This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Secrecy Performance Analysis of RIS-Aided Smart Grid Communications

Masoud Kaveh, Zheng Yan, *Senior Member, IEEE*, and Riku Jäntti, *Senior Member, IEEE*

***Abstract*—A smart grid (SG) is an advanced electrical grid that enhances the efficiency and reliability of traditional power grids. Reconfigurable intelligent surfaces (RISs) have been recently proposed to enhance communication performance in the SG. However, the communication links between different SG components could suffer from eavesdropping and unauthorized access, which makes physical layer security (PLS) a promising solution for addressing these concerns. In this article, we focus on exploring the effect of applying RIS on enhancing the PLS performance of SG communications. Specifically, we consider an RIS with reflecting elements besides a smart meter, a neighborhood gateway (NG), and an eavesdropper to develop a smart environment in the SG to improve PLS performance in terms of secrecy outage probability (SOP) and average secrecy capacity (ASC). For this purpose, we first derive a probability density function and a cumulative distribution function for the signal-to-noise ratio (SNR) at both the NG and the eavesdropper. Then, we derive closed-form expressions of SOP and ASC to evaluate the impact of various system parameters on the secrecy performance of RIS-aided SG communications. Furthermore, considering the significance of system behavior under high-SNR conditions, we conduct an asymptotic analysis of the SOP and ASC. Finally, we apply the Monte Carlo simulation to validate the analytical results. Our results indicate that using the RIS can significantly enhance the secrecy performance of SG communications compared to the conventional SG scenarios without the RIS.**

***Index Terms*—Average secrecy capacity (ASC), physical layer security (PLS), reconfigurable intelligent surfaces (RISs), secrecy outage probability (SOP), smart grid (SG).**

I. Introduction

A SMART grid (SG) is an advanced electrical grid system that uses modern information and communication technology (ICT) to enable two-way information flow besides two-way power flow to improve the efficiency, reliability, and sustainability of the traditional power grid [1]. By employing ICT, the SG can significantly contribute to the current power grid by introducing numerous improvements such as advanced monitoring and control, sound integration of renewable energy resources, enhanced reliability and resiliency, increased flexibility, better energy distribution and customization, and decreasing greenhouse gases emission [2].

However, new security and privacy risks arise in the SG due to the usage of ICT [3], [4]. For example, an eavesdropper can gain access to sensitive information about a costumer's energy consumption habit, which may lead to privacy violation or enable malicious activities. Therefore, establishing secure links is critical for ensuring the confidentiality, integrity, and availability of sensitive data in SG communications. Using physical layer security (PLS) techniques, which leverage the physical properties of a communication channel to provide secure links [5], [6], [7], offers certain advantages over traditional cryptographic approaches in certain SG scenarios, such as reduced computational burden, lower latency, and increased security features [8], [9], [10]. Analyzing the PLS performance is crucial to ensure robust and effective secure communication in wireless networks. In this context, two essential metrics, namely, secrecy outage probability (SOP) and average secrecy capacity (ASC), play pivotal roles [11], [12]. SOP quantifies the likelihood that secure communication is compromised due to unfavorable channel conditions, providing insights into the system's vulnerability against eavesdropping attacks. ASC measures the average rate at which confidential information can be securely transmitted, considering both achievable data rate and security against eavesdroppers [13], [14].

A. Related Works

Several research efforts have focused on investigating the PLS performance of SG communications in recent years. Camponogara et al. [15] explored the benefits of hybrid power line communication (PLC)/wireless channels for improving PLS in low-bit-rate applications. They derived mathematical formulations for ASC and SOP, revealing the advantages of hybrid PLC/wireless models in enhancing PLS when eavesdroppers utilize a single data communication interface. Salem et al. [16] delved into the PLS of cooperative relaying PLC systems with artificial noise. They derived expressions for ASC, highlighting the potential of cooperative relaying to significantly enhance the security of PLC systems. Building on this, Salem et al. [17] extended their study to consider PLS in correlated log-normal cooperative PLC networks. Their work analyzed the impact of

Manuscript received 18 September 2023; revised 13 October 2023; accepted 30 October 2023. This work was supported in part by the Academy of Finland under Grant 345072 and Grant 350464. Paper no. TII-23-3600. *(Corresponding author: Masoud Kaveh.)*

Masoud Kaveh and Riku Jäntti are with the Department of Information and Communication Engineering, Aalto University, 02150 Espoo, Finland (e-mail: masoud.kaveh@aalto.fi; riku.jantti@aalto.fi).

Zheng Yan is with the School of Cyber Engineering, Xidian University, Xi'an 710126, China (e-mail: zyan@xidian.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2023.3333842.

Digital Object Identifier 10.1109/TII.2023.3333842

© 2023 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

background and impulsive noise components, providing mathematical insights into ASC and SOP under various network scenarios.

Odeyemi et al. [18] introduced a dynamic wide area network (WAN) for SGs featuring a friendly jammer to enhance network secrecy. They derived closed-form expressions for connection SOP and ASC, showcasing the network's enhanced security performance. Atallah et al. [19] investigated PLS performance in wireless sensor networks within SG environments. They considered the impact of destination-assisted jamming on secrecy performance metrics and derived analytical expressions for SOP, revealing the potential for significant improvement in security using jamming techniques. El-Shafie et al. [20] studied the influence of wireless network's PLS and reliability on demand-side management in SGs. Their work explored the tradeoff between security and reliability, proposing artificial-noise-aided schemes and encoding strategies to enhance security and reliability in SG. Mohan et al. [21] examined PLS in low-frequency PLC systems, focusing on ASC and SOP. They considered both the independent and correlated log-normal channel distributions, incorporating the impact of impulsive noise and various network parameters.

In conventional SG communications, achieving robust PLS performance has been challenging due to several factors such as presence of interference, channel impairments, and unpredictable wireless conditions due to the dynamic and heterogeneous nature of the SG environment. On the other hand, the reconfigurable intelligent surface (RIS) [22], [23], [24] offers a promising avenue to enhance the PLS performance in wireless communication systems. The RIS takes the advantage of metamaterials to control the reflection and scattering of electromagnetic waves in a controlled manner to enhance the overall communication performance [25]. The controlled manipulation of signal paths through the RIS enables the creation of favorable transmission conditions for the intended receiver while introducing signal degradation for potential eavesdroppers. This dynamic alteration of the wireless channel characteristics contributes to enhanced security levels [26], [27], [28], [29], [30]. Furthermore, the RIS can be optimized to minimize signal leakage to unintended directions, effectively confining the transmission to the intended recipient [31], [32], [33]. Through these mechanisms, the RIS can play a pivotal role in bolstering PLS, making unauthorized interception more challenging and, thus, enhancing the overall security of wireless communication systems. Quite recently, the RIS has been utilized to enhance the communication performance in SG [34]. The authors in [35], [36], [37], and [38] used the RIS in the SG WAN communication system to enhance the signal-to-noise ratio (SNR) at the receiver. To that end, they derived closed-form expressions for average bit error rate and outage probability, showing that by improving the quality and reliability of the wireless communication links in SG, the RIS can help reducing the risk of communication failures, improve the accuracy of data collection, and enhance the overall performance of SG systems. Table I shows the distinctions between prior research and our work, emphasizing the unique aspects of our analysis in this article.

TABLE I
COMPARISON OF RELATED WORKS IN SECRECY PERFORMANCE ANALYSIS OF SG COMMUNICATIONS

Works	I_1	I_2	I_3	I_4	I_5
[15], [17], [21]	✓	✓	×	×	P_2, P_3, P_4
[16]	×	✓	×	×	P_3, P_4
[18]	✓	✓	✓	×	P_2, P_3
[19], [20]	✓	×	×	×	P_2, P_3, P_4
[35], [36]	×	×	✓	✓	P_1, P_2
[37], [38]	×	×	×	✓	P_1, P_2
Ours	✓	✓	✓	✓	P_1, P_2, P_3, P_4, P_5

I_1: SOP analysis, I_2: ASC analysis, I_3: Asymptotic analysis, I_4: RIS integration, I_5: Considered system parameters, P_1: Number of RIS elements, P_2: NG's location, P_3: Eve's location, P_4: SM's transmission power, P_5: Secrecy rate, ✓: Item is supported, and ×: Item is not supported.

B. Motivations and Contributions

Within the framework of typical SG scenarios, attaining effective secrecy performance presents a formidable challenge, attributed to limited received signal strength, confined power resources inherent to smart meters (SMs), the pervasive influence of interference sources, the obstruction posed by physical barriers, and an array of other intricate considerations. Although the potential of RIS to enhance communication performance in SG is intriguing [34], [35], [36], [37], [38], there has been limited exploration on whether the RIS can also improve the PLS performance of SG communication systems. Evaluating secrecy performance metrics in PLS analysis allows us to assess the system's ability to maintain secure communication, helping to design resilient wireless networks that safeguard sensitive information in SG. As a primary step in this regard, deriving closed-form expressions of important secrecy metrics can provide a quantitative analysis on the impact of various system parameters on PLS performance in RIS-aided SG communications. To that end, our analysis concentrates on evaluating the SOP and ASC as vital PLS metrics to gain a comprehensive understanding of the confidentiality and secrecy aspects of the proposed system model. Specifically, our analysis pertains to the communication between an SM and a neighborhood gateway (NG) in the presence of a passive eavesdropper. To the best of our knowledge, this is the first article that studies the PLS performance of the RIS-aided SG communication system. Therefore, the main contributions of this article can be summarized as follows.

1) We analyze the secrecy performance of the RIS-aided SG communication by taking into account the impact of various system parameters, e.g., the number of reflecting elements in the RIS and the (limited) transmission power in the SM.
2) To that end, we first derive closed-form expressions of the probability density function (PDF) and the cumulative distribution function (CDF) of the received SNR at the NG and an eavesdropper in the considered system model by assuming a perfect channel state information (CSI) of the NG and an imperfect CSI of the eavesdropper at the RIS. Then, we introduce accurate compact analytical

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

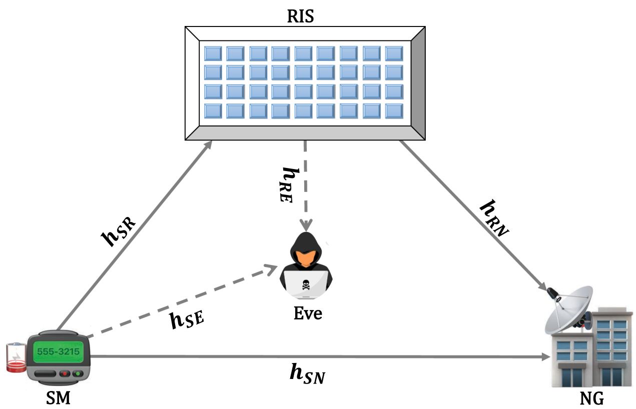


Fig. 1. System model of RIS-aided SG NAN communications.

expressions of SOP and ASC by using the derived PDFs and CDFs.

3) To examine the behavior of the RIS-aided SG communication system in conditions of high SNR and to understand the core patterns and potential of SG communication systems in optimal settings, we conduct an asymptotic analysis of the derived SOP and ASC using the residue method, as described in [44].

4) We validate the analytical results by leveraging the advantage of Monte Carlo simulation in different system settings. Our results confirm the accuracy of the proposed closed-form expressions and show that the RIS-aided SG can achieve better secrecy performance than the conventional SG scenario without the RIS.

C. Organization and Notations

The rest of this article is organized as follows. Section II presents the system and channel model of RIS-aided SG communication. Section III demonstrates the SNR distribution at an NG and an eavesdropper. The closed-form expressions of SOP and ASC are obtained in Section IV. Section V presents the asymptotic analysis of the secrecy metrics. The simulation results are discussed in Section VI. Finally, Section VII concludes this article.

Notations: $\Gamma(.)$ indicates the complete Gamma function [48, eq. (8.31)], $\Gamma(.,.)$ shows the upper Incomplete Gamma function [48, eq. (8.35)], $B(.,.)$ indicates the Beta function [48, eq. (8.38)], $G_{p,q}^{m,n}(.)$ indicates the Meijer G-function [46, eq. (8.2.1.1)], $H_{p,q:p_1,q_1;\ldots;p_r,q_r}^{m,n:m_1,n_1;\ldots;m_r,n_r}(.)$ indicates the bivariate Fox H-function [47], $i=\sqrt{-1}$, and $\vec{X}^{\mathcal{T}}$ indicates the transpose of $\vec{X}$.

II. System and Channel Model

Fig. 1 shows the proposed system model for an RIS-aided SG neighborhood area network (NAN) communications, where an SM, usually as a resource-constrained device, is typically installed at a customer's premise to measure and record the customer's energy usage patterns and send it to a corresponding NG by employing an RIS with M reflecting elements. The NG serves as a central hub for NAN communications, which collects data from SMs and then transmits the data to a utility company for further analysis and control. We assume that there is also a passive eavesdropper named Eve that tries to analyze the transmitted packets in NAN over both a direct link from the SM (SM-to-NG) and reflected links from the RIS (SM-to-RIS-to-NG). Without loss of generality, we assume that the SM knows the CSI of the NG, so the RIS is able to effectively adjust the phase-shifting coefficients of its reflecting elements for maximizing the received SNR at the NG [42]. We also assume that SM, NG, and Eve are equipped with single antenna for simplicity. Therefore, the received signal at NG and Eve can be respectively expressed as

$$y_N=\sqrt{P_s}S(t)\left(h_{SN}+\vec{H}_{SR}\vec{\Theta}\vec{H}_{RN}^{\mathcal{T}}\right)+n_N \tag{1}$$

$$y_E=\sqrt{P_s}S(t)\left(h_{SE}+\vec{H}_{SR}\vec{\Theta}\vec{H}_{RE}^{\mathcal{T}}\right)+n_E \tag{2}$$

where P_s represents the transmit power of the SM, $S(t)$ is the information signal of the SM with a unit power, and n_N and n_E represent the additive white Gaussian noise (AWGN) at NG and Eve with zero mean and variances σ_N^2 and σ_E^2, respectively. $\vec{\Theta}$ is the adjustable phase matrix induced by the reflection of RIS, which is defined as $\vec{\Theta}=\mathrm{diag}([e^{j\theta_1},e^{j\theta_2},\ldots,e^{j\theta_M}])$. The terms h_{SN} and h_{SE} denote the channel coefficients between SM and NG and between SM and Eve, respectively. Besides, $\vec{H}_{SR}$ contains the channel coefficients from the SM to M reflecting elements of the RIS, $\vec{H}_{RN}$ includes the channel coefficients from RIS's M elements to the NG, and $\vec{H}_{RE}$ consists of the channel coefficients from each element of RIS to Eve. The above channel vectors are given as $\vec{H}_{SR}=d_{SR}^{-\chi}.[h_{SR_1}e^{-j\alpha_1},h_{SR_2}e^{-j\alpha_2},\ldots,h_{SR_M}e^{-j\alpha_M}]$, $\vec{H}_{RN}=d_{RN}^{-\chi}.[h_{RN_1}e^{-j\beta_1},h_{RN_2}e^{-j\beta_2},\ldots,h_{RN_M}e^{-j\beta_M}]$, and $\vec{H}_{RE}=d_{RE}^{-\chi}.[h_{RE_1}e^{-j\eta_1},h_{RE_2}e^{-j\eta_2},\ldots,h_{RE_M}e^{-j\eta_M}]$ where d_{SR} denotes the distance between the SM and the RIS, d_{RN} is the distance between the RIS and NG, and d_{RE} defines the distance between the RIS and Eve. The term χ indicates the path-loss exponent. Furthermore, the terms h_{SR_m}, h_{RN_m}, and h_{RE_m}, where $m\in\{1,2,\ldots,M\}$, are the amplitudes of the corresponding channel coefficients, and $e^{-j\alpha_m}$, $e^{-j\beta_m}$, and $e^{-j\eta_m}$ denote the phase of the respective links. We model all the channel fading coefficients as independent Rayleigh distributed, i.e., the channel power gains are exponentially distributed.

III. SNR Distribution

In this section, an analysis is conducted on the SNR at both NG and Eve. The closed-form expressions of PDF and CDF are then obtained based on the received SNR.

A. Main Link

According to (1), the instantaneous SNR at the NG can be given as

$$\gamma_N=\frac{\left|\sqrt{P_s}(h_{SN}+\vec{H}_{SR}\vec{\Theta}\vec{H}_{RN})\right|^2}{n_N}=\frac{P_s}{d_{SN}^{\chi}\sigma_N^2}|h_{SN}|^2$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

$$+\frac{P_s}{d_{SR}^{\chi}d_{RN}^{\chi}\sigma_N^2}\left|\sum_{m=1}^{M}h_{SR_m}h_{RN_m}e^{j(\theta_m-\alpha_m-\beta_m)}\right|^2$$
$$\overset{(a)}{=}\bar{\gamma}_{N_1}|h_{SN}|^2+\bar{\gamma}_{N_2}\left|\sum_{m=1}^{M}h_{SR_m}h_{RN_m}\right|^2 \tag{3}$$

where (a) is derived by assuming the perfect knowledge of the CSI at the RIS that leads to the ideal phase adjusting for maximizing the SNR at the NG. Besides, $\bar{\gamma}_{N_1}$ and $\bar{\gamma}_{N_2}$ are the average SNR at the NG due to the direct link and the RIS-aided links, respectively. According to (3), we can express $\gamma_N=\gamma_{N_1}+\gamma_{N_2}$ Since γ_{N_1} follows Rayleigh distribution, the PDF of γ_{N_1} can be given as

$$f_{\gamma_{N_1}}(\gamma_{N_1})=\frac{e^{-\frac{\gamma_{N_1}}{a_N}}}{\bar{\gamma}_{N_1}a_N} \tag{4}$$

where a_N represents the mean value of γ_{N_1}. According to [39], $f_{\gamma_{N_2}}(\gamma_{N_2})$ is obtained as

$$f_{\gamma_{N_2}}(\gamma_{N_2})=\frac{\gamma_{N_2}^{\frac{c_N}{2}-1}\,e^{-\frac{\sqrt{\gamma_{N_2}}}{d_N}}}{2\bar{\gamma}_{N_2}\Gamma(c_N)d_N^{c_N}} \tag{5}$$

where $c_N=\frac{M\pi^2}{16-\pi^2}$ and $d_N=\frac{\sqrt{\bar{\gamma}_{N_2}}(16-\pi^2)}{4\pi}$. By having the PDF of both the terms of γ_N in (4) and (5), we can then use the moment-generating function (MGF) of γ_{N_1} and γ_{N_2} to obtain the PDF and the CDF of γ_k as

$$f_{\gamma_N}(\gamma_N)=\mathcal{L}^{-1}\left\{M_{\gamma_{N_1}}(s)\,M_{\gamma_{N_2}}(s)\right\} \tag{6}$$
$$F_{\gamma_N}(\gamma_N)=\mathcal{L}^{-1}\left\{\frac{1}{s}\,M_{\gamma_{N_1}}(s)\,M_{\gamma_{N_2}}(s)\right\} \tag{7}$$

where $\mathcal{L}^{-1}$ shows the Laplace inverse and $M_{\gamma_{N_1}}(t)=M_{\gamma_{N_1}}(-s)$ and $M_{\gamma_{N_2}}(t)=M_{\gamma_{N_2}}(-s)$ show the MGF of γ_{N_1} and γ_{N_2}, respectively.

Theorem 1: Assuming that all the channels follow Rayleigh distribution, the PDF and the CDF of γ_N are given by (8) and (9) shown at the bottom of this page, respectively, where

$$\mathscr{F}_N=\frac{\left(\frac{d_Na_N-2}{2a_N}\right)^{-\frac{c_N}{2}}}{2\bar{\gamma}_{N_1}\bar{\gamma}_{N_2}\Gamma(c_N){d_N}^{c_N}a_N}$$

and $\mathcal{F}_N=\frac{1}{2\bar{\gamma}_{N_1}\bar{\gamma}_{N_2}\Gamma(c_N){d_N}^{c_N}}$

$$f_{\gamma_N}(\gamma_N)=\mathscr{F}_Ne^{-\frac{\gamma_k}{a_N}}\left(\Gamma\left(\frac{c_N}{2}\right)-\mathcal{G}_{1,2}^{2,0}\left(\frac{(d_Na_N-2)\gamma_N}{2a_N}\middle|_{0,\,\frac{c_N}{2}}^{1}\right)\right). \tag{8}$$

Proof: The detailed proof for this theorem is presented in Appendix A. □

B. Eavesdropping Link

Similarly, according to (2), the instantaneous SNR at Eve can be obtained as

$$\gamma_E=\frac{\left|\sqrt{P_s}(h_{SE}+\vec{H}_{SR}\vec{\Theta}\vec{H}_{RE})\right|^2}{n_E}=\frac{P_s}{d_{SE}^{\chi}\sigma_E^2}|h_{SE}|^2$$
$$+\frac{P_s}{d_{SR}^{\chi}d_{RE}^{\chi}\sigma_E^2}\left|\sum_{m=1}^{M}h_{SR_m}h_{RE_m}e^{j(\theta_m-\alpha_m-\eta_m)}\right|^2$$
$$=\bar{\gamma}_{E_1}|h_{SE}|^2+\bar{\gamma}_{E_2}\left|\sum_{m=1}^{M}h_{SR_m}h_{RE_m}e^{j(\theta_m-\alpha_m-\eta_m)}\right|^2 \tag{10}$$

where $\bar{\gamma}_{E_1}$ and $\bar{\gamma}_{E_2}$ denote the average SNR at Eve regarding the direct and RIS-aided links, respectively. When RIS element phase shifts are optimally tailored according to the conditions of the legitimate link, the resultant phase distributions for each of the links to Eve ($\vec{H}_{SR}\vec{\Theta}\vec{H}_{RE}^{\mathcal{T}}$) exhibit a uniform distribution [40]. If phase-shift errors uniformly span the range $[-\pi,\pi)$, implying a complete absence of knowledge about CSI of Eve at the RIS and, consequently, a complete lack of knowledge about optimally adjusting the RIS phases according to the Eve's CSI, the channel coefficient adheres to a circularly symmetric complex normal distribution [41]. This resemblance results in the equivalent channel displaying characteristics akin to Rayleigh fading, as has been discussed in [42] and [43]. Therefore, $f_{\gamma_E}(\gamma_E)$ can be represented as

$$f_{\gamma_E}(\gamma_E)=\frac{1}{a_E}\,e^{-\frac{\gamma_E}{a_E}} \tag{11}$$

where $a_E=M\bar{\gamma}_{E_2}+\bar{\gamma}_{E_1}$. Therefore, $F_{\gamma_E}(\gamma_E)$ is obtained as

$$F_{\gamma_E}(\gamma_E)=1-e^{-\frac{\gamma_E}{a_E}}. \tag{12}$$

IV. Secrecy Performance Analysis

In this section, we analyze the secrecy performance of RIS-aided SG communication by deriving closed-form expressions of SOP and ASC. First, we define the secrecy capacity (SC), the maximum rate at which information can be transmitted over the SG communication links between the SM and the NG while keeping the information confidential from the Eve, as

$$\mathrm{SC}(\gamma_N,\gamma_E)=[C_N-C_E]^+ \tag{13}$$

where $C_N=\log(1+\gamma_N)$ and $C_E=\log(1+\gamma_E)$ show the wireless channel capacity between SM and NG, and SM and Eve, respectively, and $[X]^+=\mathrm{Max}\{X,0\}$. Note that $\log(.)$ stands for logarithm in base 2.

$$F_{\gamma_N}(\gamma_N)=\mathcal{F}_N\left(\left(\frac{d_N}{2}\right)^{-\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)-\mathcal{G}_{1,2}^{2,0}\left(\frac{d_N\gamma_N}{2}\middle|_{0,\,\frac{c_N}{2}}^{1}\right)\right)\right.$$
$$\left.-\left(\frac{d_Na_N-2}{2a_N}\right)^{-\frac{c_N}{2}}e^{-\frac{\gamma_N}{a_N}}\left(\Gamma\left(\frac{c_N}{2}\right)-\mathcal{G}_{1,2}^{2,0}\left(\frac{(d_Na_N-2)\gamma_N}{2a_N}\middle|_{0,\,\frac{c_N}{2}}^{1}\right)\right)\right). \tag{9}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

A. Secrecy Outage Probability

Here, we present the analytical expression of SOP for RIS-aided SG NAN communication. As an information-theoretical metric to evaluate the PLS performance, SOP is defined as the probability that SC is less than a certain positive secrecy rate threshold, say R_S, as

$$P_{\text{SOP}} = \Pr(\text{SC} \leq R_S). \tag{14}$$

By applying (13) in SOP definition, a mathematical expression for SOP can be derived as follows:

$$P_{\text{SOP}} = \Pr\left(\log\left(\frac{1+\gamma_N}{1+\gamma_E}\right) \leq R_S\right) = \int_0^\infty F_{\gamma_N}(\gamma_t) f_{\gamma_E}(\gamma_E) d_{\gamma_E} \tag{15}$$

where $\gamma_t = (1+\gamma_E)e^{R_S} - 1 = \gamma_E e^{R_S} + e^{R_S} - 1 = \gamma_E R_t + R'_t$ is the SNR threshold.

Theorem 2: The SOP for the RIS-aided SG communication system under Rayleigh fading channels can be expressed by (16) shown at the bottom of this page.

Proof: The detailed proof for this theorem is presented in Appendix B. □

B. Average Secrecy Capacity

The analytical expression of the ASC is presented in this section for RIS-aided SG NAN communications. ASC is the expected value of the SC over all the possible channel conditions and is a key metric in evaluating the PLS performance. According to (13), since SC for a complex AWGN wiretap channel is defined as the difference between the main and Eve channels when the Eve channel is noisier than the main channel, a mathematical expression for ASC can be derived as follows:

$$\text{ASC} \triangleq \int_0^\infty \int_0^\infty \text{SC}(\gamma_N, \gamma_E) f_{\gamma_N}(\gamma_N) f_{\gamma_E}(\gamma_E) d_{\gamma_E} d_{\gamma_E}. \tag{17}$$

Theorem 3: The ASC for the RIS-aided SG communication system under Rayleigh fading channels can be expressed as

$$\bar{C}_s = \frac{1}{\ln 2}\left(\bar{C}_s^1 + \bar{C}_s^2 - \bar{C}_s^3\right) \tag{18}$$

where $\bar{C}_s^1$, $\bar{C}_s^2$, and $\bar{C}_s^3$ are shown in (19)–(21), respectively

$$\bar{C}_s^3 = \mathcal{G}_{3,2}^{1,3}\left(a_E \middle| \begin{matrix} 0,1,1 \\ 1,0 \end{matrix}\right). \tag{21}$$

Proof: The detailed proof is presented in Appendix C. □

Remark 1: The SOP and the ASC of the considered RIS-aided SG communication system can be accurately obtained according to Theorems 2 and 3, respectively. It becomes evident that c_N acts as a parameter of Fox H-function and as a variable of complete Gamma function in (16), (19), and (20) shown at the bottom of this page; thereby, both SOP and ASC are notably affected by the number of RIS elements, M, since $c_N = \frac{M\pi^2}{16-\pi^2}$. Consequently, as the number of RIS elements M increases, we can expect improved performance in both SOP and ASC. Furthermore, an analysis of a_E in SOP and ASC analytical expressions reveals that increasing a_E results in a greater likelihood of experiencing an outage and a decreased ASC. This observation is attributed to the fact that $a_E = M\bar{\gamma}_{E_2} + \bar{\gamma}_{E_1}$ is a function of average SNRs at Eve. Therefore, a larger a_E indicates a more favorable channel condition for the eavesdropper. On the

$$\begin{aligned} P_{\text{SOP}} = {} & \mathcal{F}_N\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right) + e^{\frac{R'_t}{a_E R_t}}\mathcal{H}_{1,0:1,2;1,1}^{0,1:2,0;0,1}\left(\begin{matrix}\frac{a_E d_N R_t}{2} \\ \frac{a_E R_t}{R'_t}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1);(1,1) \\ -:(0,1),(\frac{c_N}{2},1);(0,1)\end{matrix}\right)\right) \\ & - \mathcal{F}_N\left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}}\left(\frac{2\Gamma\left(\frac{c_N}{2}\right)e^{\frac{-a_N R'_t}{2}}}{2+a_E a_N R_t} + \frac{2e^{\frac{R'_t}{a_E R_t}}}{2+a_E a_N R_t}\mathcal{H}_{1,0:1,2;1,1}^{0,1:2,0;0,1}\left(\begin{matrix}\frac{a_E R_t(d_N a_N - 2)}{a_N(2+a_E a_N R_t)} \\ \frac{2a_E R_t}{R'_t(2+a_E a_N R_t)}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1);(1,1) \\ -:(0,1),(\frac{c_N}{2},1);(0,1)\end{matrix}\right)\right). \end{aligned} \tag{16}$$

$$\begin{aligned} \bar{C}_s^1 = {} & a_N\mathscr{F}_N\left(\Gamma\left(\frac{c_N}{2}\right)\mathcal{G}_{3,2}^{1,3}\left(a_N\middle|\begin{matrix}0,1,1 \\ 1,0\end{matrix}\right) - \mathcal{H}_{1,0:2,2;1,2}^{0,1:1,2;2,0}\left(\begin{matrix}a_N \\ \frac{d_N a_N - 2}{2}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1),(1,1);(1,1) \\ -:(1,1),(0,1);(0,1),(\frac{c_N}{2},1)\end{matrix}\right)\right. \\ & \left. - \frac{a_E}{a_E + a_N}\left(\Gamma\left(\frac{c_N}{2}\right)\mathcal{G}_{3,2}^{1,3}\left(\frac{a_E a_N}{a_E + a_N}\middle|\begin{matrix}0,1,1 \\ 1,0\end{matrix}\right) - \mathcal{H}_{1,0:2,2;1,2}^{0,1:1,2;2,0}\left(\begin{matrix}\frac{a_E a_N}{a_E + a_N} \\ \frac{a_E(d_N a_N - 2)}{2(a_E + a_N)}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1),(1,1);(1,1) \\ -:(1,1),(0,1);(0,1),(\frac{c_N}{2},1)\end{matrix}\right)\right)\right). \end{aligned} \tag{19}$$

$$\begin{aligned} \bar{C}_s^2 = {} & \mathcal{F}_N\left(\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)\mathcal{G}_{3,2}^{1,3}\left(a_E\middle|\begin{matrix}0,1,1 \\ 1,0\end{matrix}\right) - \mathcal{H}_{1,0:2,2;1,2}^{0,1:1,2;2,0}\left(\begin{matrix}a_E \\ \frac{d_N a_E}{2}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1),(1,1);(1,1) \\ -:(1,1),(0,1);(0,1),(\frac{c_N}{2},1)\end{matrix}\right)\right)\right. \\ & - \frac{2a_N}{a_E + 2a_N}\left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)\mathcal{G}_{3,2}^{1,3}\left(\frac{a_E a_N}{a_E + a_N}\middle|\begin{matrix}0,1,1 \\ 1,0\end{matrix}\right)\right. \\ & \left.\left. - \mathcal{H}_{1,0:2,2;1,2}^{0,1:1,2;2,0}\left(\begin{matrix}\frac{a_E a_N}{a_E + a_N} \\ \frac{a_E(d_N a_N - 2)}{2(a_E + a_N)}\end{matrix}\middle|\begin{matrix}(0;1,1):(1,1),(1,1);(1,1) \\ -:(1,1),(0,1);(0,1),(\frac{c_N}{2},1)\end{matrix}\right)\right)\right). \end{aligned} \tag{20}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

other hand, the role of parameters related to the average SNRs at the NG in SOP and ASC analytical expressions shows that the better channel condition at the NG can lead to performance improvements in both SOP and ASC. It is important to note that the average SNRs at both Eve and NG are influenced by various factors, including the SM's transmission power, the noise power at NG and Eve, and the distance of NG and Eve from the SM and the RIS. Consequently, adjusting these parameters directly impacts the SOP and ASC performance. In addition, it is worth noting that within the analytical expression for SOP, we can observe that the SOP performance is contingent on the threshold SNR (denoted by R_t and R'_t) as a function of secrecy rate R_S. Overall, as the numerical results show later, our analysis demonstrates the intricate relationships between various system parameters and the performance of SOP and ASC in the RIS-aided SG communication system. Furthermore, our study highlights the pivotal role of RIS in shaping the overall system performance.

V. Asymptotic Analysis

In this section, given the importance of the secrecy metric performance in the high-SNR regime, we evaluate the asymptotic behavior of both SOP and ASC in RIS-aided SG communication by exploiting the residue approach [44].

A. Asymptotic SOP

Because the exact analytical expression of the SOP in the second and fourth terms of (16) is given in relation to the bivariate Fox H-function, we are able to deduce derive the asymptotic behavior of SOP as the SNR becomes significantly high (specifically, when $\bar{\gamma}_N \to \infty$). This can be achieved through the utilization of the expansion of the bivariate Fox H-function. To accomplish this, it is needed to assess the residues of the corresponding integrands at the nearest poles to the contour. These poles are identified as the minimum pole on the right for cases with large arguments of the Fox H-function and the maximum pole on the left for cases with small arguments. In light of this, the asymptotic SOP can be defined according to the subsequent proposition.

Proposition 1: The asymptotic SOP (i.e., $\bar{\gamma}_N \to \infty$) for the considered RIS-aided SG communication system is given by (22).

Proof: The proof is elaborated in Appendix D. $\square$

B. Asymptotic ASC

Since the exact analytical expression of ASC in second and fourth terms of (19) and (20) is in terms of the bivariate Fox H-function, we can derive the asymptotic behavior of the ASC at the high-SNR regime (i.e., $\bar{\gamma}_N \to \infty$) by using the expansion of the bivariate Fox H-function. To do this, we need to evaluate the residue of the corresponding integrands at the closest poles to the contour, namely, the minimum pole on the right for large Fox H-function arguments and the maximum pole on the left for small ones. In addition, we use the same strategy for the used Meijer G-functions in the first and third terms of (19) and (20). Therefore, the asymptotic ASC can be determined according to the following proposition.

Proposition 2: The asymptotic ASC for the considered RIS-aided SG communication system is given by (23).

Proof: The proof is elaborated in Appendix E. $\square$

Remark 2: By contrasting Theorems 2 and 3 with Propositions 1 and 2, it becomes apparent that the analytical expressions of SOP and ASC that are formulated in terms of the bivariate Fox H-function can be streamlined into Meijer G-function when the system is operating in a high-SNR regime, leveraging the residue method. Similar to the explanation provided in Remark 1, we can readily discern the manner in which various system parameters influence the asymptotic behavior of SOP and ASC under high-SNR conditions. In addition, as shown in numerical findings, it is noteworthy that the asymptotic results in (22) and (23) will gradually approximate the exact SOP and ASC, respectively, with high accuracy as $\bar{\gamma}_N \to \infty$.

$$
\begin{aligned}
P_{\mathrm{SOP}}^{\mathrm{asy}} = \mathcal{F}_N \Bigg(& \left(\frac{2}{d_N}\right)^{\frac{c_N}{2}} \left(\Gamma\left(\frac{c_N}{2}\right) + \frac{R'_t e^{\frac{R'_t}{a_E R_t}}}{a_E R_t} \mathcal{G}_{1,2}^{2,0}\left(\frac{d_N R'_t}{2} \middle| \begin{matrix} 1 \\ \frac{c_N}{2}, -1 \end{matrix} \right) \right) \\
& - \left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}} \left(\frac{2\Gamma\left(\frac{c_N}{2}\right) e^{\frac{-a_N R'_t}{2}}}{2 + a_E a_N R_t} + \frac{R'_t e^{\frac{R'_t}{a_E R_t}}}{a_E R_t} \mathcal{G}_{1,2}^{2,0}\left(\frac{R'_t (a_N d_N - 2)}{2a_N} \middle| \begin{matrix} 1 \\ \frac{c_N}{2}, -1 \end{matrix} \right) \right) \Bigg).
\end{aligned} \tag{22}
$$

$$
\begin{aligned}
\bar{C}_s^{\mathrm{asy}} = & \frac{\mathscr{F}_N a_N^2 \Gamma\left(\frac{c_N}{2}\right)}{\ln 2} \left(1 - \left(\frac{a_E}{a_E + a_N} \right)^2 \right) - \frac{1}{\ln 2} \mathcal{G}_{3,2}^{1,3}\left(a_E \middle| \begin{matrix} 0, 1, 1 \\ 1, 0 \end{matrix} \right) \\
& + \frac{\mathcal{F}_N}{\ln 2} \Bigg(\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}} \left(\Gamma\left(\frac{c_N}{2}\right) a_E - \frac{2}{d_N a_E} \mathcal{G}_{3,2}^{1,3}\left(\frac{2}{d_N} \middle| \begin{matrix} 1, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix} \right) \right) \\
& - \left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}} \left(\Gamma\left(\frac{c_N}{2}\right) \left(\frac{2a_N a_E}{2a_N + a_E} \right)^2 - \frac{2a_N}{a_E (d_N a_N - 2)} \mathcal{G}_{3,2}^{1,3}\left(\frac{2a_N}{d_N a_N - 2} \middle| \begin{matrix} 1, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix} \right) \right) \Bigg).
\end{aligned} \tag{23}
$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

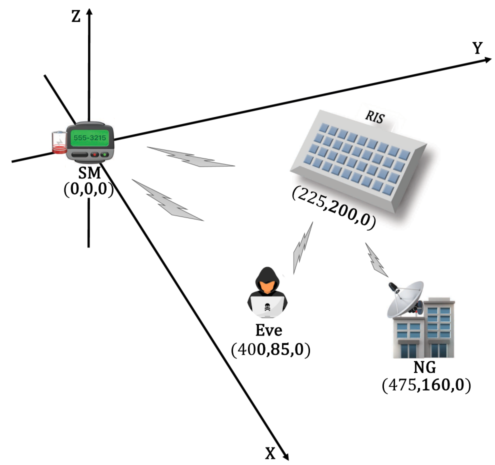


Fig. 2. Simulation setup.

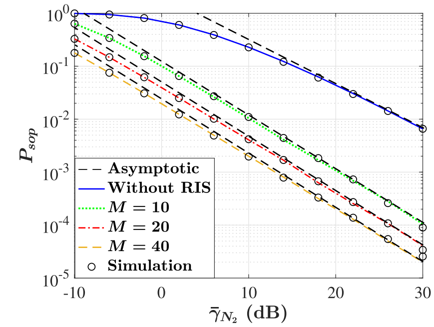


Fig. 3. SOP versus $\bar{\gamma}_{N_2}$ regarding various numbers of RIS elements.

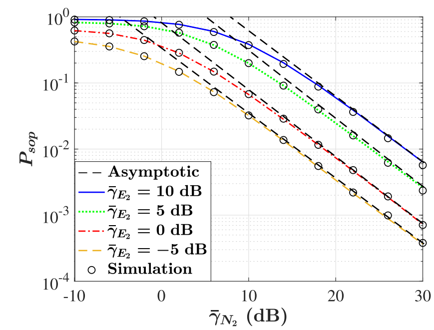


Fig. 4. SOP versus $\bar{\gamma}_{N_2}$ regarding various $\bar{\gamma}_{E_2}$ and $M = 10$.

VI. Analytical and Simulation Results

In this section, we conduct a comprehensive validation of the derived analytical expressions for both the SOP and the ASC through rigorous Monte Carlo simulations. Moreover, we meticulously analyze the influence of various system parameters on the secrecy performance of RIS-assisted SG communications.

A. Simulation Setup

We consider an RIS-aided SG NAN communication, featuring an SM with limited transmission power, a passive eavesdropper, an NG as a legitimate receiver, and an RIS with M reflecting elements. As illustrated in Fig. 2, the SM maintains a fixed location at coordinates (0,0,0), sending its collected private information to the NG. The RIS (with an optimized phase shifting) is located at coordinates (225,200,0) to enhance the connections at the NG, thereby improving the system's secrecy performance. Eve and NG are situated at (400,85,0) and (475,160,0), respectively, positioning the NG farther from the RIS and the SM compared to Eve's distance from these entities. This arrangement, designed to encapsulate the worst case scenario and enable insightful performance analysis, leads to the following fixed distances: $d_{SR} = 300$ m, $d_{SN} = 500$ m, $d_{SE} = 400$ m, $d_{RN} = 250$ m, and $d_{RE} = 200$ m. We consider $R_S = 1$ bps/Hz and model all the relevant channels with independent complex Gaussian random variables, representing Rayleigh fading with a path-loss exponent $\chi = 3.5$. The noise power received at Eve and NG is set as $\sigma_E^2 = -40$ dBm and $\sigma_N^2 = -60$ dBm, respectively. Acknowledging the pragmatic limitation of transmission power for SMs in real-world SG contexts, we set $P_S = 20$ dBm. Notably, while commonly utilized mathematical software tools, such as Mathematica, Maple, and MATLAB, lack inclusion of the extended generalized bivariate Fox H-function, its implementation was successfully achieved through programming functions, as exemplified in [45]. However, for implementing other mathematical functions, such as the Meijer G and Gamma functions, we used the preexisting functions available in MATLAB.

B. Results and Discussions

Fig. 3 demonstrates the behavior of SOP as a function of $\bar{\gamma}_{N_2}$ for different values of RIS elements, M. The findings consistently reveal that as $\bar{\gamma}_{N_2}$ increases while keeping M constant, the SOP decreases. Furthermore, as the number of RIS elements, M, grows, there is a notable reduction in SOP. This improvement in SOP can be attributed to the utilization of the RIS, which enables the establishment of a high-quality communication channel. As a result, there is an enhancement in the SNR at the receiver node NG when the phase-shift matrix of the RIS is appropriately configured. In Fig. 4, the behavior of SOP is depicted in terms of $\bar{\gamma}_{N_2}$ for fixed M and selected values of $\bar{\gamma}_{E_2}$. As $\bar{\gamma}_{N_2}$ increases, we observe a corresponding decrease in SOP, which is reasonable given that the main channel conditions are improving. Moreover, as $\bar{\gamma}_{E_2}$ increases, a higher value of SOP is obtained for a fixed value of $\bar{\gamma}_{N_2}$ since the Eve's channel is experiencing better conditions. Notably, even when the main channel is inferior to the eavesdropper channel (i.e., $\bar{\gamma}_{N_2} < \bar{\gamma}_{E_2}$), SOP is greater than 0.5. This is due to the possibility of achieving a small positive secrecy rate under such conditions. However, in practical SG communication scenarios, the main objective is to achieve the least possible value of SOP for secure communication, which can be attained when $\bar{\gamma}_{N_2} \geq \bar{\gamma}_{E_2}$. Fig. 5 demonstrates the impact of the secrecy rate, R_S, on the performance of SOP for various M. The results indicate that as the secrecy rate increases, the performance of SOP deteriorates to the point, where secure communication is no longer feasible at high rates. Nevertheless, the presence of an RIS with M elements results in a slower attenuation of SOP compared to the scenario where no RIS is

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

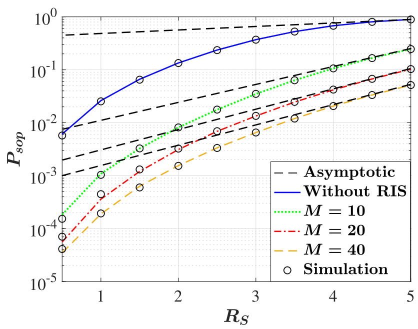


Fig. 5. SOP versus S_R regarding various numbers of RIS elements.

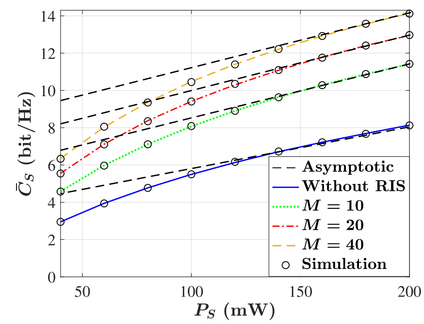


Fig. 8. ASC versus P_S regarding various numbers of RIS elements.

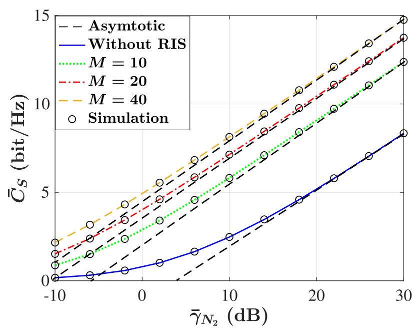


Fig. 6. ASC versus $\bar{\gamma}_{N_2}$ regarding various numbers of RIS elements.

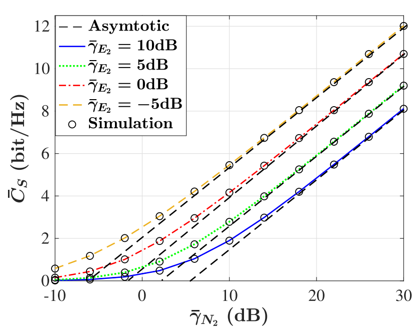


Fig. 7. ASC versus $\bar{\gamma}_{N_2}$ regarding various values of $\bar{\gamma}_{E_2}$ and $M = 4$.

employed. Fig. 6 depicts the performance of ASC as a function of $\bar{\gamma}_{N_2}$ regarding different values M. The results suggest that ASC exhibits a consistent increase as $\bar{\gamma}_{N_2}$ rises for a fixed value of M. Moreover, as the value of M increases, there is a significant boost in ASC. This can be attributed to the utilization of the RIS, which facilitates the provision of a high-quality channel that improves the received SNR at the NG when the phase matrix of the RIS is appropriately adjusted.

Fig. 7 illustrates the performance of ASC as a function of $\bar{\gamma}_{N_2}$ regarding various selected values of $\bar{\gamma}_{E_2}$, while keeping M fixed. As $\bar{\gamma}_{N_2}$ increases, the ASC also increases, which is expected because the main channel conditions improve. Moreover, as $\bar{\gamma}_{E_2}$ increases, the ASC for a fixed $\bar{\gamma}_{N_2}$ decreases. However, it is evident that even if $\bar{\gamma}_{N_2} \leq \bar{\gamma}_{E_2}$, the ASC can still be attained. Fig. 8 demonstrates the performance of ASC as a function of the SM's transmission power, P_S, regarding different values of M. The results indicate that ASC increases as P_S rises for a fixed value of M. Moreover, when the value of M increases, a considerable enhancement in ASC is observed due to gaining a superior channel and higher SNR at the NG by using the RIS. In many practical SG scenarios, increasing the SM's transmission power to improve the communication performance is not a viable option due to regulatory limits, energy consumption constraints, and interference concerns. However, as highlighted by the results, increasing the number of RIS elements offers a notable enhancement in SG communication performance, all while alleviating the burden on SMs to operate at higher transmission power levels. This dual benefit not only leads to improved ASC but also plays a crucial role in extending the battery life of SMs, ensuring their sustained operation at lower transmission power settings. As a result, the utilization of RIS emerges as a practical and effective solution for achieving improved secrecy performance while allowing SMs to operate at lower transmission power levels. In summary, both the analytical and simulation findings demonstrate that the integration of RIS technology into the SG infrastructure yields substantial improvements in PLS, significantly enhancing security and confidentiality. Specifically, employing the RIS with a larger value of M offers greater degrees of freedom for efficient beamforming, significantly improving the secrecy performance in SG communications.

VII. Conclusion

In this article, we explored the transformative potential of integrating RIS into SG communications to enhance the PLS performance. Our study involved the deployment of an RIS alongside key SG components, including SMs, NGs, and potential eavesdroppers, creating a smart environment within the SG infrastructure. Specifically, we evaluated the PLS performance in terms of SOP and ASC. Our analytical approach began by deriving closed-form expressions for the PDF and CDF of the received SNR at both NG and Eve. Then, we derived accurate analytical expressions for SOP and ASC. This allowed us to systematically assess how various system parameters influence the secrecy performance of RIS-aided SG communication system. Furthermore, we conducted an asymptotic analysis under high-SNR conditions, recognizing the significance of understanding system behavior in such regimes. To validate the analytical results and reinforce the robustness of our findings, we performed

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Monte Carlo simulations. The consistency between analytical and simulated results further substantiates the effectiveness of RIS in enhancing the secrecy performance of SG communications compared to SG scenarios without the RIS.

Appendix A
Proof of Theorem 1

We use the definition of the MGF to obtain

$$M_{\gamma_{N_1}}(t)$$

as

$$M_{\gamma_{N_1}}(t) = \int_0^\infty e^{t\gamma_{N_1}} f_{\gamma_{N_1}}(\gamma_{N_1}) d\gamma_{N_1}$$
$$= \frac{1}{\bar{\gamma}_{N_1} a_N} \int_0^\infty e^{\gamma_{N_1}\left(t-\frac{1}{a_N}\right)} d\gamma_{N_1} = \frac{1}{\bar{\gamma}_{N_1}(1-a_N t)}. \tag{24}$$

Thus, we have $M_{\gamma_{N_1}}(s)$ as

$$M_{\gamma_{N_1}}(s) = \frac{1}{\bar{\gamma}_{N_1}(1+a_N s)}. \tag{25}$$

Similar to (24), $M_{\gamma_{N_2}}(t)$ can be obtained as follows:

$$M_{\gamma_{N_2}}(t) = \frac{1}{2\bar{\gamma}_{N_2}\Gamma(c_N)\, d_N^{c_N}} \int_0^\infty e^{\gamma_{N_2}\left(t-\frac{1}{2d_N}\right)} \gamma_{N_2}{}^{\frac{c_N}{2}-1} d\gamma_{N_2}$$
$$= \frac{\Gamma\left(\frac{c_N}{2}\right)}{2\bar{\gamma}_{N_2}\Gamma(c_N) d_N^{c_N}} \left(\frac{d_N}{2} - t\right)^{-\frac{c_N}{2}}. \tag{26}$$

Then, we have $M_{\gamma_{N_2}}(s)$ as

$$M_{\gamma_{N_2}}(s) = \frac{\Gamma\left(\frac{c_N}{2}\right)}{2\bar{\gamma}_{N_2}\Gamma(c_N) d_N^{c_N}} \left(\frac{d_N}{2} + s\right)^{-\frac{c_N}{2}}. \tag{27}$$

By using the Laplace inverse transform in Mathematica, (6) can be obtained as

$$f_{\gamma_N}(\gamma_N) = \mathscr{F}_N e^{-\frac{\gamma_N}{a_N}} \left(\Gamma\left(\frac{c_N}{2}\right) - \Gamma\left(\frac{c_N}{2}, \left(\frac{d_N a_N - 2}{2a_N}\right)\gamma_N\right)\right). \tag{28}$$

Now, by writing the incomplete Gamma function based on the Meijer G-function using [47, eq. (8.4.16.2)], $f_{\gamma_N}(\gamma_N)$ is obtained as (8), and the proof is completed. According to (7) and taking the same steps of computing $f_{\gamma_N}(\gamma_N)$, $F_{\gamma_N}(\gamma_N)$ can be obtained as (29) shown at the bottom of this page. Now, by using [47, eq. (8.4.16.2)], $F_{\gamma_N}(\gamma_N)$ in (29) can be obtained as (9), and the proof is completed.

Appendix B
Proof of Theorem 2

According to the SOP definition in (15) and by having the derived CDF for the received SNR at the NG in (9) and the PDF of the received SNR at Eve in (11), we can rewrite (15) as (30) shown at the bottom of this page. In (30), we can simply obtain $I_1 = a_E$. For computing I_2, we use the integral-form definition of the Meijer G-function. Thus, we have I_2 as (31) shown at the bottom of this page. In order to compute I_2' in (31), we use [48, eq. (3.381.4)]; thus, we have I_2' as

$$I_2' = a_E^{1+\zeta_1} R_t^{\zeta_1} e^{\frac{R_t'}{a_E R_t}} \mathcal{G}_{1,2}^{2,0}\left(\frac{R_t'}{a_E R_t}\middle|\begin{matrix}1\\0, 1+\zeta_1\end{matrix}\right). \tag{32}$$

Now, by putting (32) in (31) and using the integral-form definition of the Meijer G-function, we have I_2 as (33) shown at the bottom of the next page. Since (33) demonstrates the integral-form definition of the bivariate Fox H-function, we can show I_2 as the second term of P_{SOP} in (16). I_3 can also be simply

$$F_{\gamma_N}(\gamma_N) = \mathcal{F}_N \left(\left(\frac{d_N}{2}\right)^{-\frac{c_N}{2}} \left(\Gamma\left(\frac{c_N}{2}\right) - \Gamma\left(\frac{c_N}{2}, \frac{d_N\gamma_N}{2}\right)\right) - \left(\frac{d_N a_N - 2}{2a_N}\right)^{-\frac{c_N}{2}} e^{-\frac{\gamma_N}{a_N}} \left(\Gamma\left(\frac{c_N}{2}\right) - \Gamma\left(\frac{c_N}{2}, \left(\frac{d_N a_N - 2}{2a_N}\right)\gamma_N\right)\right)\right). \tag{29}$$

$$P_{\text{SOP}} = \frac{\mathcal{F}_N}{a_E}\left(\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}} \Gamma\left(\frac{c_N}{2}\right) \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}} d\gamma_E}_{I_1} - \left(\frac{2}{d_N}\right)^{\frac{c_N}{2}} \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}} \mathcal{G}_{1,2}^{2,0}\left(\frac{d_N}{2}(R_t\gamma_E + R_t')\middle|\begin{matrix}1\\0, \frac{c_N}{2}\end{matrix}\right) d\gamma_E}_{I_2}\right.$$
$$\left. - \left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}} \left(\Gamma\left(\frac{c_N}{2}\right) \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}} e^{\frac{-(R_t\gamma_E + R't)}{2a_N}} d\gamma_E}_{I_3} - \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}} e^{\frac{-(R_t\gamma_E + R't)}{2a_N}} \mathcal{G}_{1,2}^{2,0}\left(\frac{(d_N a_N - 2)(R_t\gamma_E + R_t')}{2a_N}\middle|\begin{matrix}1\\0, \frac{c_N}{2}\end{matrix}\right) d\gamma_E}_{I_4}\right)\right). \tag{30}$$

$$I_2 = \frac{1}{2\pi i} \underbrace{\int_0^\infty e^{-\frac{\gamma_E}{a_E}} (R_t\gamma_E + R_t')^{\zeta_1} d\gamma_E}_{I_2'} \oint_{L_1} \frac{\Gamma(-\zeta_1)\Gamma(\frac{c_N}{2} - \zeta_1)\left(\frac{d_N}{2}\right)^{\zeta_1}}{\Gamma(1-\zeta_1)} d\zeta_1. \tag{31}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

obtained as

$$I_3 = \frac{2a_E e^{-\frac{a_N R_t'}{2}}}{2 + a_E a_N R_t}. \tag{34}$$

In order to solve I_4, we take the exactly same steps as we took for computing I_2; thus, I_4 can be obtained as the fourth term of P_{SOP} in (16). Therefore, the SOP expression can be obtained as shown in (16), and the proof is completed.

Appendix C
Proof of Theorem 3

By inserting (13) into (17), ASC can be expressed as (35) shown at the bottom of this page. For completing the proof, we start with J_1. For solving J_1, we use the Meijer G-function demonstration of the logarithm function, as shown in [46, eq. (8.4.6.5)]. By inserting (8) and (12) into J_1 in (35), we can rewrite J_1 as (36) shown at the bottom of this page. J_1^1 and J_1^2 can be computed using [46, eq. (2.24.3.1)] as shown in the first and third terms of (19), respectively. For computing J_1^3, we use the integral-form definition of the Meijer G-function for both the Meijer G-functions in the integral. Thus, we have J_1^3 as (37) shown at the bottom of this page. In order to compute $J_1'^3$, we use [48, eq. (3.381.4)] as

$$J_1'^3 = a_N^{1+\zeta_1+\zeta_2}\,\Gamma(1+\zeta_1+\zeta_2). \tag{38}$$

Now, by putting (38) in (37), we have J_1^3 as (39) shown at the bottom of the next page. Since (39) demonstrates the integral-form definition of the bivariate Fox H-function, we can show J_1^3 as the second term of $\bar{C}_s^1$ in (19). In order to solve J_1^4, we take the exactly same steps as we took for computing J_1^3; thus, J_1^4 can be obtained as the fourth term of $\bar{C}_s^1$ in (19). Therefore, J_1 in (35) can be derived as $\bar{C}_s^1$ shown in (19).

In order to solve J_2, we insert (9) and (11) into J_2 in (35). Therefore, we can rewrite J_2 as (40) shown at the bottom of the next page. For solving J_2^1, J_2^2, J_2^3, and J_2^4 in (40), since we have the same integrals, we can take the exactly same steps that we took for solving J_1^1, J_1^3, J_1^2, and J_1^4, respectively. Therefore, J_2 in (35) can be derived as $\bar{C}_s^2$ shown in (20). In order to solve J_3, we first insert (11) and the Meijer G-function demonstration of the logarithm function into J_3 in (35). Then, we need to solve the following integral:

$$J_3 = \frac{1}{a_E}\int_0^\infty e^{\frac{-\gamma_E}{a_E}}\,\mathcal{G}_{2,2}^{1,2}\left(\gamma_E\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)d\gamma_E \tag{41}$$

which can be computed as $\bar{C}_s^3$, as shown in (21) using [46, eq. (2.24.3.1)]. Now, by inserting the obtained closed-form

$$\begin{aligned} I_2 &= \frac{a_E e^{\frac{R_t'}{a_E R_t}}}{2\pi i}\oint_{L_1}\frac{\Gamma(-\zeta_1)\Gamma(\frac{c_N}{2}-\zeta_1)\left(\frac{a_E d_N R_t}{2}\right)^{\zeta_1}}{\Gamma(1-\zeta_1)}\,\mathcal{G}_{1,2}^{2,0}\left(\frac{R_t'}{a_E R_t}\middle|\begin{matrix}1\\0,1+\zeta_1\end{matrix}\right)d\zeta_1 \\ &= -\frac{a_E e^{\frac{R_t'}{a_E R_t}}}{(2\pi i)^2}\oint_{L_1}\oint_{L_2}\frac{\Gamma(1+\zeta_1+\zeta_2)\Gamma(-\zeta_1)\Gamma(\frac{c_N}{2}-\zeta_1)\left(\frac{a_E d_N R_t}{2}\right)^{\zeta_1}\Gamma(\zeta_2)\left(\frac{a_E R_t}{R_t'}\right)^{\zeta_2}}{\Gamma(1-\zeta_1)\,\Gamma(1+\zeta_2)}d\zeta_2 d\zeta_1. \end{aligned} \tag{33}$$

$$\bar{C}_s = \underbrace{\int_0^\infty \log(1+\gamma_N)f_{\gamma_N}(\gamma_N)F_{\gamma_E}(\gamma_N)d\gamma_N}_{J_1} + \underbrace{\int_0^\infty \log(1+\gamma_E)f_{\gamma_E}(\gamma_E)F_{\gamma_N}(\gamma_E)d\gamma_E}_{J_2} - \underbrace{\int_0^\infty \log(1+\gamma_E)f_{\gamma_E}(\gamma_E)d\gamma_E}_{J_3}. \tag{35}$$

$$\begin{aligned} J_1 = \frac{\mathcal{F}_N}{\ln 2}\Bigg(\Gamma\left(\frac{c_N}{2}\right)\Bigg(&\underbrace{\int_0^\infty e^{\frac{-\gamma_N}{a_N}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_N\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)d\gamma_N}_{J_1^1} - \underbrace{\int_0^\infty e^{\frac{-\gamma_N}{a_N}}e^{\frac{-\gamma_N}{a_E}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_N\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)d\gamma_N}_{J_1^2}\Bigg) \\ &-\underbrace{\int_0^\infty e^{\frac{-\gamma_N}{a_N}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_N\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathcal{G}_{1,2}^{2,0}\left(\frac{(d_N a_N-2)\gamma_N}{2a_N}\middle|\begin{matrix}1\\0,\frac{c_N}{2}\end{matrix}\right)d\gamma_N}_{J_1^3} - \underbrace{\int_0^\infty e^{\frac{-\gamma_N}{a_N}}e^{\frac{-\gamma_N}{a_E}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_N\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathcal{G}_{1,2}^{2,0}\left(\frac{(d_N a_N-2)\gamma_N}{2a_N}\middle|\begin{matrix}1\\0,\frac{c_N}{2}\end{matrix}\right)d\gamma_N}_{J_1^4}\Bigg). \end{aligned} \tag{36}$$

$$J_1^3 = \frac{1}{(2\pi i)^2}\underbrace{\int_0^\infty {\gamma_N}^{\zeta_1+\zeta_2}e^{-\frac{\gamma_N}{a_N}}d\gamma_N}_{J_1'^3}\oint_{L_1}\oint_{L_2}\frac{\Gamma^2(\zeta_1)\Gamma(1-\zeta_1)\Gamma(-\zeta_2)\Gamma\left(\frac{c_N}{2}-\zeta_2\right)\left(\frac{a_N d_N-2}{2a_N}\right)^{\zeta_2}}{\Gamma(1+\zeta_1)\Gamma(1-\zeta_2)}d\zeta_2 d\zeta_1. \tag{37}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

expression of J_1, J_2, and J_3 into (35), the proof for ASC is completed.

Appendix D
Proof of Proposition 1

In the case of $\bar{\gamma}_N \to \infty$, the integral-form demonstration of bivariate Fox H-function in (33) is assessed at the highest poles situated to the left of L_2, which is when $\zeta_2 = -1-\zeta_1$. As a result, we arrive at the integral presented in (42) pertaining to counter L_2

$$\mathcal{R}_1 = \frac{1}{2\pi j}\oint_{L_2} \Gamma\left(1+\zeta_1+\zeta_2\right) \underbrace{\frac{\Gamma\left(\zeta_2\right)\left(\frac{a_E R_t}{R_t'}\right)^{\zeta_2}}{\Gamma\left(1+\zeta_2\right)}}_{\chi_1(\zeta_2)} d\zeta_2. \tag{42}$$

Since $\mathcal{R}_1 = \mathrm{Res}[\chi_1(\zeta_2), -1-\zeta_1]$, we can rewrite (42) as

$$\begin{aligned}\mathcal{R}_1 &= \lim_{\zeta_2\to -1-\zeta_1}\left(1+\zeta_1+\zeta_2\right)\chi_1(\zeta_2)\\ &= \frac{\Gamma\left(-1-\zeta_1\right)\left(\frac{a_E R_t}{R_t'}\right)^{-1-\zeta_1}}{\Gamma\left(-\zeta_1\right)}.\end{aligned} \tag{43}$$

Now, by inserting (43) into (33), the asymptotic I_2 can be obtained as follows:

$$I_2^{\text{asy}} = \frac{R_t'}{a_E R_t 2\pi i}\oint_{L_1}\frac{\Gamma(\frac{c_N}{2}-\zeta_1)\Gamma(-1-\zeta_1)\left(\frac{d_N R_t'}{2}\right)^{\zeta_1}}{\Gamma\left(1-\zeta_1\right)}d\zeta_1. \tag{44}$$

Now, based on the definition of the Meijer G-function, (44) can be shown as the second term of (22). Similarly, we can assess the bivariate Fox H-function in the fourth term of (16) the highest poles situated to the left of L_2, which is when $\zeta_2 = -1-\zeta_1$. By taking the exactly same steps, the asymptotic I_4 can be obtained in the form of a Meijer G-function, as shown in the fourth term of (22). As a result, the proof will be completed for asymptotic SOP.

Appendix E
Proof of Proposition 2

In the case of $\bar{\gamma}_N \to \infty$, the asymptotic ASC can be expressed as

$$\bar{C}_{\text{s}}^{\text{asy}} = \bar{C}_s^{1,\text{asy}} + \bar{C}_s^{2,\text{asy}} - J_3. \tag{45}$$

In order to compute $\bar{C}_s^{1,\text{asy}}$, we can see that the Meijer G-function in the first term of (19) is evaluated at the highest poles on the left of L_2, i.e., $\zeta_1 = 1$, in its integral-form demonstration as follows:

$$\mathcal{R}_2 = \frac{1}{2\pi i}\oint_{L_1}\Gamma(1-\zeta_1)\underbrace{\Gamma^2(\zeta_1)a_N^{\zeta_1}}_{\chi_1(\zeta_1)}d\zeta_1. \tag{46}$$

Since $\mathcal{R}_2 = \mathrm{Res}[\chi_1(\zeta_1), 1]$, we can rewrite (46) as

$$\mathcal{R}_2 = \lim_{\zeta_1\to 1}\left(1-\zeta_1\right)\chi_1(\zeta_1) = a_N. \tag{47}$$

Following the same strategy, we can obtain the asymptotic expression of the other Meijer G-function in $\bar{C}_s^1$ [third term of (19)] as

$$\mathcal{R}_3 = \frac{a_E a_N}{a_E + a_N}. \tag{48}$$

Furthermore, the bivariate Fox H-function in $\bar{C}_s^1$ [the second term of (19)], as shown in (39), is evaluated at the highest poles on the left of L_2, which is when $\zeta_2 = -1-\zeta_1$. Thus, we have the following integral for the counter L_2:

$$\begin{aligned}\mathcal{R}_4 = {}& \frac{1}{2\pi j}\oint_{L_2}\Gamma\left(1+\zeta_1+\zeta_2\right)\\ &\times \underbrace{\frac{\Gamma\left(-\zeta_2\right)\Gamma\left(\frac{c_N}{2}-\zeta_2\right)\left(\frac{a_N d_N - 2}{2}\right)^{\zeta_2}}{\Gamma\left(1-\zeta_2\right)}}_{\chi_2(\zeta_2)}d\zeta_2.\end{aligned} \tag{49}$$

$$J_1^3 = \frac{a_N}{(2\pi i)^2}\oint_{L_1}\oint_{L_2}\frac{\Gamma(1+\zeta_1+\zeta_2)\Gamma^2(\zeta_1)\Gamma(1-\zeta_1)a_N^{\zeta_1}\Gamma\left(-\zeta_2\right)\Gamma\left(\frac{c_N}{2}-\zeta_2\right)\left(\frac{a_N d_N-2}{2}\right)^{\zeta_2}}{\Gamma\left(1+\zeta_1\right)\Gamma\left(1-\zeta_2\right)}d\zeta_2 d\zeta_1. \tag{39}$$

$$\begin{aligned}J_2 = {}& \frac{\mathcal{F}_N}{a_E \ln 2}\left(\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)\underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_E\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)d\gamma_E}_{J_2^1} - \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_E\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathcal{G}_{1,2}^{2,0}\left(\frac{d_N\gamma_E}{2}\middle|\begin{matrix}1\\0,\frac{c_N}{2}\end{matrix}\right)d\gamma_E}_{J_2^2}\right)\right.\\ &- \left(\frac{2a_N}{a_N d_N - 2}\right)^{\frac{c_N}{2}}\\ &\left.\times\left(\Gamma\left(\frac{c_N}{2}\right)\underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}}e^{\frac{-\gamma_E}{2a_N}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_E\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)d\gamma_E}_{J_2^3} - \underbrace{\int_0^\infty e^{\frac{-\gamma_E}{a_E}}e^{\frac{-\gamma_E}{2a_N}}\mathcal{G}_{2,2}^{1,2}\left(\gamma_E\middle|\begin{matrix}1,1\\1,0\end{matrix}\right)\mathcal{G}_{1,2}^{2,0}\left(\frac{(d_N a_N-2)\gamma_E}{2a_N}\middle|\begin{matrix}1\\0,\frac{c_N}{2}\end{matrix}\right)d\gamma_E}_{J_2^4}\right)\right).\end{aligned} \tag{40}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

$$J_1^{3,\text{asy}} = \frac{1}{(a_N d_N - 2)\pi i} \oint_{L_1} \frac{\Gamma(1-\zeta_1)\Gamma^2(\zeta_1)\Gamma\left(1+\frac{c_N}{2}+\zeta_1\right)\left(\frac{2a_N}{a_N d_N - 2}\right)^{\zeta_1}}{\Gamma(2+\zeta_1)} d\zeta_1 = \frac{2}{a_N d_N - 2} \mathcal{G}_{3,2}^{1,3}\left(\frac{2a_N}{a_N d_N - 2}\middle| \begin{matrix} 0, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix}\right). \tag{51}$$

$$\bar{C}_s^{2,\text{asy}} = \frac{\mathcal{F}_N}{\ln 2}\left(\left(\frac{2}{d_N}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)a_E - \frac{2}{d_N a_E}\mathcal{G}_{3,2}^{1,3}\left(\frac{2}{d_N}\middle| \begin{matrix} 1, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix}\right)\right)\right.$$
$$\left. - \left(\frac{2a_N}{d_N a_N - 2}\right)^{\frac{c_N}{2}}\left(\Gamma\left(\frac{c_N}{2}\right)\left(\frac{2a_N a_E}{2a_N + a_E}\right)^2 - \frac{2a_N}{a_E(d_N a_N - 2)}\mathcal{G}_{3,2}^{1,3}\left(\frac{2a_N}{d_N a_N - 2}\middle| \begin{matrix} 1, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix}\right)\right)\right). \tag{54}$$

Since $\mathcal{R}_4 = \text{Res}[\chi_2(\zeta_2), -1-\zeta_1]$, we can rewrite (49) as

$$\mathcal{R}_4 = \lim_{\zeta_2 \to -1-\zeta_1} (1+\zeta_1+\zeta_2)\chi_2(\zeta_2) = \frac{\Gamma(1+\zeta_1)\Gamma\left(1+\frac{c_N}{2}+\zeta_1\right)\left(\frac{a_N d_N - 2}{2}\right)^{-1-\zeta_1}}{\Gamma(2+\zeta_1)}. \tag{50}$$

Now, by inserting (50) into (39), $J_1^{3,\text{asy}}$ can be determined as (51) shown at the top of this page. Similarly, the other bivariate Fox H-function in $\bar{C}_s^1$ [the fourth term of (19)] can also be evaluated at the highest poles on the left of L_2, which is when $\zeta_2 = -1-\zeta_1$. Thus, by taking the exactly same steps, $J_1^{4,\text{asy}}$ can be obtained as

$$J_1^{4,\text{asy}} = \frac{2(a_E + a_N)}{a_E(a_N d_N - 2)}\mathcal{G}_{3,2}^{1,3}\left(\frac{2a_N}{a_N d_N - 2}\middle| \begin{matrix} 0, 1, -\frac{c_N}{2} \\ 1, -1 \end{matrix}\right). \tag{52}$$

Now, by inserting (47), (48), (51), and (52) into their corresponding Meijer G and bivariate Fox H-functions in (19), $\bar{C}_s^{1,\text{asy}}$ is obtained as

$$\bar{C}_s^{\text{asy}} = \frac{\mathscr{F}_N a_N^2 \Gamma\left(\frac{c_N}{2}\right)}{\ln 2}\left(1 - \left(\frac{a_E}{a_E + a_N}\right)^2\right). \tag{53}$$

Similarly, and by taking the exactly same steps for $\bar{C}_s^2$, $\bar{C}_s^{2,\text{asy}}$ can be obtained as (54) shown at the top of this page. Finally, by plugging (41), (53), and (54) into (45), (23) is obtained, and the proof is completed for the asymptotic ASC.

References

[1] R. Zamani, M. P. Moghaddam, and M. R. Haghifam, "Evaluating the impact of connectivity on transactive energy in smart grid," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2491–2494, May 2022.

[2] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 3, pp. 2886–2927, Third Quarter 2019.

[3] D. An, F. Zhang, F. Cui, and Q. Yang, "Toward data integrity attacks against distributed dynamic state estimation in smart grid," *IEEE Trans. Autom. Sci. Eng.*, early access, Jan. 17, 2023, doi: 10.1109/TASE.2023.3236102.

[4] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.

[5] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[6] E. K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, Aug. 2012.

[7] H. Sharma, N. Kumar, and B. K. Panigrahi, "Physical layer security of ami data transmission in smart grid environment," in *Proc. IEEE Global Workshops*, 2019, pp. 1–6.

[8] F. R. Ghadi and G. A. Hodtani, "Copula-based analysis of physical layer security performances over correlated Rayleigh fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 12, pp. 431–440, Dec. 2020.

[9] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng, and Y. Yang, "Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 948–964, 2023.

[10] P. Wang, Z. Yan, and K. Zeng, "BCAuth: Physical layer enhanced authentication and attack tracing for backscatter communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 2818–2834, 2022.

[11] F. R. Ghadi, F. J. López-Martínez, W. P. Zhu, and J. M. Gorce, "The impact of side information on physical layer security under correlated fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 3626–3636, 2022.

[12] K. N. Le, "Impact of fading correlation and finite-blocklength regimes on secrecy," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 4068–4072, Mar. 2023.

[13] S. Thakur and A. Singh, "Secrecy performance of underlay cognitive radio networks with primary interference," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 4, pp. 2641–2657, Jul./Aug. 2022.

[14] H. S. Khallaf, S. Hashima, M. Rihan, E. M. Mohamed, and H. M. Kasem, "Quantifying impact of pointing errors on secrecy performance of UAV-based relay assisted FSO links," *IEEE Internet Things J.*, early access, Jul. 21, 2023, doi: 10.1109/JIOT.2023.3297857.

[15] A. Camponogara, H. V. Poor, and M. V. Ribeiro, "The complete and incomplete low-bit-rate hybrid PLC/wireless channel models: Physical layer security analyses," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2760–2769, Apr. 2019.

[16] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, 2016, pp. 185–189.

[17] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13909–13921, 2017.

[18] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "Secure transmission in smart grid dynamic wide area network by exploiting full-duplex jamming scheme," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 1, 2023, Art. no. e4657.

[19] M. Atallah, M. S. Alam, and G. Kaddoum, "Secrecy analysis of wireless sensor network in smart grid with destination assisted jamming," *IET Commun.*, vol. 13, no. 12, pp. 1748–1752, 2019.

[20] A. El-Shafie, D. Niyato, R. Hamila, and N. Al-Dhahir, "Impact of the wireless network's PHY security and reliability on demand-side management cost in the smart grid," *IEEE Access*, vol. 5, pp. 5678–5689, 2017.

[21] V. Mohan, A. Mathur, V. Aishwarya, and S. Bhargav, "Secrecy analysis of PLC system with channel gain and impulsive noise," in *IEEE 90th Veh. Technol. Conf.*, 2019, pp. 1–6.

[22] 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.

[23] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

[24] M. A. ElMossallamy, H. Zhang, L. Song, K. G. Seddik, Z. Han, and G. Y. Li, "Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 3, pp. 990–1002, Sep. 2020.

[25] R. Ghazalian, K. Keykhosravi, H. Chen, H. Wymeersch, and R. Jäntti, "Bi-static sensing for near-field RIS localization," in *Proc. IEEE Glob. Commun. Conf.*, 2022, pp. 6457–6462.

[26] Z. Tang, T. Hou, Y. Liu, J. Zhang, and C. Zhong, "A novel design of RIS for enhancing the physical layer security for RIS-aided NOMA networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2398–2401, Nov. 2021.

[27] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3480–3495, 2021.

[28] X. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, and P. H. Ho, "Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions," *IEEE Syst. J.*, vol. 17, no. 1, pp. 848–859, Mar. 2023.

[29] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, and F. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451–4463, May 2021.

[30] 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.

[31] Y. Wang, H. Lu, D. Zhao, Y. Deng, and A. Nallanathan, "Wireless communication in the presence of illegal reconfigurable intelligent surface: Signal leakage and interference attack," *IEEE Wireless Commun.*, vol. 29, no. 3, pp. 131–138, Jun. 2022.

[32] F. Chen, H. Lu, Y. Wang, and C. Zhang, "Secure mmWave MIMO communication against signal leakage when meeting illegal reconfigurable intelligent surface," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2023, pp. 1–6.

[33] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Exploiting RIS for limiting information leakage to active eavesdropper in cell-free massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 443–447, Mar. 2022.

[34] S. Kisseleff, W. A. Martins, H. Al-Hraishawi, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1781–1797, 2020.

[35] A. K. Padhan, H. K. Sahu, P. R. Sahu, and S. R. Samantaray, "RIS assisted dual-hop mixed PLC/RF for smart grid applications," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3523–3527, Nov. 2021.

[36] A. K. Padhan, H. K. Sahu, P. R. Sahu, and S. R. Samantaray, "Performance analysis of smart grid wide area network with RIS assisted three hop system," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 9, pp. 48–59, 2023.

[37] A. K. Padhan, P. R. Sahu, and S. R. Samantaray, "Performance analysis of RIS assisted smart grid HEMS using RQAM modulation," in *Proc. IEEE Nat. Conf. Commun.*, 2021, pp. 1–6.

[38] A. Sikri, B. Selim, G. Kaddoum, M. Au, and B. L. Agba, "RIS-aided wireless sensor network in the presence of impulsive noise and interferers for smart-grid communications," *IEEE Commun. Lett.*, vol. 27, no. 9,, pp. 2501–2505, Sep. 2023.

[39] Y. Ai, A. P. Felipe, 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.

[40] J. D. V. Sánchez, P. R. Espinosa, and F. J. L. Martínez, "Physical layer security of large reflecting surface aided communications with phase errors," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 325–329, Feb. 2021.

[41] M. A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 184–188, Feb. 2020.

[42] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12296–12300, Oct. 2020.

[43] 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.

[44] H. Chergui, M. Benjillali, and S. Saoudi, "Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and Rayleigh dual-hop channel," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 610–613, Mar. 2016.

[45] K. P. Peppas, "A new formula for the average bit error probability of dual-hop amplify-and-forward relaying systems over generalized shadowed fading channels," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 85–88, Apr. 2012.

[46] A. P. Prudnikov, I. A. Brychkov, J. A. Bryäkov, and O. I. Marichev, *Integrals and Series: More Special Functions*, vol. 3. Boca Raton, FL, USA: CRC Press, 1986.

[47] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. New York, NY, USA: Springer, 2009.

[48] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.

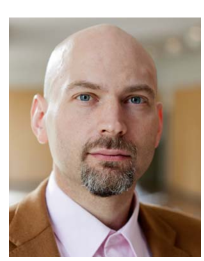
Masoud Kaveh received the Ph.D. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2021.

In 2020, he was a Visiting Scholar with the Technical University of Madrid, Madrid, Spain, under the Erasmus+Program of the European Union. He is currently a Postdoctoral Researcher with Aalto University, Espoo, Finland. His research interests include physical layer security, physical unclonable functions, applied cryptography, smart grid security, backscatter communication, field-programmable gate array design, cryptographic protocols, and machine learning.

Zheng Yan (Senior Member, IEEE) received the D.Sc. degree in technology from the Helsinki University of Technology, Espoo, Finland, in 2007.

She is currently a Full Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. Her research interests include trust, security, privacy, and security-related data analytics.

Dr. Yan is an Area Editor or an Associate Editor for *ACM Computing Surveys*, IEEE INTERNET OF THINGS JOURNAL, *Information Fusion*, IEEE NETWORK, and *Information Sciences*. She was a General Chair or Program Chair of numerous international conferences, including 2015 IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 2021 IFIP Networking Conference. She is a Founding Steering Committee Co-Chair of IEEE Blockchain Conference. She is the recipient of the IEEE TCSC Award for Excellence in Scalable Computing (Woman), the 2021 NÇWomen: Stars in Computer Networking and Communications, the Nokia Distinguished Inventor Award, the Best Journal Paper Award issued by the IEEE Communication Society Technical Committee on Big Data, and the Outstanding Associate Editor of 2017 and 2018 for IEEE ACCESS. She is a world top 2% scientist and a highly cited Chinese researcher.



Riku Jäntti (Senior Member, IEEE) received the M.Sc. (with distinction) degree in electrical engineering and the D.Sc. (with distinction) degree in automation and systems technology from the Helsinki University of Technology, Espoo, Finland, in 1997 and 2001, respectively.

He is currently a Full Professor of Communications Engineering with the School of Electrical Engineering, Aalto University, Espoo. Prior to joining Aalto University in August 2006, he was a Professor Pro Tem with the Department of Computer Science, University of Vaasa, Vaasa, Finland. His research interests include machine-type communications, disaggregated radio access networks, backscatter communications, quantum communications, and radio frequency inference.

Dr. Jäntti is a Member of the Editorial Board of IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He is also a Distinguished Lecturer (Class 2016) of the IEEE Vehicular Technology Society.