}} = 0.05$, and $\rho_e = 60$ dB.

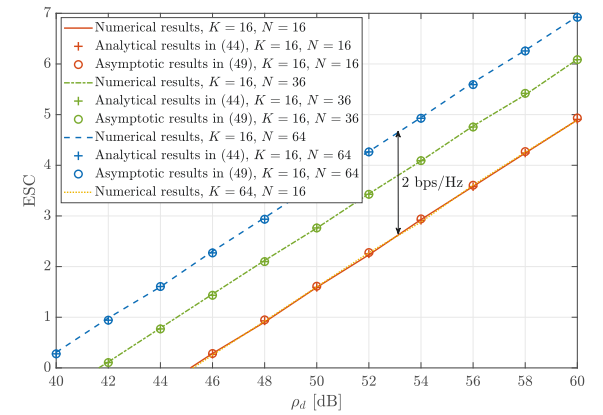

Fig. 8. The ESC versus ρ_d, with $\alpha_1 = \alpha_2 = 2$, $\epsilon = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $\lambda_e = 10^{-3}$, and $\rho_e = 50$ dB.

results calculated from (44) and (49), respectively. Fig. 8 illustrates the ESC versus the transmit SNR ρ_d for different values of N and K. We can see that both the analytical and asymptotic expressions match well with the numerical results, and the ESC increases with ρ_d. As expected from *Remark 6*, we can observe that the ESC at high SNR is independent of the number of transmit antennas, K, but obviously increases with the number of RIS reflecting elements, N. The ESC increases by approximately 2 bps/Hz when the number of RIS reflecting elements increases by a factor of 4, validating the conclusions presented in *Remark 6*, i.e., the ESC increases logarithmically with the number of RIS reflecting elements.

Fig. 9 plots the ESC as a function of the transmit SNRs ρ_d and ρ_e. First, similar to the results shown in Fig. 6, we see that increasing ρ_d and decreasing ρ_e both improve the secrecy performance. Also, as predicted in *Remark 8*, the ESC remains constant for a fixed ratio $\frac{\rho_d}{\rho_e}$, regardless of the specific value of the transmit power P_T. In addition, in Fig. 9, when the ratio $\frac{\rho_d}{\rho_e}$ increases by a factor of 4, the ESC increases by 2 bps/Hz, which confirms the results derived in (49).

Fig. 10 shows the ESC as a function of the distances d_{SR} and d_{RD}. It is clear that the ESC improves as d_{RD} decreases, and it keeps unchanged with arbitrary variation of d_{SR}, which has been validated by *Remark 7*. This phenomenon can be explained by the fact that decreasing the distance from the base

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

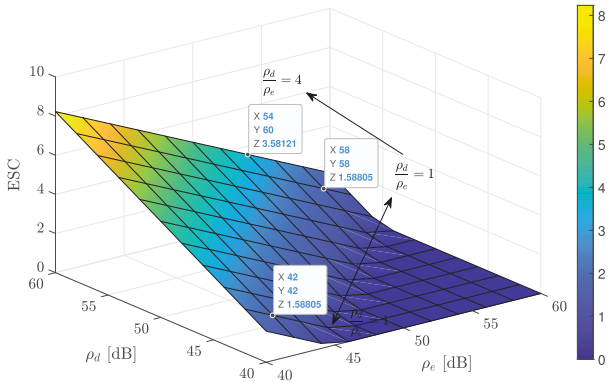

Fig. 9. The ESC versus ρ_d and ρ_e, with $K = 16$, $N = 16$, $\alpha_1 = \alpha_2 = 2$, $\epsilon = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, and $\lambda_e = 10^{-3}$.

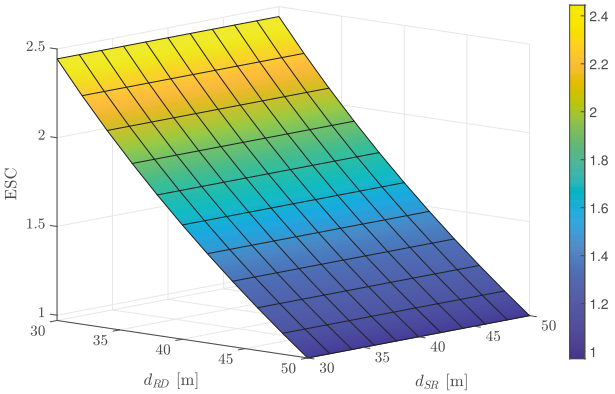

Fig. 10. The ESC versus d_{SR} and d_{RD}, with $K = 16$, $N = 16$, $\alpha_1 = \alpha_2 = 2$, $\epsilon = 2$, $r_e = 200$ m, $\lambda_e = 10^{-3}$, $\rho_d = 50$ dB, and $\rho_e = 50$ dB.

station to the RIS will simultaneously increase the received SNRs for both the legitimate user and the eavesdroppers.

Fig. 11 presents the ESC versus the density λ_e of the randomly located eavesdroppers in the logarithmic domain. It is observed that the ESC decreases linearly with $\log_2(\lambda_e)$. This behavior is due to the fact that a larger λ_e results in the presence of more eavesdroppers within a fixed range, which degrades the secrecy performance. In addition, it can also be seen from Fig. 11 that the ESC increases with the Rician factor ϵ. This is because the channels are mainly influenced by the LoS component when the Rician factor is large.

C. Cases for A Relatively Small r_e and Rician Fading Model

In this subsection, we verify the generality of the analytical results of the SOP and ESC with a relatively small value of r_e, i.e., $r_e = 50$ m, and under the assumption that the S-RIS and RIS-i channels both follow Rician fading, expressed as

$$\mathbf{H}_{SR} = \sqrt{\nu}\left(\sqrt{\frac{\epsilon_1}{\epsilon_1+1}}\overline{\mathbf{H}}_{SR} + \sqrt{\frac{1}{\epsilon_1+1}}\widetilde{\mathbf{H}}_{SR}\right), \tag{50}$$

$$\mathbf{h}_{Ri} = \sqrt{\mu_i}\left(\sqrt{\frac{\epsilon_2}{\epsilon_2+1}}\overline{\mathbf{h}}_{Ri} + \sqrt{\frac{1}{\epsilon_2+1}}\widetilde{\mathbf{h}}_{Ri}\right), \tag{51}$$

where ϵ_1 and ϵ_2 are the Rician factors for the S-RIS and RIS-i channels, respectively. Note that when the Rician factor ϵ_1 is large, (50) simplifies to the LoS model we consider in (1). Therefore, the Rician factor ϵ_1 is set to be small, e.g., $\epsilon_1 = 2$.

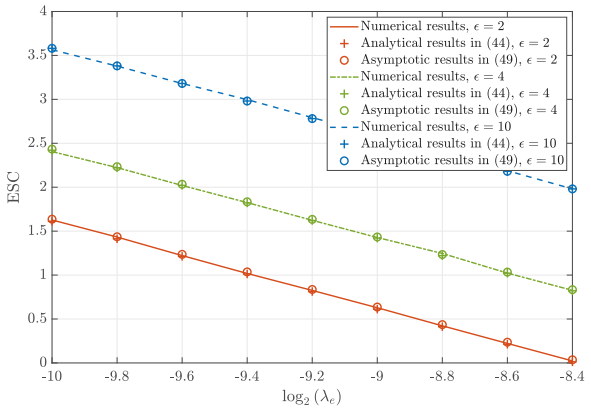

Fig. 11. The ESC versus $\log_2(\lambda_e)$, with $K = 16$, $N = 16$, $\alpha_1 = \alpha_2 = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $\rho_d = 50$ dB, and $\rho_e = 50$ dB.

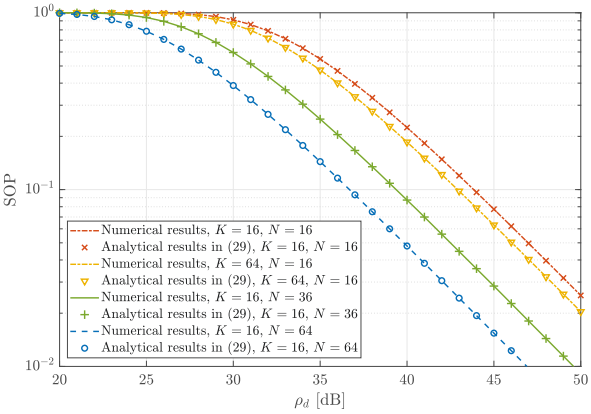

Fig. 12. The SOP versus ρ_d, with $\alpha_1 = \alpha_2 = 2$, $\epsilon_1 = \epsilon_2 = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 50$ m, $\lambda_e = 10^{-2}$, $C_{\text{th}} = 0.05$, and $\rho_e = 30$ dB.

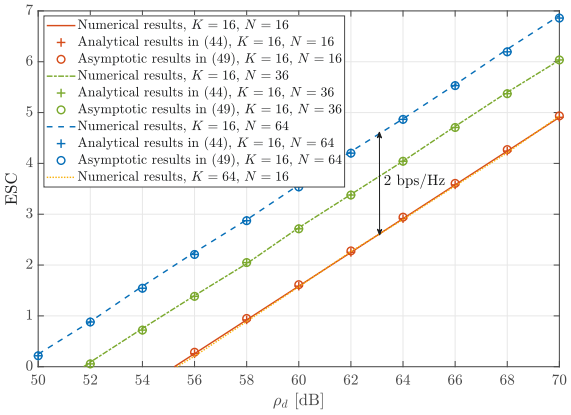

Fig. 13. The ESC versus ρ_d, with $\alpha_1 = \alpha_2 = 2$, $\epsilon_1 = \epsilon_2 = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 50$ m, $\lambda_e = 10^{-2}$, and $\rho_e = 50$ dB.

As shown in Fig. 12 and Fig. 13, it can be seen that the numerical results with small r_e and Rician fading model still match well with the analytical results under the assumption of large r_e and LoS model. Also, the observations that the SOP and ESC are mainly affected by the number of RIS reflecting

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

elements rather than the number of transmit antennas, which is obtained with large r_e and LoS model, are also applicable.

VII. Conclusion

In this paper, the secrecy performance of an RIS-assisted communication system with spatially random eavesdroppers was studied. Specifically, the exact distributions of the received SNRs at the legitimate user and the eavesdroppers were first derived. Then, based on these distributions, the closed-form SOP and ESC expressions were derived. Furthermore, a high-SNR secrecy diversity order and the asymptotic ESC analysis have also been conducted. The obtained results quantify the impact of key parameters on the secrecy performance and provide insightful guidelines for system design. Several simulations were provided to demonstrate the obtained results.

Appendix A
Proof of Theorem 1

For the transmit beamformer $\mathbf{f} = \frac{\mathbf{g}_D}{\|\mathbf{g}_D^H\|}$, we compute the optimal reflecting phase shifts at the RIS by maximizing the received signal power as follows

$$\begin{aligned}\boldsymbol{\Theta}^{\text{opt}} &= \arg\max_{\boldsymbol{\Theta}} \left|\mathbf{g}_D^H\mathbf{f}\right|^2 = \arg\max_{\boldsymbol{\Theta}} \left\|\mathbf{h}_{RD}^H\boldsymbol{\Theta}\mathbf{H}_{SR}\right\|^2 \\ &= \arg\max_{\boldsymbol{\Theta}} \left|\mathbf{h}_{RD}^H\boldsymbol{\Theta}\mathbf{a}_{N,SR}\right|^2 \left\|\mathbf{a}_{K,SR}^H\right\|^2 \\ &\overset{(\mathrm{d})}{=} \arg\max_{\boldsymbol{\Theta}} \left|\boldsymbol{\theta}^H \operatorname{diag}\left\{\mathbf{h}_{RD}^H\right\}\mathbf{a}_{N,SR}\right|^2 \\ &= \arg\max_{\boldsymbol{\Theta}} \left|\sum_{n=1}^{N} h_{RD}^*(n)\,\mathrm{a}_{N,SR}(n)\,\mathrm{e}^{j\theta_n}\right|^2, \end{aligned} \tag{52}$$

where (d) follows by defining $\boldsymbol{\theta}^H = \left[\mathrm{e}^{j\theta_1}, \ldots, \mathrm{e}^{j\theta_n}, \ldots, \mathrm{e}^{j\theta_N}\right]$, and using the identity $\left\|\mathbf{a}_{K,SR}^H\right\|^2 = K$. From (52), we see that maximizing $\left|\mathbf{g}_D^H\mathbf{f}\right|^2$ is equivalent to ensuring the phases of N complex RVs $h_{RD}^*(n)\,\mathrm{a}_{N,SR}(n)\,\mathrm{e}^{j\theta_n}$ being identical. Therefore, the optimal RIS phase shifts are given by

$$\theta_n^{\text{opt}} = -\angle\left(h_{RD}^*(n)\,\mathrm{a}_{N,SR}(n)\right), \tag{53}$$

and the corresponding reflection matrix can be easily obtained as (8). This completes the proof.

Appendix B
Proof of Lemma 1

Since $|h_{RD}(1)|, |h_{RD}(2)|, \ldots, |h_{RD}(N)|$ are i.i.d. RVs, the mean and variance of the RV $|\mathrm{A}| = \sqrt{K\nu}\sum_{n=1}^{N}|h_{RD}(n)|$ can be respectively calculated as

$$\mathbb{E}\{|\mathrm{A}|\} = \sqrt{K\nu}N \cdot \mathbb{E}\{|h_{RD}(n)|\}, \tag{54}$$

and

$$\operatorname{Var}\{|\mathrm{A}|\} = K\nu N \cdot \operatorname{Var}\{|h_{RD}(n)|\}, \tag{55}$$

where $|h_{RD}(n)| \sim Rice\left(\sqrt{\frac{\mu_D\epsilon}{\epsilon+1}}, \sqrt{\frac{1}{2}\frac{\mu_D}{\epsilon+1}}\right)$, whose mean and variance are given as $\mathbb{E}\{|h_{RD}(n)|\} = \sqrt{\frac{\mu_D}{\epsilon+1}}\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)$ and $\operatorname{Var}\{|h_{RD}(n)|\} = \frac{\mu_D}{\epsilon+1}\left[1+\epsilon-\frac{\pi}{4}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2\right]$, respectively. Therefore, according to [40], the RV $|\mathrm{A}|$ can be approximated by a Gamma distributed RV with shape parameter $k = \frac{\mathbb{E}\{|\mathrm{A}|\}^2}{\operatorname{Var}\{|\mathrm{A}|\}}$ and scale parameter $\theta = \frac{\operatorname{Var}\{|\mathrm{A}|\}}{\mathbb{E}\{|\mathrm{A}|\}}$, which yields the desired result in (9).

Appendix C
Proof of Proposition 1

The received SNR at E_m can be written as

$$\begin{aligned}\gamma_{E_m} &= \rho_e\left|\mathbf{h}_{RE_m}^H\boldsymbol{\Theta}\mathbf{H}_{SR}\mathbf{f}\right|^2 \\ &\overset{(\mathrm{e})}{=} \rho_e\left|\mathbf{h}_{RE_m}^H\boldsymbol{\Theta}\mathbf{H}_{SR}\frac{\mathbf{H}_{SR}^H\boldsymbol{\Theta}^H\mathbf{h}_{RD}}{\left\|\mathbf{h}_{RD}^H\boldsymbol{\Theta}\mathbf{H}_{SR}\right\|}\right|^2 \\ &= \rho_e\nu\frac{\left|\mathbf{h}_{RE_m}^H\boldsymbol{\Theta}\mathbf{a}_{N,SR}\right|^2\left|\mathbf{a}_{N,SR}^H\boldsymbol{\Theta}^H\mathbf{h}_{RD}\right|^2\left\|\mathbf{a}_{K,SR}^H\right\|^4}{\left|\mathbf{h}_{RD}^H\boldsymbol{\Theta}\mathbf{a}_{N,SR}\right|^2\left\|\mathbf{a}_{K,SR}^H\right\|^2} \\ &= \rho_e K\nu\left|\mathbf{h}_{RE_m}^H\boldsymbol{\Theta}\mathbf{a}_{N,SR}\right|^2 \\ &= \rho_e K\nu\left|\sum_{n=1}^{N} h_{RE_m}^*(n)\,\mathrm{a}_{N,SR}(n)\,\mathrm{e}^{j\theta_n}\right|^2 \\ &\overset{(\mathrm{f})}{=} \rho_e K\nu\left|\sum_{n=1}^{N} h_{RE_m}^*(n)\,\mathrm{e}^{-j\angle h_{RD}^*(n)}\right|^2, \end{aligned} \tag{56}$$

where (e) is obtained by substituting the expressions of $\mathbf{f}$ and $\mathbf{g}_D^H$, and (f) comes from (53) with $|\mathrm{a}_{N,SR}(n)| = 1$.

Appendix D
Proof of Lemma 2

From (2), we see that $h_{Ri}(n) \sim \mathcal{CN}\left(\sqrt{\frac{\mu_i\epsilon}{\epsilon+1}}\bar{h}_{Ri}(n), \frac{\mu_i}{\epsilon+1}\right)$, and $|h_{Ri}(n)| \sim Rice\left(\sqrt{\frac{\mu_i\epsilon}{\epsilon+1}}, \sqrt{\frac{1}{2}\frac{\mu_i}{\epsilon+1}}\right)$. Then, it can be easily obtained that $\mathbb{E}\{h_{Ri}(n)\} = \sqrt{\frac{\mu_i\epsilon}{\epsilon+1}}\mathrm{a}_{N,Ri}(n)$, $\mathbb{E}\{|h_{Ri}(n)|\} = \sqrt{\frac{\mu_i}{\epsilon+1}}\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)$, and $\mathbb{E}\{|h_{Ri}(n)|^2\} = \mu_i$. It follows that

$$\mathbb{E}\{\mathrm{e}^{-j\angle h_{RD}^*(n)}\} = \left(\frac{\mathbb{E}\{h_{RD}^*(n)\}}{\mathbb{E}\{|h_{RD}^*(n)|\}}\right)^* = \frac{\sqrt{\epsilon}\mathrm{a}_{N,RD}(n)}{\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)}. \tag{57}$$

Therefore, the mean and variance of the RV $x_n = h_{RE_m}^*(n)\,\mathrm{e}^{-j\angle h_{RD}^*(n)}$ can be calculated, respectively, as

$$\mathbb{E}\{x_n\} = \sqrt{\frac{\mu_{E_m}\epsilon^2}{\epsilon+1}}\frac{\mathrm{a}_{N,RE_m}^*(n)\,\mathrm{a}_{N,RD}(n)}{\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)}, \tag{58}$$

and

$$\operatorname{Var}\{x_n\} = \mu_{E_m}\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]. \tag{59}$$

It can be seen from (58) that $\mathbb{E}\{x_n\}$ depends on n, which means that x_n is not identically distributed. Therefore, the distribution of the RV $Z_{E_m} = \sum_{n=1}^{N} x_n$ cannot be directly approximated as Gaussian by applying the central limit theorem (CLT). In order to characterize the

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

distribution of Z_{E_m}, we first define a new RV $x_n - \mathbb{E}\{x_n\}$, and it can be easily verified that $x_1 - \mathbb{E}\{x_1\}, x_2 - \mathbb{E}\{x_2\}, \ldots, x_N - \mathbb{E}\{x_N\}$ are i.i.d. RVs with zero mean and variance $\mathrm{Var}\{x_n\}$. By virtue of the CLT, $\sum_{n=1}^{N}(x_n - \mathbb{E}\{x_n\})$ converges in distribution to a complex Gaussian RV with zero mean and variance $N \cdot \mathrm{Var}\{x_n\}$. Then, we can obtain that $Z_{E_m} = \sum_{n=1}^{N} x_n = \sum_{n=1}^{N}(x_n - \mathbb{E}\{x_n\}) + \sum_{n=1}^{N}\mathbb{E}\{x_n\} \sim \mathcal{CN}\left(\sum_{n=1}^{N}\mathbb{E}\{x_n\}, N \cdot \mathrm{Var}\{x_n\}\right)$, where

$$\begin{aligned}\sum_{n=1}^{N}\mathbb{E}\{x_n\} &= \sqrt{\frac{\mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\sum_{n=1}^{N}\mathrm{a}^{*}_{N,RE_m}(n)\,\mathrm{a}_{N,RD}(n)\\ &\overset{(g)}{=} \sqrt{\frac{\mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\sum_{0\le x,y\le\sqrt{N}-1}\mathrm{e}^{j2\pi\frac{d}{\lambda}(x\delta_1+y\delta_2)}\\ &= \sqrt{\frac{\mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}}\mathrm{e}^{j\pi\frac{d}{\lambda}\left(\sqrt{N}-1\right)(\delta_1+\delta_2)}\\ &\quad\times\frac{\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_2\right)}{\sin\left(\pi\frac{d}{\lambda}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\delta_2\right)},\end{aligned}\tag{60}$$

and (g) follows by making use of a mapping from the index n to the two-dimensional index (x, y) and substituting $\mathrm{a}_{N,Ri}(n) = \mathrm{e}^{j2\pi\frac{d}{\lambda}(x\sin\psi^{a}_{Ri}\sin\psi^{e}_{Ri}+y\cos\psi^{e}_{Ri})}$ from (5), $\delta_1 = \sin\psi^{a}_{RD}\sin\psi^{e}_{RD} - \sin\psi^{a}_{RE_m}\sin\psi^{e}_{RE_m}$, and $\delta_2 = \cos\psi^{e}_{RD} - \cos\psi^{e}_{RE_m}$.

Appendix E
Proof of Proposition 2

When $r_e \to \infty$, the CDF of the overall eavesdropper SNR in (23) is given as

$$\begin{aligned}F_{\gamma_E}(x) &= \exp\left[-t_0x^{-t_4}\Gamma(t_1)\right]\exp\left[t_0x^{-t_4}\Gamma\left(t_1, t_2x^{t_3}\right)\right]\\ &\overset{(h)}{=}\exp\left[-t_0x^{-t_4}\Gamma(t_1)\right]\\ &\quad\times\left(1+t_0x^{-t_4}\mathcal{O}\left(\left(t_2x^{t_3}\right)^{t_1-1}\mathrm{e}^{-t_2x^{t_3}}\right)\right),\end{aligned}\tag{61}$$

where (h) comes from the asymptotic expansion of the upper incomplete Gamma function when $t_2 = \mathrm{e}^{v(\varpi)}\Xi^{\mu(\varpi)}r_e^{\frac{\alpha_2}{2}\mu(\varpi)} \to \infty$ [48, Eq. (6.5.32)]. Therefore, for large r_e, the SOP in (25) is further rewritten as

$$\begin{aligned}\mathrm{SOP} &= 1 - \int_0^{+\infty} F_{\gamma_E}\left(\frac{1}{\varphi}(1+x)-1\right) f_{\gamma_D}(x)\mathrm{d}x\\ &\overset{(i)}{\simeq} 1 - \int_0^{+\infty}\exp\left[-t_0\Gamma(t_1)\left(\frac{x}{\varphi}\right)^{-t_4}\right]\\ &\quad\times\frac{1}{\Gamma(k)}\frac{\mathrm{e}^{-\frac{\sqrt{x/\rho_d}}{\theta}}\left(\frac{\sqrt{x/\rho_d}}{\theta}\right)^{k}}{2x}\mathrm{d}x\\ &= 1 - \frac{1}{2\Gamma(k)}\left(\sqrt{\rho_d}\theta\right)^{-k}\ I,\end{aligned}\tag{62}$$

where (i) is obtained by substituting (11) and (61), $I = \int_0^{+\infty} x^{a}\exp\left[-bx^{-c} - \upsilon\sqrt{x}\right]\mathrm{d}x$, $a = \frac{k}{2} - 1$, $b = t_0\Gamma(t_1)\varphi^{t_4}$, $c = t_4 = \frac{2q}{p}$, and $\upsilon = \frac{1}{\sqrt{\rho_d}\theta}$.

By applying the Mellin convolution theorem [42], the Mellin transform of I is given by

$$\mathcal{M}[I;s] = \frac{2p}{2q\upsilon^{2s+2a+2}}\Gamma\left(\frac{ps}{2q}\right)\Gamma(2s+2a+2).\tag{63}$$

Therefore, we can calculate I using the inverse transform as follows

$$\begin{aligned}I &= \frac{p}{\pi i\upsilon^{2a+2}}\int_{u-i\infty}^{u+i\infty}\Gamma(ps)\Gamma\left(4q\left(s+\frac{a+1}{2q}\right)\right)\left(\upsilon^{4q}b^{p}\right)^{-s}\mathrm{d}s\\ &\overset{(j)}{=}\frac{p^{\frac{1}{2}}q^{2a+\frac{3}{2}}}{\upsilon^{2a+2}2^{\frac{p+4q}{2}-4a-5}\pi^{\frac{p+4q}{2}-1}}\frac{1}{2\pi i}\int_{u-i\infty}^{u+i\infty}\left(\frac{\upsilon^{4q}b^{p}}{p^{p}256^{q}q^{4q}}\right)^{-s}\\ &\quad\times\prod_{n=0}^{p-1}\Gamma\left(s+\frac{n}{p}\right)\prod_{n=0}^{4q-1}\Gamma\left(s+\frac{n+2a+2}{4q}\right)\mathrm{d}s\\ &= \frac{p^{\frac{1}{2}}q^{2a+\frac{3}{2}}}{\upsilon^{2a+2}2^{\frac{p+4q}{2}-4a-5}\pi^{\frac{p+4q}{2}-1}}G^{p+4q,0}_{0,p+4q}\left(\frac{\upsilon^{4q}b^{p}}{p^{p}256^{q}q^{4q}}\middle|\begin{matrix}-\\ \Delta\end{matrix}\right),\end{aligned}\tag{64}$$

where (j) follows from Gauss' multiplication formula [48, Eq. (6.1.20)], and the last equality is derived by applying the definition of Meijer's G function. Subsequently, by substituting (64) into (62), the SOP is obtained as shown in (29).

Appendix F
Proof of Lemma 3

First, by using Jensen's inequality, we have

$$\mathbb{E}\{\log_2(1+\gamma_D)\} \le \log_2(1+\mathbb{E}\{\gamma_D\}) = \log_2(1+\rho_d K\nu J),\tag{65}$$

where J is expressed as

$$\begin{aligned}J &= \mathbb{E}\left\{\left(\sum_{n=1}^{N}|h_{RD}(n)|\right)^2\right\}\\ &= \mathbb{E}\left\{\sum_{n=1}^{N}|h_{RD}(n)|^2 + 2\sum_{1\le i<j\le N}|h_{RD}(i)|\,|h_{RD}(j)|\right\}\\ &= N\cdot\mathbb{E}\left\{|h_{RD}(n)|^2\right\} + N(N-1)\cdot\left(\mathbb{E}\{|h_{RD}(n)|\}\right)^2\\ &= N\mu_D\left[1+(N-1)\frac{1}{\epsilon+1}\frac{\pi}{4}\left(L_{1/2}(-\epsilon)\right)^2\right].\end{aligned}\tag{66}$$

Then, substituting (66) into (65), the upper bound for R_D is obtained as shown in (48).

Appendix G
Proof of Corollary 6

By substituting (48) into (44), the approximate ESC can be represented in (67), shown at the top of the next page, where $t_0 = \frac{2\pi\lambda_e}{\mu(\varpi)\mathrm{e}^{\frac{2v(\varpi)}{\mu(\varpi)}}\Xi^2} = \frac{1}{\mu(\varpi)\mathrm{e}^{\frac{2v(\varpi)}{\mu(\varpi)}}}\pi\lambda_e NK\nu\beta_0\rho_e\left[1-\frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]$, and (k) comes from the fact that when $\rho_d, \rho_e \to \infty$, the formula $\lim_{t_0\Gamma(t_1)\to\infty}\{\mathrm{Shi}(t_0\Gamma(t_1)) - \mathrm{Chi}(t_0\Gamma(t_1))\} = 0$ holds. We complete the proof by substituting the expressions of ρ_d, ρ_e, and μ_D into (67).

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

$$\begin{aligned}\bar{C}_s &= \left\{ \log_2 \left(1 + \rho_d K N \nu \mu_D \left(1 + \frac{\pi}{4} (N-1) \frac{\left(L_{\frac{1}{2}} (-\epsilon) \right)^2}{\epsilon + 1} \right) \right) \right. \\ &\quad \left. - \frac{1}{\ln 2} \{ \gamma + \ln t_0 \Gamma(t_1) + \exp(t_0 \Gamma(t_1)) \times (\mathrm{Shi}(t_0 \Gamma(t_1)) - \mathrm{Chi}(t_0 \Gamma(t_1))) \} \right\}^+ \\ &\overset{(k)}{\to} \left\{ \log_2 \rho_d K N \nu \mu_D \left[1 + (N-1) \frac{1}{\epsilon + 1} \frac{\pi}{4} \left(L_{\frac{1}{2}} (-\epsilon) \right)^2 \right] - \frac{1}{\ln 2} \{ \gamma + \ln t_0 \Gamma(t_1) \} \right\}^+ \\ &= \left\{ \log_2 \frac{\rho_d}{\rho_e} + \log_2 \frac{\mu_D}{\pi \lambda_e \beta_0} + \log_2 \frac{1 + (N-1) \frac{1}{\epsilon+1} \frac{\pi}{4} \left(L_{\frac{1}{2}} (-\epsilon) \right)^2}{1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1) \left(L_{\frac{1}{2}} (-\epsilon) \right)^2}} - \frac{\gamma}{\ln 2} + C \right\}^+, \end{aligned} \tag{67}$$

ACKNOWLEDGMENT

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of the Ministry of Education, Singapore.

REFERENCES

[1] W. Shi et al., "Secure outage analysis for RIS-aided MISO systems with randomly located eavesdroppers," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Kuala Lumpur, Malaysia, Dec. 2023.

[2] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[3] X. Lei, M. Wu, F. Zhou, X. Tang, R. Q. Hu, and P. Fan, "Reconfigurable intelligent surface-based symbiotic radio for 6G: Design, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 210–216, Oct. 2021.

[4] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1196–1217, 2023.

[5] W. Shi, W. Xu, X. You, C. Zhao, and K. Wei, "Intelligent reflection enabling technologies for integrated and green Internet-of-Everything beyond 5G: Communication, sensing, and security," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 147–154, Apr. 2023.

[6] S. Li, B. Duo, X. Yuan, Y.-C. Liang, and M. Di Renzo, "Reconfigurable intelligent surface assisted UAV communication: Joint trajectory design and passive beamforming," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 716–720, May 2020.

[7] H. Zhang, B. Di, L. Song, and Z. Han, "Reconfigurable intelligent surfaces assisted communications with limited phase shifts: How many phase shifts are enough?" *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4498–4502, Apr. 2020.

[8] S. Lin, B. Zheng, G. C. Alexandropoulos, M. Wen, F. Chen, and S. Mumtaz, "Adaptive transmission for reconfigurable intelligent surface-assisted OFDM wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2653–2665, Nov. 2020.

[9] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[10] S. Liu, Z. Gao, J. Zhang, M. Di Renzo, and M.-S. Alouini, "Deep denoising neural network assisted compressive channel estimation for mmWave intelligent reflecting surfaces," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9223–9228, Aug. 2020.

[11] Z. Wan, Z. Gao, F. Gao, M. Di Renzo, and M.-S. Alouini, "Terahertz massive MIMO with holographic reconfigurable intelligent surfaces," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4732–4750, Jul. 2021.

[12] J. Yao, J. Xu, W. Xu, D. W. K. Ng, C. Yuen, and X. You, "Robust beamforming design for RIS-aided cell-free systems with CSI uncertainties and capacity-limited backhaul," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4636–4649, Aug. 2023.

[13] W. Ni, Y. Liu, Y. C. Eldar, Z. Yang, and H. Tian, "STAR-RIS integrated nonorthogonal multiple access and over-the-air federated learning: Framework, analysis, and optimization," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17136–17156, Sep. 2022.

[14] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," *IEEE J. Sel. Topics Signal Process.*, vol. 17, no. 1, pp. 9–39, Jan. 2023.

[15] J. Xu et al., "Reconfiguring wireless environments via intelligent surfaces for 6G: Reflection, modulation, and security," *Sci. China Inf. Sci.*, vol. 66, no. 3, pp. 1–20, Mar. 2023.

[16] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[17] G. Zhou, C. Pan, H. Ren, K. Wang, and Z. Peng, "Secure wireless communication in RIS-aided MISO system with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1309–1313, Jun. 2021.

[18] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Nov. 2020.

[19] 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 Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[20] W. Shi, J. Xu, W. Xu, M. Di Renzo, and C. Zhao, "Secure outage analysis of RIS-assisted communications with discrete phase control," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5435–5440, Apr. 2023.

[21] P. Xu, G. Chen, G. Pan, and M. Di Renzo, "Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[22] 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, May 2021.

[23] Y. Ai, F. A. P. de Figueiredo, L. Kong, M. Cheffena, S. Chatzinotas, and B. Ottersten, "Secure vehicular communications through reconfigurable intelligent surfaces," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7272–7276, Jul. 2021.

[24] D. Wang, M. Wu, Z. Wei, K. Yu, L. Min, and S. Mumtaz, "Uplink secrecy performance of RIS-based RF/FSO three-dimension heterogeneous networks," *IEEE Trans. Wireless Commun.*, early access, Jul. 12, 2023, doi: 10.1109/TWC.2023.3292073.

[25] J. Yuan, G. Chen, M. Wen, R. Tafazolli, and E. Panayirci, "Secure transmission for THz-empowered RIS-assisted non-terrestrial networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5989–6000, May 2023.

[26] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*. Hoboken, NJ, USA: Wiley, 2013.

[27] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

[28] L. Wei, K. Wang, C. Pan, and M. Elkashlan, "Secrecy performance analysis of RIS-aided communication system with randomly flying eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 11, no. 10, pp. 2240–2244, Oct. 2022.

[29] W. Wang, H. Tian, and W. Ni, "Secrecy performance analysis of IRS-aided UAV relay system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2693–2697, Dec. 2021.

[30] J. Yao, J. Xu, W. Xu, C. Yuen, and X. You, "A universal framework of superimposed RIS-phase modulation for MISO communication," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5413–5418, Apr. 2023.

[31] J. Yao, J. Xu, W. Xu, C. Yuen, and X. You, "Superimposed RIS-phase modulation for MIMO communications: A novel paradigm of information transfer," *IEEE Trans. Wireless Commun.*, early access, Aug. 18, 2023, doi: 10.1109/TWC.2023.3304695.

[32] A. Papazafeiropoulos, C. Pan, P. Kourtessis, S. Chatzinotas, and J. M. Senior, "Intelligent reflecting surface-assisted MU-MISO systems with imperfect hardware: Channel estimation and beamforming design," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 2077–2092, Mar. 2022.

[33] S. Fang, G. Chen, Z. Abdullah, and Y. Li, "Intelligent omni surface-assisted secure MIMO communication networks with artificial noise," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1231–1235, Jun. 2022.

[34] J. Bai, H.-M. Wang, and P. Liu, "Robust IRS-aided secrecy transmission with location optimization," *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 6149–6163, Sep. 2022.

[35] S. Zhou, W. Xu, K. Wang, M. Di Renzo, and M.-S. Alouini, "Spectral and energy efficiency of IRS-assisted MISO communication with hardware impairments," *IEEE Wireless Commun. Lett.*, vol. 9, no. 9, pp. 1366–1369, Sep. 2020.

[36] Z.-Q. He and X. Yuan, "Cascaded channel estimation for large intelligent metasurface assisted massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 210–214, Feb. 2020.

[37] L. Wei, C. Huang, G. C. Alexandropoulos, C. Yuen, Z. Zhang, and M. Debbah, "Channel estimation for RIS-empowered multi-user MISO wireless communications," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4144–4157, Jun. 2021.

[38] 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, Oct. 2020.

[39] S. Primak, V. Kontorovich, and V. Lyandres, *Stochastic Methods and Their Applications to Communications: Stochastic Differential Equations Approach*. West Sussex, U.K.: Wiley, 2004.

[40] R. W. Heath Jr., M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using Poisson point processes," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4114–4126, Aug. 2013.

[41] M. Z. Bocus, C. P. Dettmann, and J. P. Coon, "An approximation of the first order Marcum Q-function with application to network connectivity analysis," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 499–502, Mar. 2013.

[42] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[43] H. Lei et al., "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1230–1244, Feb. 2020.

[44] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[45] F. Baccelli and B. Blaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume II: Applications*. Hanover, MA, USA: Now, 2009.

[46] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[47] Wolfram Research. (2001). *The Wolfram Functions Site: Meijer G-Function*. [Online]. Available: https://functions.wolfram.com/PDF/MeijerG.pdf

[48] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1972.

[49] Y. Guo, R. Zhao, S. Lai, L. Fan, X. Lei, and G. K. Karagiannidis, "Distributed machine learning for multiuser mobile edge computing systems," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 460–473, Apr. 2022.

[50] J. Xu, W. Xu, D. W. K. Ng, and A. L. Swindlehurst, "Secure communication for spatially sparse millimeter-wave massive MIMO channels via hybrid precoding," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 887–901, Feb. 2020.

Wei Shi (Graduate Student Member, IEEE) received the B.S. degree in communication engineering from Nanjing University, Nanjing, China, in 2017, and the M.S. degree in information and communication engineering from Southeast University, Nanjing, in 2019, where he is currently pursuing the Ph.D. degree in information and communication engineering. His current research interests include reconfigurable intelligent surface and physical layer security.

Jindan Xu (Member, IEEE) received the B.E. and Ph.D. degrees in electrical engineering from the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2015 and 2020, respectively. From September 2018 to September 2019, she was a Visiting Student with the Department of Electrical Engineering and Computer Science, University of California at Irvine, Irvine, CA, USA. From June 2022 to June 2023, she was a Post-Doctoral Fellow with the Engineering Product Development Pillar, Singapore University of Technology and Design (SUTD), Singapore. She is currently a Post-Doctoral Fellow with the School of Electrical and Electronics Engineering, Nanyang Technological University (NTU), Singapore. Her current research interests include RIS, physical-layer security, and massive MIMO communications.

Wei Xu (Senior Member, IEEE) received his B.Sc. degree in electrical engineering and his M.S. and Ph.D. degrees in communication and information engineering from Southeast University, Nanjing, China in 2003, 2006, and 2009, respectively. Between 2009 and 2010, he was a Post-Doctoral Research Fellow at the University of Victoria, Canada. He was an Adjunct Professor of the University of Victoria in Canada from 2017 to 2020, and a Distinguished Visiting Fellow of the Royal Academy of Engineering, U.K. in 2019. He is currently a Professor at Southeast University. His research interests include information theory, signal processing, and machine learning for wireless communications.

He received the Science and Technology Award for Young Scholars of the China Institute of Communications in 2018, the Science and Technology Award of the Chinese Institute of Electronics (Second Prize) in 2019, the National Natural Science Foundation of China for Outstanding Young Scholars in 2020, the IEEE Communications Society Heinrich Hertz Award in 2023, and the Best Paper Awards at IEEE Globecom 2014, IEEE ICCC 2014, ISWCS 2018, and WCSP 2017, 2021. He served as an Editor for IEEE TRANSACTIONS ON COMMUNICATIONS from 2018 to 2023. He also served for IEEE COMMUNICATIONS LETTERS as firstly an Editor from 2012 to 2017, then a Senior Editor from 2020 to 2023, and is now an Area Editor. He is a Fellow of IET.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.

Chau Yuen (Fellow, IEEE) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively.

He was a Post-Doctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, in 2005, and a Visiting Assistant Professor with The Hong Kong Polytechnic University, in 2008. From 2006 to 2010, he was with the Institute for Infocomm Research, Singapore. From 2010 to 2023, he was with the Engineering Product Development Pillar, Singapore University of Technology and Design. Since 2023, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University. He has three U.S. patents and published over 500 research papers at international journals or conferences.

Dr. Yuen received the IEEE Communications Society Fred W. Ellersick Prize in 2023, the IEEE Marconi Prize Paper Award in Wireless Communications in 2021, and the EURASIP Best Paper Award for *Journal on Wireless Communications and Networking* in 2021. He was a recipient of the Lee Kuan Yew Gold Medal, the Institution of Electrical Engineers Book Prize, the Institute of Engineering of Singapore Gold Medal, and the Merck Sharp and Dohme Gold Medal, and twice a recipient of the Hewlett Packard Prize. He received the IEEE Asia–Pacific Outstanding Young Researcher Award in 2012 and the IEEE VTS Singapore Chapter Outstanding Service Award on 2019. He currently serves as the Editor-in-Chief for *Computer Science* (Springer Nature) and an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE SYSTEMS JOURNAL, and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, where he was awarded as the IEEE TNSE Excellent Editor Award and the Top Associate Editor for TVT from 2009 to 2015. He served as the Guest Editor for several special issues, including IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *IEEE Wireless Communications Magazine*, *IEEE Communications Magazine*, *IEEE Vehicular Technology Magazine*, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and *Applied Energy* (Elsevier). He is a Distinguished Lecturer of the IEEE Vehicular Technology Society, a Top 2% Scientists by Stanford University, and a Highly Cited Researcher by Clarivate Web of Science.

A. Lee Swindlehurst (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from Brigham Young University (BYU) in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University, in 1991. He was with the Department of Electrical and Computer Engineering, BYU, from 1990 to 2007, where he was the Department Chair, from 2003 to 2006. From 1996 to 1997, he held a joint appointment as a Visiting Scholar with Uppsala University and the Royal Institute of Technology, Sweden. From 2006 to 2007, he was on leave working as the Vice President of Research of ArrayComm LLC., San Jose, CA, USA. Since 2007, he has been a Professor with the Electrical Engineering and Computer Science (EECS) Department, University of California at Irvine, where he was the Associate Dean of the Research and Graduate Studies, Samueli School of Engineering, from 2013 to 2016. From 2014 to 2017, he was a Hans Fischer Senior Fellow with the Institute for Advanced Studies, Technical University of Munich. In 2016, he was elected as a Foreign Member with the Royal Swedish Academy of Engineering Sciences (IVA). He is currently the Chair of the EECS Department. His research interests include array signal processing for radar, wireless communications, and biomedical applications. He has over 400 publications in these areas. He received the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, the 2006, 2010, and 2021 IEEE Signal Processing Society's best paper awards, the 2017 IEEE Signal Processing Society Donald G. Fink Overview Paper Award, the Best Paper Award at the 2020 IEEE International Conference on Communications, and the 2022 Claude Shannon-Harry Nyquist Technical Achievement Award from the IEEE Signal Processing Society. He was the Inaugural Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING.

Chunming Zhao (Member, IEEE) received the B.Sc. and M.S. degrees from the Nanjing Institute of Posts and Telecommunications in 1982 and 1984, respectively, and the Ph.D. degree from the Department of Electrical and Electronic Engineering, University of Kaiserslautern, Germany, in 1993. He has been a Post-Doctoral Researcher with the National Mobile Communications Research Laboratory, Southeast University, where he is currently a Professor and the Vice Director of the Laboratory. He has managed several key projects of the Chinese Communications High-Tech Program. His research interests include communication theory, coding/decoding, mobile communications, and VLSI design. He received the First Prize of National Technique Invention of China in 2011 and the Excellent Researcher Award from the Ministry of Science and Technology, China.

Authorized licensed use limited to: Access paid by The UC Irvine Libraries. Downloaded on June 08,2025 at 04:29:42 UTC from IEEE Xplore. Restrictions apply.