Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems

Liang Yang, Jinxia Yang, Wenw Xie, Mazen O Hasna, Theodoros Tsiftsis, Marco Di Renzo

Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems

Liang Yang, Jinxia Yang, Wenwu Xie, Mazen O. Hasna, Theodoros Tsiftsis, Marco Di Renzo

***Abstract*—In this work, we study the secrecy performance of a reconfigurable intelligent surfaces (RIS)-aided wireless communication system in the presence of an eavesdropping user. Specifically, we assume that the RIS is placed between the source and the legitimate user to create a smart environment and used to improve the link security. In particular, analytical results for the secrecy outage probability (SOP) is derived. We also provide an asymptotic analysis to investigate the effect of the main parameters on the secrecy performance of our proposed system, such as the number of the reflectors in the RIS and the average signal-to-noise ratios. Finally, we verify our analytical results via simulations. Results show the positive effect of utilizing the RIS for enhancing wireless systems secrecy performance.**

***Index Terms*—Physical layer security, RIS, secrecy outage probability.**

I. Introduction

RECONFIGURABLE Intelligence Surfaces (RISs), which are man-made surfaces of electromagnetic (EM) material that are electronically controlled with integrated electronics, have received considerable attention due to their unique wireless communication capabilities [1]. The main advantage of RISs is their ability to control the transmission environment and improve the signal quality at the receiver, and hence they can be thought of as enablers in converting propagation environments into smart ones. In comparison with the competing wireless relaying technology, RIS devices do not need extra energy sources and can shape the transmission signal by soft programming. Moreover, the process of signal transmission through the RISs is not complicated due to the characteristics of EM materials. Thus, encoding and decoding operations are not needed. Another advantage of RISs is the fact that they are not easily affected by external electromagnetic interference and can operate in full-duplex transmission mode with full-band response. Hence, RISs are expected to play a key role and to be one of the major technologies for future wireless systems.

Being a new technology, RISs and their typical applications in wireless communication systems have been studied only in few papers [2]-[5]. For example, the authors in [2] proposed using RISs to realize massive device-to-device (D2D) communications where each RIS acts as a signal reflection hub to support simultaneous low-power transmissions through interference mitigation. In addition, the application of RISs for realizing simultaneous wireless information and power transfer (SWIPT) to various devices in an Internet-of-things (IoT) network was considered in [3], where the large aperture of the RIS can improve the efficiency of wireless power transfer. Besides, in [4], Huang *et al.* studied the adoption of RIS devices for downlink multi-user communication.

In recent years, physical layer security (PLS) in wireless communication systems has gained more attention and several techniques have been proposed to improve the secrecy performance of wireless systems, such as cooperative diversity, spatial diversity. Given that PLS leverages the physical characteristics of the propagation environment, it is both natural and interesting to study the PLS performance when using RISs. While PLS for different wireless systems has been extensively studied in the literature [6]-[8], applying the RIS to improve the PLS is still not well investigated. To the best of the authors knowledge, the secrecy performance for systems employing RISs has been recently considered only in [9]-[12]. However, the authors in [9]-[12] focus on the optimization design, such as beamforming and jamming.

In this work, we study the secrecy performance of systems using the RIS. More specifically, we assume a smart environment in which an RIS is placed between the source and the legitimate user to enhance the main link. Meanwhile, the eavesdropper also can receive signals from the RIS. For a practical consideration, we consider a general system model where the direct links between the source and the the legitimate user (or the eavesdropper) exist. The goal of the paper is to quantify the gain received from using RISs in such setup on the PLS of the system in terms of the secrecy outage probability (SOP) metric. To obtain more insights, the paper also provides an asymptotic SOP analysis for high signal to noise ratios (SNRs) and large number of RIS elements.

II. System and Channel Model

As shown in Fig. 1, consider an RIS-aided wireless communication system including a source, a legitimate user, an eavesdropper, and an RIS that is composed of N reflecting meta-surfaces, where all the nodes are only equipped with single antennas and the direct links for both the legitimate user and the eavesdropper exist. We assume that all the channels experience Rayleigh fading and the channel gains

L. Yang is with the college of Computer Science and Electronic Engineering. Hunan University, Changsha 410082, China (Email: liangyang.guangzhou@gmail.com)

J. Yang and W. Xie are with the Department of Information Science and Engineering, Hunan Institute of Science and Technology, Yueyang, 414006 China (Email: gavinxie2015@qq.com; magicyangyeah@qq.com).

M. O. Hasna is with the Qatar University, Doha, Qatar.

T. Tsiftsis is with the Jinan University Zhuhai College, Zhuhai, Guangdong, 519070.

M. Di Renzo is with Paris-Saclay University (L2S-CNRS, CentraleSup'elec, University Paris Sud), Paris, France.

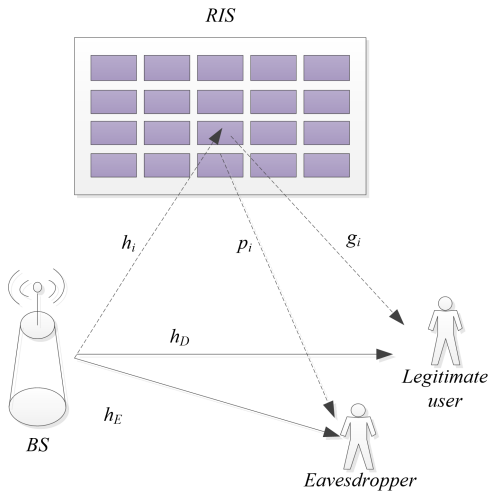

Fig. 1: System diagram of an RIS-based system with an eavesdropper

follow the complex Gaussian distribution with zero mean and unit variance. The signal propagates from the source to the legitimate user by one or more specular reflections and adjustments of the RIS, which aims to improve the signal quality at the legitimate user. Meanwhile, the eavesdropper attempts to obtain the signal from the source and can receive signals from the RIS reflection. Furthermore, we assume that the RIS can obtain the channel state information (CSI) of the legitimate user. Thus, the RIS can use this obtained CSI to implement the phase shifting for the main channels, which maximizes the received SNR at the legitimate user. However, for physical layer security consideration, it is not necessary to assume that the RIS can obtain the CSI of the wiretap channels to maximize the SNR at the eavesdropper. Thus, this is a passive eavesdropping scenario. For such a case, the eavesdropper remains silence and the source transmits signals at a fixed rate R_s. Then, the secure transmission can not be guaranteed when the secrecy rate is lower than R_s and the metric to compute the secrecy performance would be the SOP.

A. The Main Link

We assume a slowly varying and flat fading channel model for all the involved channels. Then, the received signal reflected by the RIS can be expresses as [1]

$$r = \left[h_D + \sum_{i=1}^{N} h_i g_i e^{j\phi_i} \right] x + n \tag{1}$$

where ϕ_i is the adjustable phase induced by the ith reflecting meta-surface of the RIS, x stands for the data symbol selected from an M-ary phase shift keying/quadrature amplitude modulation (PSK/QAM) constellation, and $n \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) modeled as a zero-mean complex Gaussian distribution with variance N_0. In (1), h_D is the channel gain between the source and the the legitimate user, h_i is the channel gain between the source and the RIS, while g_i is the channel coefficient between the RIS and the legitimate user for the ith reflecting meta-surface $(i = 1, 2, ..., N)$. Furthermore, $h_D = d_{bd}^{-\chi/2} \eta e^{-j\tau}$ [13], where d_{bd} and τ are the distance and adjustable phase between the source and legitimate user, respectively, χ denote the path loss coefficient, and η is the Rayleigh distributed random variable (RV). The RIS is assumed to provide adjustable phase shifts that are controlled and programmed through a communication-oriented software. Similar to [1], perfect knowledge of the channel phases of h_i and g_i for $i = 1, 2, ..., N$ at the RIS is also assumed, which corresponds to the best scenario in terms of system operation and yields a performance benchmark for practical applications. Then, we have

$$h_i = d_{br}^{-\chi/2} \alpha_i e^{-j\theta_i} \tag{2}$$

$$g_i = d_{rd}^{-\chi/2} \beta_i e^{-j\psi_i} \tag{3}$$

where d_{br} is the distance between the source and the RIS, d_{rd} is the distance between the RIS and the legitimate user, θ_i and ψ_i are the channel phases, and α_i and β_i are independent Rayleigh-distributed RVs. From [13], we consider the diffuse scattering, then the resulting SNR can be formulated as

$$\begin{aligned}
\gamma_D &= \frac{\left| h_D \sqrt{E_s} + \sum_{i=1}^{N} h_i g_i \sqrt{E_s} \right|^2}{N_0} \\
&\approx \frac{|h_D|^2 E_s}{N_0} + \frac{\left| \sum_{i=1}^{N} \alpha_i \beta_i e^{j(\phi_i - \theta_i - \psi_i)} \right|^2 E_s}{d_{br}^{\chi} d_{rd}^{\chi} N_0} \\
&= \frac{|h_D|^2 E_s}{N_0} + \frac{\left| \sum_{i=1}^{N} \alpha_i \beta_i \right|^2 E_s}{d_{br}^{\chi} d_{rd}^{\chi} N_0} \\
&= |h_D|^2 \bar{\gamma}_{bd} + A^2 \bar{\gamma}_{brd}
\end{aligned} \tag{4}$$

where $\bar{\gamma}_{bd}$ and $\bar{\gamma}_{brd}$ are the average SNRs. In (4), for tractable analysis, we adopt the approximate equation and $\phi_i = \theta_i + \psi_i$ is assumed to maximize the received SNR. From [1], the mean value and the variance of A are $s = \frac{N\pi}{4}$ and $\sigma^2 = N\left(1 - \frac{\pi^2}{16}\right)$, respectively. According to the central limit theorem (CLT), A^2 is a non-central chi-square random variable with one degree of freedom. From [14, eq.(2.3.29)], the probability density function (PDF) of A^2 is given by

$$f_{A^2}(x) = \frac{\sqrt{s}}{2\sigma^2} e^{-\frac{s^2}{2\sigma^2}} x^{\frac{-1}{4}} e^{-\frac{x}{2\sigma^2}} I_{-\frac{1}{2}}\left(\frac{s\sqrt{x}}{\sigma^2}\right) \tag{5}$$

where $I_a(x)$ is the modified Bessel function of the first kind. However, using Eq.(5) to evaluate the SOP is very difficult. Thus, we apply the developed method in [15] to express the PDF of A^2. Then, the PDF of A_2 can be rewritten as

$$f_{A^2}(x) = \sum_{i=1}^{M} \omega_i x^{\kappa_i - 1} e^{-\frac{x}{2\sigma^2}} \tag{6}$$

where $\omega_i = \frac{\sqrt{s}}{2\sigma^2} e^{-\frac{s^2}{2\sigma^2}} \frac{1}{(i-1)!\Gamma(i-1/2)} \left(\frac{s}{2\sigma^2}\right)^{2i-\frac{5}{2}}$, $\kappa_i = i - \frac{1}{2}$, M is the number of terms, and $\Gamma(\cdot)$ is the gamma function. Thus, the cumulative distribution function (CDF) of γ_D can be written as

$$F_{\gamma_D}(\gamma_D) = P\left(|h_D|^2\bar{\gamma}_{bd}+A^2\bar{\gamma}_{brd} < \gamma_D\right) = \int_0^{\infty}\left[\int_0^{\frac{\gamma_D-\bar{\gamma}_{brd}y}{\bar{\gamma}_{bd}}} f_{|h_D|^2}(x)\,dx\right] f_{A^2}(y)\,dy \quad (7)$$

Then, substituting (6) into (7) and making use of [15, eq.(2)], the CDF of γ_D can be further expressed as

$$F_{\gamma_D}(\gamma_D) = \sum_{i=1}^{M}\omega_i\left(\frac{1}{2\sigma^2}\right)^{-\kappa_i}\gamma\left(\kappa_i, \frac{\gamma_D}{2\sigma^2\bar{\gamma}_{brd}}\right) - e^{-\frac{\gamma_D}{\bar{\gamma}_{bd}}}\sum_{i=1}^{M}\omega_i\left(\frac{c}{\bar{\gamma}_{brd}}\right)^{-\kappa_i}\gamma(\kappa_i, c\gamma_D) \quad (8)$$

where $c = \frac{\bar{\gamma}_{bd}-2\sigma^2\bar{\gamma}_{brd}}{2\sigma^2\bar{\gamma}_{bd}\bar{\gamma}_{brd}}$, $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function. With (8), the PDF of γ_D can be obtained as

$$f_{\gamma_D}(\gamma_D) = \sum_{i=1}^{M}\omega_i\left(\frac{\gamma_D}{\bar{\gamma}_{brd}}\right)^{\kappa_i-1}\left(e^{-\frac{\gamma_D}{2\sigma^2\bar{\gamma}_{brd}}} - e^{-c\gamma_D}\right) \quad (9)$$

B. The Eavesdropping Link

For the eavesdropper, except the signal from the direct link, it also receives signals from the RIS. Let $h_E = d_{be}^{-\chi/2}\eta_e e^{-j\tau_e}$ denote the channel gain between the source and the eavesdropper, where τ_e is channel phase and d_{be} is the distance between the source and the eavesdropper. Furthermore, let $p_i = d_{re}^{-\chi/2}\beta_{ei}e^{-j\psi_{ei}}$ denote the channel gain between the RIS and the eavesdropper, where ψ_{ei} is channel phase and d_{re} denotes the distance between the RIS and the eavesdropper, both η_e and β_{ei} are independent Rayleigh-distributed RVs. Then, the resulting SNR at the eavesdropper can be expressed as

$$\begin{aligned}\gamma_E &= \frac{\left|h_E\sqrt{E_s} + \sum_{i=1}^{N} h_i p_i e^{j\phi_{ei}}\sqrt{E_s}\right|^2}{N_0} \\ &\approx \frac{|h_E|^2 E_s}{N_0} + \frac{\left|\sum_{i=1}^{N}\alpha_i\beta_i^e e^{j(\phi_{ei}-\theta_i-\psi_{ei})}\right|^2 E_s}{d_{br}^{\chi}d_{re}^{\chi}N_0} \\ &= |h_E|^2\bar{\gamma}_{be} + \left|\sum_{i=1}^{N}\alpha_i\beta_{ei}e^{j(\phi_{ei}-\theta_i-\psi_{ei})}\right|^2\bar{\gamma}_{bre} \\ &= |h_E|^2\bar{\gamma}_{be} + B^2\bar{\gamma}_{bre} \end{aligned} \quad (10)$$

where $\bar{\gamma}_{be}$ and $\bar{\gamma}_{bre}$ are the average SNRs. Note that B^2 is a central chi-square random variable with two degrees of freedom. Similar to the analysis for Eq.(7), the CDF of γ_E can be readily expressed as

$$F_{\gamma_E}(\gamma_E) = 1 - \frac{\bar{\gamma}_{be}e^{-\frac{\gamma_E}{\bar{\gamma}_{be}}} + 2\sigma_e^2\bar{\gamma}_{bre}e^{-\frac{\gamma_E}{2\bar{\gamma}_{bre}\sigma_e^2}}}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}} \quad (11)$$

Similarly, the PDF of γ_E is given by

$$f_{\gamma_E}(\gamma_E) = \frac{1}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}}\left(e^{-\frac{\gamma_E}{\bar{\gamma}_{be}}} - e^{-\frac{\gamma_E}{2\bar{\gamma}_{bre}\sigma_e^2}}\right) \quad (12)$$

III. Secrecy Outage Probability Analysis

In this section, we analyze the SOP. Also, an asymptotic SOP analysis is presented.

A. SOP analysis

SOP, which is defined as the probability that both communication sides can realize secure communication under certain conditions, is a typical performance measure for PLS. Then, the instantaneous secrecy rate can be expressed as

$$C_s(\gamma_D,\gamma_E) = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\} \quad (13)$$

From [16], SOP can be written as

$$\begin{aligned} SOP &= \Pr\{C_s(\gamma_D,\gamma_E) < C_{th}\} \\ &= \Pr\left\{\gamma_E > \frac{1+\gamma_D-\theta}{\theta}\right\} \\ &= \int_0^{\infty}\int_{\frac{\gamma_D+1-\theta}{\theta}}^{\infty} f_{\gamma_E}(\gamma_E)d\gamma_E f_{\gamma_D}(\gamma_D)d\gamma_D \end{aligned} \quad (14)$$

where C_{th} is the target secrecy rate and $\theta = e^{C_{th}}$. Then, substituting (9), (12) into (14), we obtain

$$\begin{aligned} SOP &= \int_0^{\infty}\int_{\frac{\gamma_D+1-\theta}{\theta}}^{\infty} f_E(\gamma_E)d\gamma_E f_{\gamma_D}(\gamma_D)d\gamma_D \\ &= \int_0^{\infty}\frac{\bar{\gamma}_{be}}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}}e^{-\frac{\gamma_D+1-\theta}{\bar{\gamma}_{be}\theta}}f_{\gamma_D}(\gamma_D) - \\ &\quad \frac{2\bar{\gamma}_{bre}\sigma_e^2}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}}e^{-\frac{\gamma_D+1-\theta}{2\sigma_e^2\bar{\gamma}_{bre}\theta}}f_{\gamma_D}(\gamma_D)d\gamma_D \\ &= I_1 - I_2 \end{aligned} \quad (15)$$

where $\sigma_e^2 = N/2$, using [17, eq.(6.451.1)] and the Taylor form of the exponential function, I_1 and I_2 can be obtained as

$$\begin{aligned} I_1 &= \frac{\bar{\gamma}_{be}^2 c_e\theta}{\bar{\gamma}_{bd}+\bar{\gamma}_{be}\theta}e^{\frac{\theta-1}{\bar{\gamma}_{be}\theta}}\sum_{i=1}^{M}\omega_i\Gamma(\kappa_i)\left(1+\frac{\bar{\gamma}_{brd}}{\bar{\gamma}_{be}\theta}+\frac{\bar{\gamma}_{brd}}{\bar{\gamma}_{bd}}\right)^{i+\frac{1}{2}} \\ &= \frac{\bar{\gamma}_{be}^2\theta c_e}{\bar{\gamma}_{bd}+\bar{\gamma}_{be}\theta}\left(\frac{\bar{\gamma}_{be}\theta}{\bar{\gamma}_{be}\theta+2\bar{\gamma}_{brd}\sigma^2}\right)^{\frac{1}{2}}e^{-\frac{\bar{\gamma}_{brd}s^2}{\bar{\gamma}_{be}\theta+2\bar{\gamma}_{brd}\sigma^2}+\frac{\theta-1}{\bar{\gamma}_{be}\theta}} \end{aligned} \quad (16)$$

and

$$\begin{aligned} I_2 &= \sum_{i=1}^{M}\omega_i\Gamma(\kappa_i)\left(\varsigma_2+\frac{\bar{\gamma}_{brd}}{2\bar{\gamma}_{bre}\sigma_e^2\theta}+\frac{\bar{\gamma}_{brd}}{\bar{\gamma}_{bd}}\right)^{i+\frac{1}{2}} \\ &\quad\times\frac{4\bar{\gamma}_{bre}^2\sigma_e^4\theta}{\bar{\gamma}_{bd}+2\bar{\gamma}_{bre}\sigma_e^2\theta}\frac{1}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}}e^{\frac{\theta+1}{2\bar{\gamma}_{bre}\sigma_e^2\theta}} \\ &= \frac{4\sigma_e^4\bar{\gamma}_{bre}^2\theta c_e}{\bar{\gamma}_{bd}+2\sigma_e^2\bar{\gamma}_{bre}\theta}\left(\frac{\bar{\gamma}_{bre}\sigma_e^2\theta}{2\bar{\gamma}_{bre}\sigma_e^2\theta+2\bar{\gamma}_{brd}\sigma^2}\right)^{\frac{1}{2}} \\ &\quad\times e^{-\frac{s^2}{2}\frac{\bar{\gamma}_{brd}}{\bar{\gamma}_{bre}\sigma_e^2\theta+\bar{\gamma}_{brd}\sigma^2}-\frac{1-\theta}{2\bar{\gamma}_{bre}\sigma_e^2\theta}} \end{aligned} \quad (17)$$

where $c_e = \frac{1}{\bar{\gamma}_{be}-2\sigma_e^2\bar{\gamma}_{bre}}$, $\varsigma_2 = \frac{\bar{\gamma}_{bd}-2\sigma^2\bar{\gamma}_{brd}}{2\sigma^2\bar{\gamma}_{bd}}$. Finally, substituting I_1 and I_2 into (15) completes the SOP analysis.

B. Asymptotic SOP Analysis

To obtain some insights, we analyze the asymptotic behavior of the above results. On the one hand, if let $\bar{\gamma}_{brd} \to \infty$ and

fix $\bar{\gamma}_{bre}$, we can readily observe that $SOP \to 0$. On the other hand, if let $\bar{\gamma}_{brd} \to \infty$, and fix the ratios $\frac{\bar{\gamma}_{bd}}{\bar{\gamma}_{be}} = K$ and $\rho = \frac{\bar{\gamma}_{bd}}{\bar{\gamma}_{brd}}$, we have

$$SOP \to \frac{\theta^{3/2}}{(K+\theta)\sqrt{\varepsilon}} e^{-\frac{Ks^2}{\rho\varepsilon}} \tag{18}$$

where $\varepsilon = \theta + 2K/\left(\rho\sigma^2\right)$. From (18), we see that the asymptotic SOP expression converges to a constant at high $\bar{\gamma}_{brd}$ when the ratio K is fixed. Moreover, we can observe that the SOP is related to the mean value s and the variance σ^2 of A which are functions of the number of reflecting meta-surface elements N. Moreover, we can readily observe that $SOP \to 0$ when $N \to \infty$. Hence, as expected, increasing the value of N improves the secrecy performance significantly.

IV. Numerical results

In this section, we present numerical examples to verify our analytical results along with the simulation results. In the simulation results, we assume that all the channels suffer from Rayleigh fading.

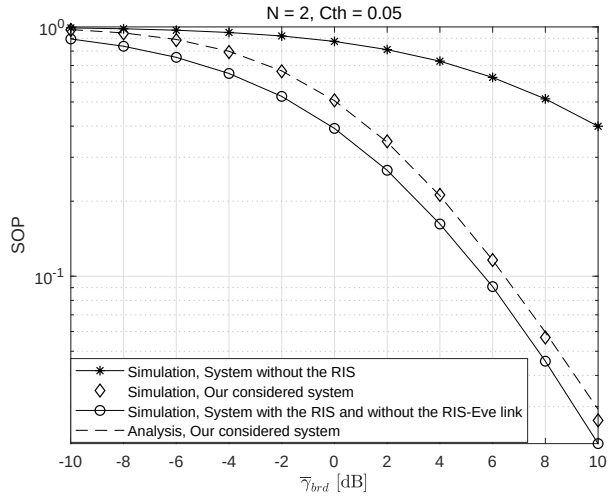

Fig. 2: SOP comparison for the systems with and without the RIS.

In Fig. 2, we plot the SOP versus $\bar{\gamma}_{brd}$ for a single antenna system in the presence of an eavesdropper with and without the RIS, where $N = 2$, $C_{th} = 0.05$, $\bar{\gamma}_{be} = 10dB$, and $\bar{\gamma}_{bre} = 0dB$. Furthermore, we provide the simulation result for the system where the link between the RIS and the eavesdropper does not exist and the eavesdropper only receives signals from the source. It is clearly shown that applying the RIS results in better secrecy performance compared to the other two schemes. The reason is that the RIS can improve the channel quality and enhance the received SNR when phase processing is used. Moreover, we can see that the system with the RIS and without the RIS-Eve link has the best secrecy performance, which means that the secrecy performance becomes worse when the eavesdropper also utilizes the advantage of the RIS.

In Fig. 3, we plot the SOP versus $\bar{\gamma}_{brd}$ for the analytical result (18) along with the asymptotical result, where we set $K = 5$ and $\rho = 6$. From Fig. 3, we can see that increasing

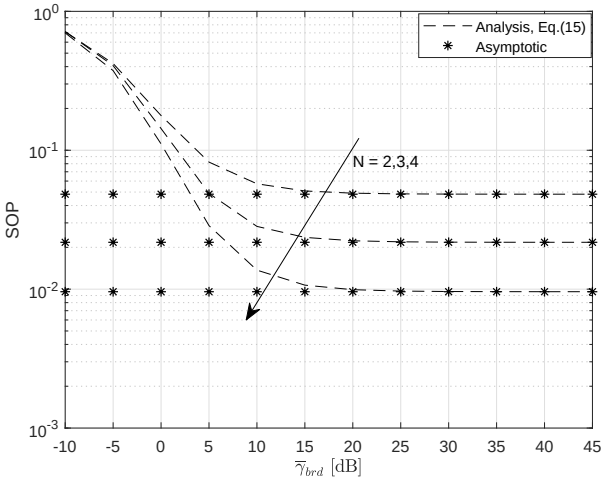

Fig. 3: SOP versus $\bar{\gamma}_{brd}$ for different N.

the number of reflecting meta-surface elements N improves the secrecy performance. Moreover, error floors appear at relatively high $\bar{\gamma}_{brd}$, which verifies our asymptotic analysis.

V. Conclusions

In this work, we provided SOP analysis for a single antenna system in the presence of an eavesdropping link with the help of the RIS. More specially, the expression for SOP was derived and validated through simulations. Results show that applying the RIS can improve the secrecy performance significantly. However, the secrecy performance would become worse when the eavesdropper also enjoy the advantage of the RIS.

References

[1] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access,* vol. 7, pp. 116753-116773, 2019.

[2] Q. Wu, and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,"2019, arXiv:1905.00152. [online]. Available:https://arxiv.org/abs/1905.00152.

[3] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: opportunities and challenges." *IEEE Commun. Mag,* Apr. 2015.

[4] C. Huang, A. Zappone et al., "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.,* vol. 18, no.8, pp. 4157-4170, June 2019.

[5] J. Ye, S. Guo,"Joint reflecting and precoding designs for SER minimization in reconfigurable intelligent surfaces assisted MIMO system,"Jun 2019, arXiv:1906.11466. [online]. Available:https://arxiv.org/abs/1906.11466.

[6] Q. Li , L. Yang,"Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. Inf. Forensics Security.,* vol.15, no.1, 2020.

[7] J. Barros, and M. R. Rodrigues, "Secrecy capacity of wireless channels," *2006 IEEE Inter Symposium on Inf Theory,* pp. 356-360, 2006.

[8] J. Chen, L. Yang and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol,* vol. 67, no. 5, pp. 4645-4649, May 2018.

[9] M. Cui, G. Zhang and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun Lett.,* doi: 10.1109/LWC.2019.2919685.

[10] X. Yu, D. Xu, R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces,"2019, arXiv:1904.09573. [online]. Available: https://arxiv.org/abs/1904.09573.

[11] X. Guan, Q. Wu, R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.,* Jan. 2020, DOI: 10.1109/LWC.2020.2969629.

[12] B. Feng, Y. Wu, M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system, "2019, arXiv:1909.00629.[online]. Available: https://arxiv.org/abs/1909.00629.

[13] K. Ntontin, J. Song, M. Di Renzo, "Multi-Antenna Relaying and Reconfigurable Intelligent Surfaces: End-to-End SNR and Achievable Rate ,"2019, arXiv:1908.07967. [online]. Available:https://arxiv.org/abs/1908.07967.

[14] John G. Proakis, Masoud Salehi, Digital Communications, 5th ed. McGraw-Hill, New York. 2008

[15] A. Saman , T. Chintha , J. Hai, "A Mixture Gamma Distribution to Model the SNR of Wireless Channels," *IEEE Trans Wireless Commun,*vol. 10, no. 12, pp. 4193-4203, Dec. 2011.

[16] Z. Liao, L. Yang, J. Chen, H. Yang and M. Alouini, "Physical layer security for dual-hop VLC/RF communication systems," *IEEE Commun Lett,* vol.22, no.12, pp. 2603-2606, Dec. 2018.

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