Secrecy Performance Analysis of RIS-aided Communication System with Randomly Flying Eavesdroppers

Lai Wei, Kezhi Wang, *Member, IEEE,* Cunhua Pan, *Member, IEEE,* Maged Elkashlan, *Senior Member, IEEE*

Abstract—In this letter, we analyze the secrecy performance of a reconfigurable intelligent surface (RIS)-aided communication system with spatially random unmanned aerial vehicles (UAVs) acting as eavesdroppers. We consider the scenarios where the base station (BS) is equipped with single and multiple antennas. The signal-to-noise ratios (SNRs) of the legitimate user and the eavesdroppers are derived analytically and approximated through a computationally effective method. The ergodic secrecy capacity is approximated and derived in closed-form expressions. Simulation results validate the accuracy of the analytical and approximate expressions and show the security-enhanced effect of the deployment of the RIS.

Index Terms—Physical layer security, unmanned aerial vehicles, reconfigurable intelligent surface, Poisson point process.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) have been regarded as one of the promising techniques in wireless communication systems. The UAVs could not only serve as flying base stations but also as relays to enhance performance of wireless networks, which help provide broader signal coverage and higher data rates in both military and civilian applications.

However, due to the flexibility of placement and the high mobility of the UAVs, they could be applied to various illegal activities such as launching attacks, conducting surveillance and creating security threats. Moreover, the higher chance of a line-of-sight (LoS) link makes wireless networks more vulnerable to UAV eavesdroppers compared with ground eavesdroppers [1]. Recently, the physical layer security (PLS) of UAV-enabled wireless communications have attracted extensive research interests. In [2], the authors analyzed the secrecy performance of a UAV-to-UAV communication system considering large-scale fading channel. In [3], the detection probability of a wireless system with a spatially random UAV eavesdropper was investigated. Furthermore, to enhance the secrecy performance in UAV-enabled wireless systems,

several techniques have been proposed, such as jamming [4], trajectory design [5] and artificial noise [6], etc.

Among the existing PLS schemes, the reconfigurable intelligent surface (RIS)-aided secure communication has attracted wide attentions [7]. Through sophisticated phase shift design, RIS could improve legitimate user's received SNR without increasing power budget. In addition, due to the randomness of the wireless channel, the signal reflected by the RIS could not only be added constructively at the legitimate user, but also destructively at the eavesdroppers [8]. The application of RIS in UAV-enabled wireless system could improve the secrecy performance with lower energy and cost. Nevertheless, the existing literature mainly focused on the scenario where the UAVs are acting as friendly relays or flying BSs to enhance secrecy performance of RIS-aided wireless systems, which inspires us to analyze the case where the UAVs act as eavesdroppers. Moreover, the impact of the randomness of Eve's spatial distribution on RIS-aided wireless systems has not been fully addressed in existing works.

Against the above background, in this work, we study the secrecy performance of a RIS-aided wireless system in the presence of spatially random UAVs acting as eavesdroppers. Firstly, we derive the cumulative distribution functions (CDFs) of the SNRs of the legitimate user and the eavesdroppers in analytical forms where the BS is equipped with single antenna. Next, we approximate the results through a computationally effective method. Then, we consider the scenario where the BS is equipped with multiple antennas. Finally, we carry out Monte-Carlo simulations to validate the accuracy of the analytical and the approximate results.

II. SYSTEM MODEL

We consider a RIS-aided communication system with one BS and one legitimate user (i.e., Bob), where Bob is equipped with a single antenna. Due to the blockage caused by obstacles such as buildings and trees, the direct link between the BS and Bob is negligibly weak. Therefore, a RIS is applied to assist end-to-end communication. Furthermore, there exists a group of UAV acting as eavesdroppers (i.e., Eves) aiming to eavesdrop the information of the legitimate user.

We assume that the BS is located on the origin of a Cartesian coordinate. For the sake of tractability, we assume that the UAVs are distributed randomly within a hemisphere with radius R surrounding the BS. We further assume that the spatial distribution of the UAVs follows a homogeneous 3-D

Poisson point process (PPP) $\mathcal{S}$ with density ρ_S. It is assumed that the RIS is installed on the point $(0, D, 0)$ where D denotes the distance between the BS and the RIS. The legitimate user Bob is assumed to be located at a fixed location. Also, the BS-UAV and the RIS-UAV communication links are assumed to follow Rician fading while the BS-RIS and the RIS-Bob links are assumed to follow Rayleigh fading. Throughout this paper, we use d_B to denote the distance between the RIS and Bob and $d_{p,E_k}(p \in \{\text{BS}, \text{RIS}\})$ to denote the distance between position p and the k-th UAV. Moreover, we use h_i and $g_i(i = 1, 2, \cdots N)$ to denote the small-scale fading of BS-RIS and RIS-Bob channel with i denoting the index of RIS element, respectively.

III. SECURE PERFORMANCE ANALYSIS IN SINGLE ANTENNA SCENARIO

A. Legitimate Link

We first consider the case where the BS is equipped with a single antenna. With the aid of the RIS, the received SNR at the legitimate user Bob could be expressed as

$$\gamma_B = \rho(Dd_B)^{-\alpha} \left| \sum_{i=1}^{N} g_i h_i e^{j\phi_i} \right|^2, \quad (1)$$

where ϕ_i is the phase shift applied by the i-th RIS element, $\rho = \frac{P}{\sigma_0^2}$ denotes the normalized transmit power of the BS and α is the pathloss factor for the BS-RIS and the RIS-Bob links.

Assuming perfect instantaneous CSI is available at the BS, the phase shift that maximizes the Bob's received SNR is given by

$$\phi_i^* = -\angle g_i - \angle h_i, \quad (2)$$

which yields the optimal instantaneous SNR of Bob as follows

$$\gamma_B = \rho(Dd_B)^{-\alpha} \left(\sum_{i=1}^{N} |g_i| |h_i| \right)^2 \triangleq \rho(Dd_B)^{-\alpha} Z. \quad (3)$$

According to [9], the random variable $Z = (\sum_{i=1}^{N} |g_i| |h_i|)^2$ could be approximated by a Gamma distributed random variable with shape parameter $\hat{k} = \frac{\mathbb{E}[Z]^2}{\mathbb{E}[Z^2] - \mathbb{E}[Z]^2}$ and scale parameter $\hat{\theta} = \frac{\mathbb{E}[Z^2] - \mathbb{E}[Z]^2}{\mathbb{E}[Z]}$, in which the first and second order moments of random variable Z_u could be calculated as

$$\begin{aligned} \mathbb{E}[Z] &= a_1 N + a_2 N(N-1) \\ \mathbb{E}[Z^2] &= b_1 N(N-1)(N-2)(N-3) \\ &\quad + b_2 N(N-1)(2N-1) + b_3 N^2 + b_4 N, \end{aligned} \quad (4)$$

where the constants are given by $a_1 = 1, a_2 = \frac{\pi^2}{16}, b_1 = \frac{\pi^4}{256}, b_2 = \frac{3\pi^2}{16}, b_3 = 3, b_4 = 1$ [10], respectively.

The CDF of Bob's received SNR could then be approximated as

$$F_{\gamma_B}(x) \approx \frac{1}{\Gamma(\hat{\theta})} \gamma \left(\hat{k}, \frac{x}{\rho(Dd_B)^{-\alpha}\hat{\theta}} \right), \quad (5)$$

where $\gamma(s, z) = \int_0^z e^{-t} t^{s-1} dt$ denotes the lower incomplete Gamma function and $\Gamma(z)$ denotes the Gamma function.

B. Eavesdropping Link

Considering both the reflected link and the direct link, the received SNR at the k-th Eve E_k is given by

$$\begin{aligned} \gamma_{E_k} &\triangleq \rho |Z_{E_k}|^2 \\ &= \rho \left| (Dd_{RIS,E_k})^{-\frac{\alpha}{2}} \sum_{i=1}^{N} v_{k,i} h_i e^{j\phi_i} + (d_{BS,E_k})^{-\frac{\alpha}{2}} v_{k,0} \right|^2, \end{aligned} \quad (6)$$

where $v_{k,i}$ denotes the small-scale fading between E_k and the i-th RIS element while $v_{k,0}$ denotes the channel coefficient of the direct link between E_k and the BS. For the sake of simplicity, we define the channel vector between E_k and all the RIS elements as follows

$$\mathbf{v}_k \triangleq [v_{k,1}, \cdots, v_{k,N}]^T = \sqrt{\frac{\beta_1}{\beta_1 + 1}} \bar{\mathbf{v}}_k + \sqrt{\frac{1}{\beta_1 + 1}} \widetilde{\mathbf{v}}_k. \quad (7)$$

Similarly, the channel between the BS and E_k can be given by

$$v_{k,0} = \sqrt{\frac{\beta_2}{\beta_2 + 1}} \bar{v}_{k,0} + \sqrt{\frac{1}{\beta_2 + 1}} \widetilde{v}_{k,0}, \quad (8)$$

where β_1 and β_2 denote the Rician factors.

According to [8], $\bar{\mathbf{v}}_k$ could be calculated as

$$\begin{aligned} \bar{\mathbf{v}}_k &= e^{-j\frac{2\pi d_{RIS,E_k}}{\lambda}} \times [1, \cdots, e^{-j\frac{2\pi(N_r-1)\delta_r \sin \xi_k \cos \psi_k}{\lambda}}]^T \\ &\otimes [1, e^{-j\frac{2\pi\delta_c \sin \xi_k \cos \psi_k}{\lambda}}, \cdots, e^{-j\frac{2\pi(N_c-1)\delta_c \sin \xi_k \cos \psi_k}{\lambda}}]^T. \end{aligned} \quad (9)$$

where $\lambda = \frac{c}{f}$ is the carrier wavelength, δ_r and δ_c are respectively the row and the column spacing of RIS elements, ξ_k and ψ_k depict respectively the azimuth and elevation angles of departure (AoD) from the RIS to E_k. Moreover, the symbol $\otimes$ represents the Kronecker product. Similarly, we have $\bar{v}_{k,0} = e^{-j\frac{2\pi d_{BS,E_k}}{\lambda}}$. Furthermore, the NLoS components of $\mathbf{v}_k$ and $v_{k,0}$ could be given as $\widetilde{\mathbf{v}}_k \sim \mathcal{CN}(0, \mathbf{I})$, $\widetilde{v}_{k,0} \sim \mathcal{CN}(0, 1)$, respectively.

Using spherical coordinate transformation, the RIS is located on the point $(D, \pi/2, \pi/2)$, thus the distance between E_k and the RIS could be expressed as

$$d_{RIS,E_k} = \sqrt{r_k^2 + D^2 - 2r_k D \sin \theta_k \sin \varphi_k}, \quad (10)$$

where r_k, θ_k and φ_k denote the radius, the polar angle and the azimuth angle of E_k, respectively. Note that $r_k = d_{BS,E_k}$, thus we substitute r_k for d_{BS,E_k} in the following analysis.

Since γ_{E_k} involves the randomness of large-scale fading, small-scale fading and the sum of a series of random variables, the exact distribution of γ_{E_k} is difficult to get, if not impossible. Therefore, we obtain an approximate distribution of γ_{E_k} in the following.

To begin with, according to central limit theorem (CLT), the random variable $\sum_{i=1}^{N} v_{k,i} h_i e^{j\phi_i}$ could be approximated by a complex Gaussian random variable with zero mean and variance N, namely, $\sum_{i=1}^{N} v_{k,i} h_i e^{j\phi_i} \sim \mathcal{CN}(0, N)$ [7].

Next, because the randomness of d_{RIS,E_k} is difficult to handle, similar to [11], we assume that the distance between the BS and E_k is much less than the distance between the BS

and the RIS. As a result, the distance between the RIS and E_k could be approximated by D, namely, $d_{RIS,E_k} \approx D$.

Moreover, since $v_{k,0}$ is a Gaussian random variable and the sum of independent Gaussian random variables is still Gaussian distributed, the distribution of Z_{E_k} conditioned on r_k could be approximated by a complex Gaussian random variable, namely, $Z_{E_k}|r_k \sim \mathcal{CN}\left(r_k^{-\frac{\alpha}{2}}\sqrt{\frac{\beta_2}{\beta_2+1}}e^{-j\frac{2\pi r_k}{\lambda}}, \frac{N}{D^{2\alpha}} + \frac{r_k^{-\alpha}}{\beta_2+1}\right)$.

Then, γ_{E_k} becomes a non-central Chi-square distributed random variable with two degrees-of-freedom, the CDF of which could be given as follows using Marcum-Q function

$$F_{\gamma_{E_k}}(x) = 1 - Q_1(\sqrt{2\mu}/\sigma_{E_k}, \sqrt{2x}/\sqrt{\rho}\sigma_{E_k}), \quad (11)$$

where $\mu = r_k^{-\alpha}\frac{\beta_2}{\beta_2+1}$ and $\sigma_{E_k}^2 = \frac{N}{D^{2\alpha}} + \frac{r_k^{-\alpha}}{\beta_2+1}$.

Considering non-colluded eavesdroppers, the CDF of the overall eavesdropping SNR could be derived as

$$
\begin{aligned}
F_{\gamma_E}(x) &= \max_{k\in\mathcal{S}} F_{\gamma_{E_k}}(x) \\
&= \mathbb{E}_{r_k,\theta_k,\varphi_k}\left[\prod_{k\in\mathcal{S}} F_{\gamma_{E_k}}(x|r_k,\theta_k,\varphi_k)\right] \\
&= \exp\left\{-\int_{\mathcal{S}}\rho_S\left[1 - F_{\gamma_{E_k}}(x|r_k,\theta_k,\varphi_k)\right]\mathrm{d}r_k\mathrm{d}\theta_k\mathrm{d}\varphi_k\right\} \\
&= \exp\left\{-2\pi\rho_S\int_0^R r^2 \right. \\
&\quad \left. Q_1\left(\frac{\sqrt{\frac{2\beta_2}{\beta_2+1}}}{\sqrt{N(\frac{r}{D^2})^\alpha + \frac{1}{\beta_2+1}}}, \frac{\sqrt{2x}}{\sqrt{\rho(\frac{N}{D^{2\alpha}} + \frac{r^{-\alpha}}{\beta_2+1})}}\right)\mathrm{d}r\right\}.
\end{aligned}
$$
$$(12)$$

For the sake of simplicity, we define the following function

$$I(x) = \int_0^R r^2 Q_1\left(\frac{\sqrt{\frac{2\beta_2}{\beta_2+1}}}{\sqrt{N(\frac{r}{D^2})^\alpha + \frac{1}{\beta_2+1}}}, \frac{\sqrt{2x}}{\sqrt{\rho(\frac{N}{D^{2\alpha}} + \frac{r^{-\alpha}}{\beta_2+1})}}\right)\mathrm{d}r. \quad (13)$$

Due to the complicated structure of Marcum-Q function, it is challenging to obtain a closed-form expression of $I(x)$. Therefore, we make further approximations to calculate the function $I(x)$ defined above.

Recalling that we assume that the distance between the BS and the RIS is much larger than that between the BS and E_k, it is reasonable to treat the item $\frac{r}{D^2}$ as a small variable. With the help of the series expansion of Marcum-Q function [12], we approximate the Marcum-Q function in $I(x)$ as follows

$$
\begin{aligned}
&Q_1\left(\frac{\sqrt{\frac{2\beta_2}{\beta_2+1}}}{\sqrt{N(\frac{r}{D^2})^\alpha + \frac{1}{\beta_2+1}}}, \frac{\sqrt{2x}}{\sqrt{\rho(\frac{N}{D^{2\alpha}} + \frac{r^{-\alpha}}{\beta_2+1})}}\right) \\
&\approx Q_1\left(\sqrt{2\beta_2}, \sqrt{2(\beta_2+1)r^\alpha[1 - (\beta_2+1)N(\frac{r}{D^2})^\alpha]x/\rho}\right) \\
&\approx \sum_{n=0}^{+\infty}\sum_{k=0}^n \frac{e^{-\beta_2}(\beta_2)^n}{n!k!}\exp\left(-(\beta_2+1)r^\alpha x/\rho\right) \\
&\quad \times [1 - (\beta_2+1)N(\frac{r}{D^2})^\alpha]^k\left(\frac{(\beta_2+1)r^\alpha x}{\rho}\right)^k.
\end{aligned}
$$
$$(14)$$

Using binomial expansion and the integral formula [13, (8.350.1)], the function $I(x)$ could be calculated as

$$
\begin{aligned}
I(x) &\approx \sum_{n=0}^{+\infty}\sum_{k=0}^n\sum_{l=0}^k \frac{e^{-\beta_2}}{\alpha(\beta_2+1)^{\frac{3}{\alpha}}}\frac{(\beta_2)^n}{n!k!}\binom{k}{l}\left(-\frac{N}{D^{2\alpha}}\right)^l \\
&\quad \left(\frac{x}{\rho}\right)^{-\frac{3}{\alpha}-l}\gamma\left(k+l+\frac{3}{\alpha}, (\beta_2+1)\frac{x}{\rho}R^\alpha\right).
\end{aligned}
$$
$$(15)$$

Note that an infinite summation is involved in the above result. To reduce the computational complexity as well as preserve approximation accuracy, we truncate the summation up to $\bar{n}$. As shown by our simulation results in the following section, the approximate expressions match their exact values very well.

Then, the CDF of the overall eavesdropping SNR is given by

$$F_{\gamma_E}(x) = \exp\left(-2\pi\rho_S I(x)\right). \quad (16)$$

C. Secrecy Capacity Analysis

With the aid of $F_{\gamma_B}(x)$ and $F_{\gamma_E}(x)$, the ergodic secrecy capacity could be expressed as follows

$$C_s = \frac{1}{\ln 2}\left(\int_0^{+\infty}\frac{\bar{F}_{\gamma_B}(x)}{1+x}\mathrm{d}x - \int_0^{+\infty}\frac{\bar{F}_{\gamma_B}(x)\bar{F}_{\gamma_E}(x)}{1+x}\mathrm{d}x\right), \quad (17)$$

where $\bar{F}_{\gamma_B}(x)$ and $\bar{F}_{\gamma_E}(x)$ denote the complementary CDFs of γ_B and γ_E, respectively [3].

By substituting (5) and (16) into (17), using the representations of elementary functions in terms of Meijer's G-Function [14, (8.4.2.5), (8.4.16.2)] [15, Eq. (21)] and invoking the Gauss-Chebyshev quadrature approximation [16], the ergodic secrecy capacity could be expressed as

$$
\begin{aligned}
C_s &\approx \frac{1}{\ln 2}\left(\frac{G_{2,3}^{3,1}\left[\frac{1}{\rho(Dd_B)^{-\alpha}\theta}\Big|_{0,\hat{k},0}^{0,1}\right]}{\Gamma(\hat{k})} - \frac{\pi^2}{4W}\sum_{j=1}^W \frac{\sqrt{1-t_j^2}}{1+\nu(t_j)}\right. \\
&\quad \left.\sec^2(\frac{\pi}{4}(t_j+1))\left[1 - e^{-2\pi\rho_S I(\nu(t_j))}\right]\frac{\Gamma(\hat{k}, \frac{\nu(t_j)}{\rho(Dd_B)^{-\alpha}\theta})}{\Gamma(\hat{k})}\right),
\end{aligned}
$$
$$(18)$$

where $t_j = \cos(\frac{2j-1}{2W}\pi)$ and $\nu(t_j) = \tan(\frac{\pi}{4}(t_j+1))$.

IV. SECRECY PERFORMANCE ANALYSIS IN MULTIPLE ANTENNAS SCENARIO

In this section, we consider the scenario where the BS is equipped with multiple antennas. We assume that the number of antenna elements is K and the BS's beamforming vector is $\mathbf{w}$. The received SNR of Bob could then be calculated as

$$\gamma_B = \rho(Dd_B)^{-\alpha}\left|\mathbf{g}^H\Phi\mathbf{H}\mathbf{w}\right|^2, \quad (19)$$

where $\mathbf{g}_{N\times 1}$, $\Phi = \mathrm{diag}\{e^{j\phi_1},\cdots,e^{j\phi_N}\}$ and $\mathbf{H}_{N\times K}$ denote the RIS-Bob channel, the phase shift matrix of the RIS and the BS-RIS channel, respectively.

The received SNR of E_k could be expressed as

$$\gamma_{E_k} \approx \rho\left|D^{-\alpha}\mathbf{v}_k^H\Phi\mathbf{H}\mathbf{w} + r_k^{-\frac{\alpha}{2}}\mathbf{u}_k^H\mathbf{w}\right|^2 \triangleq \rho\left|Z_{E_k}\right|^2, \quad (20)$$

where $\mathbf{v}_k$ and $\mathbf{u}_k$ denote the small scale fading of the RIS-UAV link and the BS-UAV link, respectively. Since it is quite challenging to derive the optimal phase shift design and the exact distribution of γ_B and γ_{E_k} in general cases, we consider a special case where the phase shifts of RIS are randomly distributed and the BS leverages maximum ratio transmission (MRT) beamforming scheme, namely, we assume that ϕ_i is randomly distributed and $\mathbf{w} = \frac{(\mathbf{g}^H \boldsymbol{\Phi} \mathbf{H})^H}{||\mathbf{g}^H \boldsymbol{\Phi} \mathbf{H}||}$ with $|| \cdot ||$ denoting the l^2-norm of a vector. Under such assumptions, the received SNR of Bob and E_k could be given as

$$\gamma_B = \rho \sum_{j=1}^{K} \left| \sum_{i=1}^{N} g_i^* h_{i,j} e^{j\phi_i} \right|^2, \qquad (21)$$

and

$$\gamma_{E_k} = \rho \left| \sum_{j=1}^{K} \left(D^{-\alpha} \sum_{i=1}^{N} v_{k,i}^* h_{i,j} e^{j\phi_i} + r_k^{-\frac{\alpha}{2}} u_{k,i}^* \right) \mathrm{w}_j \right|^2, \qquad (22)$$

respectively, where $h_{i,j}$ denotes the (i,j)-th element of $\mathbf{H}$, $v_{k,i}$ and $u_{k,i}$ denotes the i-th element of $\mathbf{v}_k$ and $\mathbf{u}_k$, w_j denotes the j-th element of $\mathbf{w}$, and $(\cdot)^*$ denotes the conjugate of a complex number.

Due to the fact that $\mathbb{E}(||\mathbf{w}||^2) = \sum_{j=1}^{k} \mathbb{E}(||\mathrm{w}_j||^2) = 1$, we have $\mathbb{E}(Z_{E,k}) = 0$ and $\mathbb{E}(|Z_{E,k}|^2) = r_k^{-\alpha} + \frac{N}{D^{2\alpha}}$. Therefore, when the number of antennas is large, according to CLT, the received SNR of the k-th eavesdropper could be approximated as a complex Gaussian random variable with zero mean and variance $r_k^{-\alpha} + \frac{N}{D^{2\alpha}}$, namely, $Z_{E_k}|r_k \sim \mathcal{CN}\left(0, r_k^{-\alpha} + \frac{N}{D^{2\alpha}}\right)$. Consequently, the unconditional SNR of the eavesdroppers could be approximated as

$$F_{\gamma_E}(x) \approx \exp\left\{ -2\pi \rho_S \int_0^R r^2 e^{-\frac{x}{\rho\left(\frac{N}{D^{2\alpha}} + r_k^{-\alpha}\right)}} \mathrm{d}r \right\}, \quad (23)$$

defining $I(x) \triangleq \int_0^R r^2 e^{-\frac{x}{\rho\left(\frac{N}{D^{2\alpha}} + r_k^{-\alpha}\right)}} \mathrm{d}r$ and similar to the derivation of (15), we obtain

$$\begin{aligned} I(x) \approx &\frac{1}{\alpha}\left(\frac{x}{\rho}\right)^{-\frac{3}{\alpha}} \gamma\left(\frac{3}{\alpha}, \frac{x}{\rho\left(R^{-\alpha} + \frac{N}{D^{2\alpha}}\right)}\right) + \frac{3}{\alpha}\left(\frac{3}{\alpha} + 1\right) \\ &\times \frac{N}{D^{2\alpha}}\left(\frac{x}{\rho}\right)^{-\frac{3}{\alpha}-1} \gamma\left(\frac{3}{\alpha}+1, \frac{x}{\rho\left(R^{-\alpha} + \frac{N}{D^{2\alpha}}\right)}\right). \end{aligned} \qquad (24)$$

Similarly, the CDF of Bob's received SNR could be approximated as

$$F_{\gamma_B}(x) \approx \frac{1}{\Gamma(K)} \gamma\left(K, \frac{x}{N\rho(Dd_B)^{-\alpha}}\right). \qquad (25)$$

Finally, leveraging Gauss-Chebyshev quadrature again, the ergodic secrecy capacity in multiple antenna scenario could be calculated in a similar way to (18).

V. SIMULATION RESULTS

In this section, we validate the analytical and approximate results through Monte-Carlo simulations. Unless otherwise stated, the parameters are set as follows: $\rho = 20$dB, $N = 100$, $K = 200$, $R = 50$m, $D = 100$m, $d_B = 10$m, $\alpha = 2$, $\rho_S = 10^{-4}$, $\beta_1 = \beta_2 = 3$dB, $f = 2.4$GHz and $\delta = \lambda/4$. Moreover, the infinite summations of the approximated expressions are truncated to $\bar{n} = 10$ and the Gauss-Chebyshev parameter W is set to $W = 20$ to reduce computational complexity as well as preserve approximation accuracy.

In Fig. 1, the approximate and empirical CDFs of the legitimate user and Eves under different average transmit SNRs are presented. Firstly, it could be readily found that the Gamma distribution approximation of the legitimate SNR is close to its exact CDF, which validates the effectiveness of the proposed Gamma distribution approximate procedure. Secondly, the approximation of Eve's received SNR matches the simulation results in various scenarios, which demonstrates the accuracy of our mathematical derivations. Furthermore, when the BS is equipped with multiple antennas, the SNR of Bob increases significantly while the SNR of Eve changes slightly, which demonstrates that the integration of multiple antennas and RIS will be a promising technique to enhance the secrecy performance of wireless systems. One can also figure out that the approximation of Eve's SNR is much more computationally effective than directly calculating numerical integration, since the infinite summation of the approximation is truncated to tens of times instead of calculating an infinite integral. Actually, the effectiveness of the truncated summation approach could be validated by the mathematical structure of Marcum-Q function according to [17]. Specifically, a Marcum-Q function could be expressed as a weighted summation of an infinite number of lower incomplete Gamma functions. Due to the monotonically decreasing property of lower incomplete Gamma function $\gamma(n, z)$ with respect to n and the rapid growth speed of $n!$ as n increases, it would be reasonable to neglect the higher order items which contribute a little in the infinite summation, thus an accurate approximation to Marcum-Q function could be obtained henceforth.

In Fig. 2, we plot the secrecy capacity versus average transmit SNR in single antenna scenario. As observed from Fig. 2, the secrecy capacity increases with the transmit power, which demonstrates that the deployment of a RIS greatly enhances the legitimate channel while slightly strengthens the eavesdropping channel. Moreover, the slope of the secrecy capacity versus ρ increases as the number of RIS elements increases, which demonstrates the SNR-enhanced effect of the RIS and motivates the deployment of a larger scale RIS to improve the secrecy performance.

Fig. 3 depicts the secrecy capacity versus the number of antenna elements K. It is shown that the secrecy capacity increases with K, which demonstrates that the integration of multiple antennas and RIS is a potential technique in enhancing physical layer security of wireless system.

Fig. 4 characterizes the secrecy capacity versus the maximum distance between Eves and the BS. As expected, the secrecy capacity increases as the UAVs gradually moves further from the BS, which illustrates that a setup of a protected zone around the BS to surveil Eves would improve the secrecy performance and alleviate information leakage. Nevertheless, Fig. 4 presents that the secrecy capacity increases slightly versus R but increases significantly as the number of RIS

elements increases, which demonstrates that the deployment of RIS would be a beneficial method to enhance secure information transmissions with lower cost and higher energy efficiency.

VI. Conclusion

In this letter, we study the secrecy performance of a RIS-aided communication system with spatially random UAVs acting as eavesdroppers. We derive the analytical expressions for the SNRs of the legitimate user and Eves and approximate the results in a computational effective method, considering both single and multiple antennas scenarios using stochastic geometry. Finally, we validate our results through Monte-Carlo simulations. We have found that the deployment of a larger scale RIS would effectively and economically secure the information transmission. The integration of multiple antennas with RIS and the setup of a protected zone would further enhance the secrecy performance of wireless system.

References

[1] J. Tang, G. Chen and J. P. Coon, "Secrecy Performance Analysis of Wireless Communications in the Presence of UAV Jammer and Randomly Located UAV Eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 3026-3041, Nov. 2019.
[2] J. Ye, C. Zhang, H. Lei, G. Pan and Z. Ding, "Secure UAV-to-UAV Systems With Spatially Random UAVs," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 564-567, Apr. 2019.
[3] K. Wang, H. Lei, G. Pan, C. Pan and Y. Cao, "Detection Performance to Spatially Random UAV Using the Ground Vehicle," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16320-16324, Dec. 2020.
[4] C. Liu, et al., "Secure UAV communication in the presence of active eavesdropper (invited paper)," *Proc. WCSP*, Nanjing, China, 2017.
[5] S. Li, et al., "Robust Secure UAV Communications With the Aid of Reconfigurable Intelligent Surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402-6417, Oct. 2021.
[6] Y. Li, et al., "Joint Resource, Trajectory, and Artificial Noise Optimization in Secure Driven 3-D UAVs With NOMA and Imperfect CSI," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3363-3377, Nov. 2021.
[7] L. Yang, et al., "Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296-12300, Oct. 2020.
[8] 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.
[9] Z. Xie, W. Yi, X. Wu, Y. Liu and A. Nallanathan, "STAR-RIS Aided NOMA in Multi-Cell Networks: A General Analytical Framework with Gamma Distributed Channel Modeling", Aug. 2021, *arXiv: 2108.06704*.
[10] H. Ren, K. Wang and C. Pan, "Intelligent Reflecting Surface-Aided URLLC in a Factory Automation Scenario," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 707-723, Jan. 2022.
[11] J. Ye, et al., "Spatially-Distributed RISs vs Relay-Assisted Systems: A Fair Comparison," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 799-817, 2021.
[12] H. Sun, D. I. Laurenson and C. Wang, "Computationally Tractable Model of Energy Detection Performance over Slow Fading Channels," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 924-926, Oct. 2010.
[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th. San Diego,CA: Academic Press, 2007.
[14] A. P. Prudnikov, et al., *Integrals and Series. Vol. 3, More Special Functions*, New York, NY, USA: Gordon Breach, 2003.
[15] V. S. Adamchik et al., "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," *Proc. Int. Symp. Symb. Algebraic Comput.,* Tokyo, Japan, Aug. 1990, pp. 212–224.
[16] Do. D and Le. C, "Ergodic capacity computation in cognitive radio aided non-orthogonal multiple access systems," Bulletin of Electrical Engineering and Informatics, v. 11, n. 1, p. 270-277, Feb. 2022.
[17] Gil, A., Segura, J. and Temme, N.M. (2014), "The Asymptotic and Numerical Inversion of the Marcum Q-Function," *STUDIES IN APPLIED MATHEMATICS*, 133: 257-278.
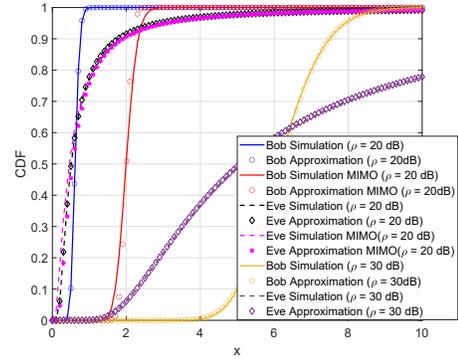
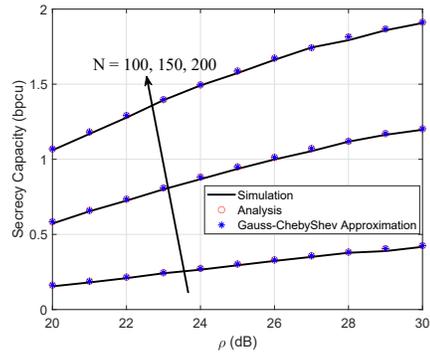Fig. 1. Approximate and empirical CDFs of legitimate user and UAV Eves.

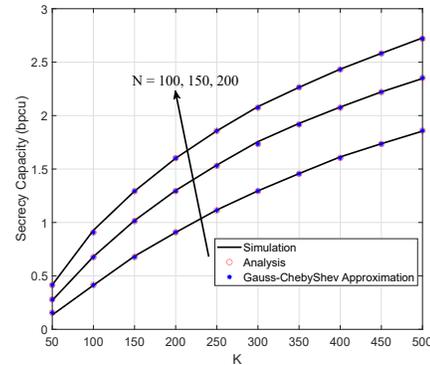Fig. 2. Ergodic secrecy capacity versus transmit power in single antenna scenario.

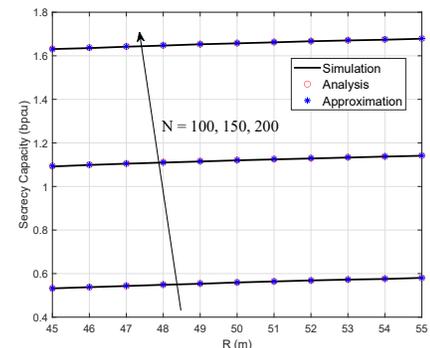Fig. 3. Ergodic secrecy capacity versus number of antenna elements in multiple antenna scenario.

Fig. 4. Ergodic secrecy capacity versus the maximum radius of Eves' distribution area.