Secure Outage Analysis for RIS-Aided MISO Systems with Randomly Located Eavesdroppers

Wei Shi*†, Jindan Xu‡, Wei Xu*†, Chau Yuen‡, A. Lee Swindlehurst§, Xiaohu You*†, and Chunming Zhao*†

*National Mobile Communications Research Laboratory, Southeast University, Nanjing, China

†Purple Mountain Laboratories, Nanjing, China

‡School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore

§Center for Pervasive Communications and Computing, University of California, Irvine, USA

Emails: wshi@seu.edu.cn, jindan1025@gmail.com, wxu@seu.edu.cn, chau.yuen@ntu.edu.sg, swindle@uci.edu, xhyu@seu.edu.cn, cmzhao@seu.edu.cn

Abstract—In this paper, we consider the physical layer security of an RIS-assisted multiple-antenna communication system with randomly located eavesdroppers. The 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 a closed-form expression for the secrecy outage probability (SOP) is obtained. It is revealed that the secrecy performance is mainly affected by the number of RIS reflecting elements, and the impact of the 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. We also perform an analytical study demonstrating that the secrecy diversity order depends on the path loss exponent of the RIS-to-ground links. Finally, numerical simulations are conducted to verify the accuracy of these theoretical observations.

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]–[4]. An RIS comprises a large number of low-cost passive reflecting elements that are able to independently control the phases and/or amplitudes of their reflection coefficients. Due to their reconfigurable behavior, RISs have been widely considered for various wireless applications [5]–[10].

In recent years, security for wireless communication has become a critical issue [11] [12]. The capability of RIS to create a smart controllable wireless propagation makes it a promising approach for providing physical layer security (PLS) [13]. There are multiple works that investigate the theoretical secrecy performance for RIS-enhanced PLS systems [14]–[16]. However, for analytical simplicity and mathematical tractability, most work has considered single-antenna nodes and Rayleigh fading channels, and overlooked randomly distributed eavesdropper locations. Although the authors of [15] and [16] considered the random eavesdropper locations, there are still several research gaps left to be filled. In [15], Rician

fading channels and optimization of the RIS phase shifts were not taken into consideration for the considered multiple-antenna scenario. In [16], the study was conducted based on a simplified transmit beamforming design and a secrecy diversity order analysis was not conducted.

In this paper, we investigate the secrecy performance of an RIS-assisted multiple-input single-output (MISO) system with randomly located eavesdroppers. We first derive the exact distributions of the received signal-to-noise-ratios (SNRs) for the legitimate user and the eavesdroppers. Then, we present a closed-form expression for the secrecy outage probability (SOP). The obtained expression shows that the SOP is mainly affected by the number of RIS reflecting elements, and is not a strong function of the number of transmit antennas nor the transmit power at the base station. In addition, when the locations of the randomly located eavesdroppers are unknown, it is shown that deploying the RIS closer to the legitimate user is more efficient. To obtain more insightful observations, an asymptotic SOP analysis at high SNR is also conducted. It is shown that the secrecy diversity order ultimately only depends on the path loss exponent of the RIS-to-ground links.

II. SYSTEM MODEL

We consider an RIS-assisted secure communication system consisting of a base station (S) with K antennas and an RIS with N reflecting elements, as illustrated in Fig. 1. The reflection coefficient matrix of the RIS is denoted by $\boldsymbol{\Theta} \triangleq \mathrm{diag}\left\{\eta_1 e^{j\theta_1}, \ldots, \eta_n e^{j\theta_n}, \ldots, \eta_N e^{j\theta_N}\right\}$, where $\mathrm{diag}\{\cdot\}$ indicates a diagonal matrix, and $\theta_n \in [0, 2\pi)$ $(\eta_n \in [0,1])$ is the phase (amplitude) coefficient of the n-th reflecting element. In order to exploit the maximum reflection capability of the RIS, the amplitude coefficients in this work are set to 1, i.e., $\eta_n=1$ for all n. The spatial distribution of the randomly located eavesdroppers (E) in a disk of radius r_e centered at the RIS is modeled using a homogeneous Poisson point process (PPP), which is denoted by Φ_e with a density λ_e, while the legitimate user can locate randomly without the restriction of this disk.

We assume that the direct link between S and the legitimate user (D) is blocked by obstacles. In this scenario, the data transmission between S and D is ensured by the RIS. Since

Fig. 1. System model in the presence of randomly located eavesdroppers.

the base station and RIS are usually deployed at an elevated height, the channel between S and the RIS can be assumed to be line-of-sight (LoS) [17] [18], 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

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

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} (d_{Ri}) and α_1 (α_2) are the distances and the path loss exponents of the S-RIS (RIS-i) links respectively, and ϵ denotes the Rician factor. 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 random variables (RVs). The LoS components $\overline{\mathbf{H}}_{SR}$ and $\overline{\mathbf{h}}_{Ri}$ are expressed as

$$\overline{\mathbf{H}}_{SR} = \mathbf{a}_N\left(\phi_{SR}^a, \phi_{SR}^e\right)\mathbf{a}_K^H\left(\psi_{SR}^a, \psi_{SR}^e\right) = \mathbf{a}_{N,SR}\mathbf{a}_{K,SR}^H, \ (2)$$

$$\overline{\mathbf{h}}_{Ri} = \mathbf{a}_N\left(\psi_{Ri}^a, \psi_{Ri}^e\right) = \mathbf{a}_{N,Ri}, \quad (3)$$

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 expressed as [19]

$$\mathbf{a}_Z\left(\vartheta^a, \vartheta^e\right) = \left[1, \ldots, e^{j2\pi\frac{d}{\lambda}(x\sin\vartheta^a\sin\vartheta^e + y\cos\vartheta^e)}, \ldots, \right.$$
$$\left. e^{j2\pi\frac{d}{\lambda}\left(\left(\sqrt{Z}-1\right)\sin\vartheta^a\sin\vartheta^e + \left(\sqrt{Z}-1\right)\cos\vartheta^e\right)}\right]^T, \ (4)$$

where d and λ are the element spacing and signal wavelength, and $0 \leq x, y < \sqrt{Z}$ are the element indices in the plane.

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

$$r_D = \mathbf{g}_D^H\mathbf{f}s + n_D, \quad (5)$$

where $\mathbf{g}_D^H \triangleq \mathbf{h}_{RD}^H\boldsymbol{\Theta}\mathbf{H}_{SR}$ denotes the cascaded channel, $\mathbf{f}$ is the normalized beamforming vector, s denotes the transmit signal that satisfies the power constraint $\mathbb{E}\{|s|^2\} = P_T$, $\mathbb{E}\{\cdot\}$ is the expectation of a RV, and $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ is the additive white Gaussian noise (AWGN) at D with variance σ_D^2, where $\mathcal{CN}$ is the complex Gaussian distribution. Therefore, the received SNR at D is calculated as

$$\gamma_D = \frac{P_T\left|\mathbf{g}_D^H\mathbf{f}\right|^2}{\sigma_D^2} = \rho_d|A|^2, \quad (6)$$

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

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

$$\boldsymbol{\Theta}^\star = \mathrm{diag}\left\{e^{-j\angle\left(\mathrm{diag}\{\mathbf{h}_{RD}^H\}\mathbf{a}_{N,SR}\right)}\right\}, \quad (7)$$

where $\angle$ returns the phase of a complex value.

Proof: See Appendix A. ∎

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

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

$$F_{|A|}(x) = \frac{1}{\Gamma(k)}\gamma\left(k, \frac{x}{\theta}\right), \quad (8)$$

where $\Gamma(\cdot)$ is the Gamma function, $\gamma(\cdot, \cdot)$ denotes the lower incomplete Gamma function [20, Eq. (8.350.1)], 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 [21, Eq. (2.66)].

Proof: See Appendix B. ∎

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

$$F_{\gamma_D}(x) = F_{|A|}\left(\sqrt{x/\rho_d}\right) = \frac{1}{\Gamma(k)}\gamma\left(k, \frac{\sqrt{x/\rho_d}}{\theta}\right), \quad (9)$$

and

$$f_{\gamma_D}(x) = \frac{dF_{\gamma_D}(x)}{dx} = \frac{e^{-\frac{\sqrt{x/\rho_d}}{\theta}}\left(\frac{\sqrt{x/\rho_d}}{\theta}\right)^k}{2\Gamma(k)x}. \quad (10)$$

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

$$r_{E_m} = \mathbf{h}_{RE_m}^H \boldsymbol{\Theta} \mathbf{H}_{SR} \mathbf{f} s + n_{E_m}, \tag{11}$$

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 as follows.

Proposition 1: The received SNR at E_m is expressed as

$$\gamma_{E_m} = \rho_e \left| \mathbf{h}_{RE_m}^H \boldsymbol{\Theta} \mathbf{H}_{SR} \mathbf{f} \right|^2 = \rho_e K \nu |Z_{E_m}|^2, \tag{12}$$

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

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

$V_{E_m} = N\mu_{E_m}\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]$, $\delta_1 = \sin\psi_{RD}^a \sin\psi_{RD}^e$ $-\sin\psi_{RE_m}^a \sin\psi_{RE_m}^e$ and $\delta_2 = \cos\psi_{RD}^e - \cos\psi_{RE_m}^e$.

Proof: See Appendix C. ∎

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

$$F_{\gamma_{E_m}}(x) = 1 - Q_1\left(\frac{s}{\sigma}, \frac{\sqrt{x}}{\sigma}\right), \tag{13}$$

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

$\sigma^2 = \frac{1}{2}\rho_e K N \nu \mu_{E_m}\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]$, and $Q_1(\mathrm{a},\mathrm{b})$ is the first-order Marcum Q-function [22].

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

$$F_{\gamma_E}(x) = \Pr\left\{\max_{m\in\Phi_e}\gamma_{E_m} \leq x\right\}$$

$$\overset{(a)}{=} \mathbb{E}_{\Phi_e}\left\{\prod_{m\in\Phi_e, r_m\leq r_e} F_{\gamma_{E_m}}(x)\right\}$$

$$\overset{(b)}{=} \exp\left[-2\pi\lambda_e\int_0^{r_e}\left(1 - F_{\gamma_{E_m}}(x)\right)r\,\mathrm{d}r\right]$$

$$\overset{(c)}{=} \exp\left[-2\pi\lambda_e\int_0^{r_e} Q_1\left(\varpi, \Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)r\,\mathrm{d}r\right], \tag{14}$$

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 [23, Eq. (4.55)], and (c) is obtained by using $\mu_{E_m} = \beta_0 r^{-\alpha_2}$ and defining $\varpi \triangleq \sqrt{2}\left|\frac{\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\sqrt{N}\delta_2\right)}{\sin\left(\pi\frac{d}{\lambda}\delta_1\right)\sin\left(\pi\frac{d}{\lambda}\delta_2\right)}\right|\left[N\left(\frac{\frac{\pi}{4}(\epsilon+1)\left(L_{1/2}(-\epsilon)\right)^2}{\epsilon^2} - 1\right)\right]^{-\frac{1}{2}}$ and $\Xi \triangleq \sqrt{2}\left(NK\nu\beta_0\rho_e\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{1/2}(-\epsilon)\right)^2}\right]\right)^{-\frac{1}{2}}$.

From the characterization in [22, Eq. (2)], we have a tight approximation for the Marcum Q-function in (14), that is, $Q_1\left(\varpi, \Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right) \simeq \exp\left[-e^{v(\varpi)}\left(\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)^{\mu(\varpi)}\right]$, 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, (14) is further calculated as

$$F_{\gamma_E}(x) = \exp\left[-2\pi\lambda_e\int_0^{r_e}\exp\left[-e^{v(\varpi)}\left(\Xi\sqrt{x}r^{\frac{\alpha_2}{2}}\right)^{\mu(\varpi)}\right]r\,\mathrm{d}r\right]$$

$$= \exp\left[-t_0\frac{\Gamma(t_1) - \Gamma(t_1, t_2 x^{t_3})}{x^{t_4}}\right], \tag{15}$$

where the last equality is obtained from [20, Eq. (3.326)] with the definitions $t_0 = \frac{2\pi\lambda_e}{\frac{\alpha_2}{2}\mu(\varpi)e^{\frac{4v(\varpi)}{\alpha_2\mu(\varpi)}}\Xi^{\frac{4}{\alpha_2}}}$, $t_1 = \frac{2}{\frac{\alpha_2}{2}\mu(\varpi)}$, $t_2 = e^{v(\varpi)}\Xi^{\mu(\varpi)}r_e^{\frac{\alpha_2}{2}\mu(\varpi)}$, $t_3 = \frac{\mu(\varpi)}{2}$, and $t_4 = \frac{2}{\alpha_2}$.

Therefore, the PDF of the overall eavesdropper SNR could be further derived from (15) as

$$f_{\gamma_E}(x) = \frac{dF_{\gamma_E}(x)}{dx} = t_0 x^{-t_4-1}\left(t_4\gamma(t_1, t_2 x^{t_3})\right.$$

$$\left. - t_3\left(t_2 x^{t_3}\right)^{t_1} e^{-t_2 x^{t_3}}\right) e^{-t_0 x^{-t_4}\gamma(t_1, t_2 x^{t_3})}. \tag{16}$$

IV. SECRECY OUTAGE ANALYSIS

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

A. Theoretical SOP Analysis

A popular metric for quantifying the 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

$$\text{SOP} = \Pr\left(\ln(1+\gamma_D) - \ln(1+\gamma_E) < C_{\text{th}}\right)$$

$$= \int_0^\infty F_{\gamma_D}\left((1+x)\varphi - 1\right)f_{\gamma_E}(x)\,\mathrm{d}x, \tag{17}$$

where $\varphi \triangleq e^{C_{\text{th}}}$.

In order to analyze the secrecy performance, a closed-form expression for the SOP is presented in *Proposition 2*.

Proposition 2: When $r_e \to \infty$, the SOP can be approximated by the following

$$\text{SOP} \simeq 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}$$

$$\times G_{0,p+4q}^{p+4q,0}\left(\frac{\left(t_0\Gamma(t_1)\varphi^{t_4}\right)^p}{p^p\left(4q\sqrt{\rho_d}\theta\right)^{4q}}\middle|\begin{matrix}-\\\Delta\end{matrix}\right), \tag{18}$$

where $G_{s,t}^{m,n}(z)$ is Meijer's G function [20], $p, q \in \mathbb{Z}^+$, $p/q = \alpha_2$, 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 D. ∎

A number of interesting points can be noted from (18).

Remark 1: From (18), we see that the transmit power P_T affects only the term $\frac{t_0^p}{\rho_d^{2q}} \propto \left(\frac{\rho_e}{\rho_d}\right)^{2q}$. Thus, we see that the SOP is not a function of P_T, and increasing the transmit power does not improve the secrecy performance. This is intuitive since an increase in P_T yields a proportional increase in both the transmit SNRs at the legitimate user and the eavesdroppers.

Remark 2: Acoording to (18), we obtain that $\frac{t_0^p}{\theta^{4q}} \propto (\Xi\theta)^{-4q}$, where $\Xi\theta = \frac{\chi}{\sqrt{N}}$, and the coefficient χ is independent of N and K. This implies that the SOP is mainly affected by the number of RIS reflecting elements, N, and the impact of the number of transmit antennas, K, is marginal.

In addition, we see that *Proposition 2* is the general analysis for any rational path loss exponent. Some specific case studies are reported as follows.

Corollary 1: For the special case of $\alpha_2 = 2$, i.e., $p = 2$ and $q = 1$, which corresponds to free space propagation [24], the SOP in (18) reduces to

$$\text{SOP} \simeq 1 - \frac{2^{k-1}}{\sqrt{\pi}\Gamma(k)} \, G_{0,3}^{3,0}\left(\frac{t_0\Gamma(t_1)\varphi}{4\rho_d\theta^2}\bigg|\begin{matrix}-\\0, \frac{k}{2}, \frac{k+1}{2}\end{matrix}\right). \quad (19)$$

Corollary 2: 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 [24], the SOP in (18) simplifies to the following expression

$$\text{SOP} \simeq 1 - \frac{2}{\Gamma(k)}\left(\frac{t_0\Gamma(t_1)\sqrt{\varphi}}{\sqrt{\rho_d}\theta}\right)^{\frac{k}{2}} K_k\left(2\left(\frac{t_0\Gamma(t_1)\sqrt{\varphi}}{\sqrt{\rho_d}\theta}\right)^{\frac{1}{2}}\right), \quad (20)$$

where $K_\nu(\cdot)$ denotes the ν-th-order modified Bessel function of the second kind [20, Eq. (8.407)].

Remark 3: From (20), we obtain that the SOP is a monotonically increasing function w.r.t. $\frac{t_0}{\sqrt{\rho_d}\theta} = \sqrt{\frac{\rho_e}{\rho_d}}\lambda_e d_{RD}^2 \beta(N, \epsilon)$ with fixed k, where $\beta(N, \epsilon)$ consists of parameters N, ϵ, and constant terms. We note 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 [25] where the secrecy diversity order is defined as follows

$$d_s = -\lim_{\rho_d \to \infty} \frac{\log \text{SOP}^\infty}{\log \rho_d}, \quad (21)$$

where SOP^∞ represents the asymptotic value of the SOP in (18) for $\rho_d \to \infty$, and the transmit SNR ρ_e is set to arbitrary fixed values.

According to [26, Eq. (07.34.06.0006.01)], the SOP in (18) can be expanded as

$$\text{SOP} \simeq 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}} \times G_{0,p+4q}^{p+4q,0}\left(x\bigg|\begin{matrix}-\\\Delta\end{matrix}\right)$$

$$= 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}} \times$$

$$\sum_{l=1}^{p+4q} \prod_{j=1, j\neq l}^{p+4q} \Gamma(\Delta(j) - \Delta(l)) x^{\Delta(l)}(1 + \mathcal{O}(x)), \quad (22)$$

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 $\rho_d \to \infty$, only the dominant terms $l = 0$ and $l = 1$ in the summation of (22) are retained, which yields the asymptotic SOP as

$$\text{SOP}^\infty = 1 - \frac{1}{\Gamma(k)}\frac{p^{\frac{1}{2}}q^{k-\frac{1}{2}}}{2^{\frac{p+4q}{2}-2k}\pi^{\frac{p+4q}{2}-1}}\left[\prod_{j=2}^{p+4q}\Gamma(\Delta(j))x^0\right.$$

$$\left. + \prod_{j=1, j\neq 2}^{p+4q}\Gamma\left(\Delta(j) - \frac{1}{p}\right)x^{\frac{1}{p}}\right]$$

$$= \frac{t_0\Gamma(t_1)\varphi^{\frac{2}{\alpha_2}}\Gamma\left(k - \frac{4}{\alpha_2}\right)}{\theta^{\frac{4}{\alpha_2}}\Gamma(k)}(\rho_d)^{-\frac{2}{\alpha_2}}, \quad (23)$$

where the last step is calculated by applying Gauss' multiplication formula [27, Eq. (6.1.20)].

Remark 4: By substituting (23) into (21), 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. SIMULATION RESULTS

In this section, Monte-Carlo simulations are illustrated to validate the analytical results. Fig. 2 depicts the SOP versus the transmit SNR ρ_d for different values of N and K. The analytical expressions in (18) match very well with the numerical results. Furthermore, as expected from *Remark 2*, 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 performance is negligible.

Fig. 3 shows the SOP versus the transmit SNR ρ_d for different values of the path loss exponent α_2. It can be seen that the negative slope of secrecy outage curves becomes less steep as α_2 increases. Furthermore, the secrecy diversity order presented in *Remark 4* can be verified by calculating the negative slope of the SOP curves on a log-log scale.

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

Fig. 3. The SOP versus ρ_d, with $K = 16$, $N = 16$, $\alpha_1 = 2$, $\epsilon = 2$, $d_{SR} = 30$ m, $d_{RD} = 40$ m, $r_e = 200$ m, $\lambda_e = 10^{-3}$, $C_{\text{th}} = 0.05$, and $\rho_e = 60$ dB.

VI. CONCLUSION

In this paper, the secrecy performance of an RIS-assisted communication system with randomly located eavesdroppers was studied. The exact distributions of the received SNRs at the legitimate user and the eavesdroppers were presented. Then, closed-form expressions for the SOP and secrecy diversity order were derived. It was demonstrated that the secrecy diversity order primarily depends on the path loss exponent of the RIS-to-ground links. The impact of other key parameters was also analyzed to provide insightful guidelines.

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

$$\boldsymbol{\Theta}^\star = \arg\max_{\boldsymbol{\Theta}} \left| \mathbf{g}_D^H \mathbf{f} \right|^2 \overset{(d)}{=} \arg\max_{\boldsymbol{\Theta}} \left| \boldsymbol{\theta}^H \text{diag}\{\mathbf{h}_{RD}^H\} \mathbf{a}_{N,SR} \right|^2, \quad (24)$$

where (d) follows by defining $\boldsymbol{\theta}^H = [e^{j\theta_1}, \ldots, e^{j\theta_n}, \ldots, e^{j\theta_N}]$. Therefore, the optimal RIS phase shifts are given by

$$\theta_n^\star = -\angle \left(h_{RD}^*(n) \, a_{N,SR}(n) \right), \quad (25)$$

and the phase shift matrix can be easily obtained as (7).

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 $|A|$ are calculated as $\mathbb{E}\{|A|\} =$

$\sqrt{K}\nu N \mathbb{E}\{|h_{RD}(n)|\}$ and $\text{Var}\{|A|\} = K\nu N \text{Var}\{|h_{RD}(n)|\}$, where $|h_{RD}(n)| \sim Rice\left(\sqrt{\frac{\mu_D \epsilon}{\epsilon+1}}, \sqrt{\frac{1}{2}\frac{\mu_D}{\epsilon+1}}\right)$, and $Rice$ denotes the Rician distribution, 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 $\text{Var}\{|h_{RD}(n)|\} = \frac{\mu_D}{\epsilon+1}\left[1 + \epsilon - \frac{\pi}{4}\left(L_{\frac{1}{2}}(-\epsilon)\right)^2\right]$, respectively.

Therefore, according to [28, Lemma 3], the RV $|A|$ can be approximated by a Gamma distributed RV with shape parameter $k = \frac{\mathbb{E}\{|A|\}^2}{\text{Var}\{|A|\}}$ and scale parameter $\theta = \frac{\text{Var}\{|A|\}}{\mathbb{E}\{|A|\}}$, which yields the desired result in (8).

APPENDIX C
PROOF OF LEMMA 2

From (1), we see that $h_{Ri}(n) \sim \mathcal{CN}\left(\sqrt{\frac{\mu_i\epsilon}{\epsilon+1}}\overline{h}_{Ri}(n), \frac{\mu_i}{\epsilon+1}\right)$, 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 $\mathbb{E}\{h_{Ri}(n)\} = \sqrt{\frac{\mu_i\epsilon}{\epsilon+1}}a_{N,Ri}(n)$, $\mathbb{E}\{|h_{Ri}(n)|\} = \sqrt{\frac{\mu_i}{\epsilon+1}}\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)$, and $\mathbb{E}\{|h_{Ri}(n)|^2\} = \mu_i$. It follows that

$$\mathbb{E}\{e^{-j\angle h_{RD}^*(n)}\} = \left(\frac{\mathbb{E}\{h_{RD}^*(n)\}}{\mathbb{E}\{|h_{RD}^*(n)|\}}\right)^* = \frac{\sqrt{\epsilon}a_{N,RD}(n)}{\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)}. \quad (26)$$

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

$$\mathbb{E}\{x_n\} = \sqrt{\frac{\mu_{E_m}\epsilon^2}{\epsilon+1}}\frac{a_{N,RE_m}^*(n)\,a_{N,RD}(n)}{\frac{\sqrt{\pi}}{2}L_{\frac{1}{2}}(-\epsilon)}, \quad (27)$$

and

$$\text{Var}\{x_n\} = \mu_{E_m}\left[1 - \frac{\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{\frac{1}{2}}(-\epsilon)\right)^2}\right]. \quad (28)$$

It can be seen from (27) that for different n, $\mathbb{E}\{x_n\}$ is related to n, which means that x_n is not identically distributed. 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 $\text{Var}\{x_n\}$. By virtue of the central limit theorem (CLT) [29], $\sum_{n=1}^N (x_n - \mathbb{E}\{x_n\})$ converges in distribution to a complex Gaussian RV with zero mean and variance $N \cdot \text{Var}\{x_n\}$. Then, we can obtain that $Z_{E_m} \sim \mathcal{CN}\left(\sum_{n=1}^N \mathbb{E}\{x_n\}, N \cdot \text{Var}\{x_n\}\right)$, where $\sum_{n=1}^N \mathbb{E}\{x_n\} = \sqrt{\frac{\mu_{E_m}\epsilon^2}{\frac{\pi}{4}(\epsilon+1)\left(L_{1/2}(-\epsilon)\right)^2}}\sum_{0\leq x,y\leq\sqrt{N}-1}e^{j2\pi\frac{d}{\lambda}(x\delta_1+y\delta_2)}$ by mapping the index n to the index (x,y), $\delta_1 = \sin\psi_{RD}^a\sin\psi_{RD}^e - \sin\psi_{RE_m}^a\sin\psi_{RE_m}^e$, and $\delta_2 = \cos\psi_{RD}^e - \cos\psi_{RE_m}^e$.

APPENDIX D
PROOF OF PROPOSITION 2

Using the asymptotic expansion of the upper incomplete gamma function [27, Eq. (6.5.32)], when $r_e \to \infty$, the CDF of the overall eavesdropping SNR in (15) can be given as follows

$$F_{\gamma_E}(x) \simeq \exp\left[-t_0 x^{-t_4}\Gamma(t_1)\right]. \quad (29)$$

Therefore, the SOP in (17) is further rewritten as

$$
\begin{aligned}
\mathrm{SOP} &= 1 - \int_0^{+\infty} F_{\gamma_E}\left(\frac{1}{\varphi}\left(1+x\right)-1\right) f_{\gamma_D}\left(x\right)\mathrm{d}x \\
&\simeq 1 - \frac{1}{2\Gamma\left(k\right)}\left(\sqrt{\rho_d}\theta\right)^{-k}\,I,
\end{aligned} \tag{30}
$$

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

By applying the Mellin convolution theorem [30], we can get the Mellin transform of I as

$$
\mathcal{M}\left[I;s\right] = \frac{2p}{2q\upsilon^{2s+2a+2}}\Gamma\left(\frac{ps}{2q}\right)\Gamma\left(2s+2a+2\right). \tag{31}
$$

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

$$
\begin{aligned}
I &= \frac{p}{\pi i \upsilon^{2a+2}}\int_{u-i\infty}^{u+i\infty}\Gamma\left(ps\right)\Gamma\left(4q\left(s+\frac{a+1}{2q}\right)\right)\left(\upsilon^{4q}b^p\right)^{-s}\mathrm{d}s \\
&\overset{(e)}{=} \frac{p^{\frac{1}{2}}q^{2a+\frac{3}{2}}}{\upsilon^{2a+2}2^{\frac{p+4q}{2}-4a-5}\pi^{\frac{p+4q}{2}-1}}\frac{1}{2\pi i}\int_{u-i\infty}^{u+i\infty}\left(\frac{\upsilon^{4q}b^p}{p^p256^q q^{4q}}\right)^{-s} \\
&\quad\times\prod_{n=0}^{p-1}\Gamma\left(s+\frac{n}{p}\right)\prod_{n=0}^{4q-1}\Gamma\left(s+\frac{n+2a+2}{4q}\right)\mathrm{d}s \\
&= \frac{p^{\frac{1}{2}}q^{2a+\frac{3}{2}}}{\upsilon^{2a+2}2^{\frac{p+4q}{2}-4a-5}\pi^{\frac{p+4q}{2}-1}}G_{0,p+4q}^{p+4q,0}\left(\frac{\upsilon^{4q}b^p}{p^p256^q q^{4q}}\bigg|\begin{array}{c}-\\\Delta\end{array}\right),
\end{aligned} \tag{32}
$$

where (e) follows from Gauss' multiplication formula [27, Eq. (6.1.20)], and the last equality is derived by applying the definition of Meijer's G function. Subsequently, by substituting (32) into (30), the SOP is obtained as shown in (18).

REFERENCES

[1] W. Shi, J. Xu, W. Xu, C. Yuen, A. L. Swindlehurst, and C. Zhao, "On secrecy performance of RIS-assisted MISO systems over Rician channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, early access. doi: 10.1109/TWC.2023.3348591.

[2] W. Xu *et al.*, "Toward ubiquitous and intelligent 6G networks: From architecture to technology," *Sci China Inf Sci*, vol. 66, no. 3, pp. 130300:1–2, Mar. 2023.

[3] 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, May 2023.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] J. Yao, W. Xu, X. You, D. W. K. Ng, and J. Fu, "Robust beamforming design for reconfigurable intelligent surface-aided cell-free systems," *in Proc. IEEE Int. Symp. Wireless Commun. Syst. (ISWCS)*, Hangzhou, China, 2022, pp. 1–6.

[10] W. Xu *et al.*, "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.

[11] 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.

[12] 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.

[13] J. Xu *et al.*, "Reconfiguring wireless environment via intelligent surfaces for 6G: Reflection, modulation, and security," *Sci China Inf Sci*, vol. 66, no. 3, pp. 130304:1–20, Mar. 2023.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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. doi: 10.1109/TWC.2023.3304695.

[19] 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, Sept. 2020.

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

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

[22] 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.

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

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

[25] 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.

[26] Wolfram Research, "The Wolfram functions site: Meijer G-function," 2001. [Online]. Available: https://functions.wolfram.com/PDF/MeijerG.pdf

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

[28] R. W. Heath, 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.

[29] W. Xu, J. Liu, S. Jin, and X. Dong, "Spectral and energy efficiency of multi-pair massive MIMO relay network with hybrid processing," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3794–3809, Sept. 2017.

[30] 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.