IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 October 2023, accepted 4 November 2023, date of publication 8 November 2023,
date of current version 17 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3331593

RESEARCH ARTICLE

Enhancing Physical Layer Secrecy Performance for RIS-Assisted RF-FSO Mixed Wireless System

TAHMID AHMED[1], A. S. M. BADRUDDUZA[1], (Member, IEEE), S. M. RIAZUL ISLAM[2], (Senior Member, IEEE), SHEIKH HABIBUL ISLAM[3], MD. IBRAHIM[4], (Graduate Student Member, IEEE), M. ABDULLAH-AL-WADUD[5], (Member, IEEE), AND IMRAN SHAFIQUE ANSARI[6], (Senior Member, IEEE)

[1]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering & Technology (RUET), Rajshahi 6204, Bangladesh
[2]School of Natural and Computing Sciences, University of Aberdeen, AB24 3FX Aberdeen, U.K.
[3]Department of Electrical and Computer Engineering, University of Massachusetts Lowell, Lowell, MA 01854, USA
[4]Institute of ICT, RUET, Rajshahi 6204, Bangladesh
[5]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[6]James Watt School of Engineering, University of Glasgow, G12 8QQ Glasgow, U.K.

Corresponding author: S. M. Riazul Islam (riazul.islam@abdn.ac.uk)

This work was supported by the Researchers Supporting Project number (RSPD2023R951), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT The reconfigurable intelligent surface (RIS) is widely recognized as an effective solution for enhancing security in wireless communications, owing to its passive reflective components and the ability to adjust signal phases. In light of this, this study investigates the physical layer security issues for a dual-hop RIS-aided system that makes use of both radio frequency (RF) and free space optical (FSO) connections, while taking into account three different eavesdropping scenarios: i) RF eavesdropping, ii) FSO eavesdropping, and iii) simultaneous RF and FSO eavesdropping. While Nakagami-*m* distributed fading affects the RF link, Málaga turbulence with pointing error affects the FSO link. The main goal of this research is to guarantee the confidentiality of information, preventing unauthorized access or disclosure. To this end, closed-form expressions are developed for the average secrecy capacity, secrecy outage probability, probability of strictly positive secrecy capacity, and effective secrecy throughput. Monte Carlo simulations are used to verify the precision of these expressions. To further explore the suggested model, the asymptotic formulations of various performance metrics are produced. The impact of different factors, such as fading severity, atmospheric conditions, and detection techniques, on the secrecy performance is analyzed through simulations. Numerical results highlight the significant role of the proposed model in ensuring the security of confidential information and emphasize the substantial impact of key factors on its secrecy performance.

INDEX TERMS Reconfigurable intelligent surface, dual-hop system, effective secrecy throughput, secrecy outage probability.

I. INTRODUCTION

A. BACKGROUND AND RELATED WORKS

Over the past few years, there has been a remarkable surge in wireless connectivity as well as mobile data traffic, which is likely to be sustained with the introduction of sixth-generation (6G) wireless communication networks [1], [2], [3]. These networks are anticipated to offer efficient and reliable wireless communication services to a vast number of devices [4]. However, the necessity for high data rates, reliability, and wide connection has created substantial challenges in the design of wireless systems, driving the investigation of novel physical layer technologies. Among these technologies, reconfigurable intelligent surfaces (RIS) have been established as an emerging solution to address the energy and spectrum efficiency limitations of current wireless networks [5]. The main idea underlying RIS is to alter wireless communication settings by intelligently

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

adjusting the phase shifts and amplitude of incident signals through reflection using multiple passive reflecting elements, such as low-cost printed dipoles [6]. In comparison to conventional wireless networks, the integration of RIS into wireless networks has the potential to offer a better level of flexibility and compatibility [7]. Therefore, RIS has gained significant attention from researchers and has become a focal point in wireless communication research.

Due to its appealing benefits, RIS technology has garnered a lot of interest from the academic and industrial sectors. For instance, [8], [9] the authors considered various system parameters, including the number of RIS elements, the distance between RIS and the receiver, and the phase shift and amplitude response of RIS, to provide a thorough analysis of the performance of RIS-aided systems. Another study in [10] obtained the analytical expressions of outage probability (OP) and demonstrated multi multi-RIS-aided systems can significantly enhance wireless communication system performance by increasing coverage, reducing the outage probability, and boosting the average SNR. In [11], by assuming Nakagami-*m* fading channels, the closed-form formulas of OP and bit error rate (BER) for the RIS-aided network were determined. The authors of [12] showed that incorporating statistical channel state information into RIS-assisted systems can significantly improve system performance. Moreover, the proposed optimization scheme demonstrates a higher capacity and lower OP than the existing schemes. In [13], the effect of co-channel interference on a wireless network supported by RIS was measured by the authors. Here, the authors compared the proposed model with other existing schemes, and the results indicated that the suggested scheme performs better than them in terms of the BER and OP. The researchers in [14] studied how RIS-assisted wireless communications perform in indoor and outdoor scenarios and found that indoor communication yields better outcomes because fewer obstacles scatter the signal compared to outdoor. Recent wireless systems have introduced the idea of RIS technology in non-orthogonal multiple-access wireless networks in [15], [16], and [17]. In a recent study [18], the authors assessed the impact of RIS on underwater optical communication, noting that an increased number of RIS elements positively contributes to system performance.

Dual-hop systems have been introduced as a potential architecture to integrate emerging wireless networks and extend the coverage area [19]. Several research papers have analyzed the performance of dual-hop networks [20], [21], [22], [23], but very few have taken into account the use of RIS technology in mixed dual-hop systems [24], [25], [26], [27]. The article [24] examined the performance of a combined radio frequency (RF)-free space optical (FSO) network and found that incorporating RIS technology in such a network can result in a significant improvement in performance, with potential practical implications. Another study, [25], studied the effects of different system characteristics including pointing errors and atmospheric turbulence conditions using an RIS in a hybrid FSO and RF communication system, providing essential insights into how these factors affect system performance. Additionally, [26] has performed a thorough investigation of how a RIS might affect the RF and underwater optical wireless communication (UOWC) paradigm. By concurrently optimizing the transmit power and the phase shifts of the RIS components in [27], a new technique for enhancing the functionality of hybrid RF-FSO communication systems was studied. The authors concluded that this optimization approach is a practical and effective solution for improving the system coverage and capacity. In [28], the authors examined the application of the signal space diversity (SSD) technique to enhance system performance. They showed that the implementation of the SSD technique leads to increased spectral efficiency within RF-FSO mixed systems. Therefore, a study in [29] scrutinized a full-duplex (FD) relaying-based RF-FSO mixed system, revealing substantial performance enhancements achieved through the utilization of parallel RF/FSO links within an FD relaying channel. In [30], it was demonstrated that the RIS-aided mixed downlink system clearly performs better than the hybrid downlink system without RIS.

The inherent broadcast nature of wireless networks provides wide coverage but also poses a risk of eavesdropping by unauthorized users [31], which has raised significant concerns regarding privacy and security in RIS-aided networks [32]. To address this issue, cryptographic protocols such as the advanced encryption standard have traditionally been employed at the upper layers. However, with the growing computational power of potential eavesdroppers, the effectiveness of cryptographic protocols is becoming increasingly uncertain. In order to improve the secured transmission of wireless communications, physical layer security (PLS) has been established, using an information-theoretic approach in conjunction with upper-layer cryptographic protocols [33]. In recent times, extensive research has been conducted exploring the security capabilities of RIS-aided wireless systems. A new model for the RIS-assisted system has been proposed at the work of [34] and the performance in terms of secrecy of the system is analyzed using two important metrics: average secrecy capacity (ASC) and secrecy outage probability (SOP). While [35] demonstrated that the RIS-aided communication model can be a successful solution to mitigate the impact of randomly flying eavesdroppers and the secrecy performance of wireless systems can be improved, [36] propose that using a small number of quantization levels can optimize the system performance and energy consumption, thereby achieving a good balance between the two factors. In [37], the authors derived the SOP in closed form and presented a general framework of RIS-assisted vehicular wireless networks that can enhance the system's secrecy performance. The PLS for NOMA systems were introduced in [38], [39], [40], and [41] where the authors revealed that implementing a RIS between

the source and the receiver can lead to a considerable improvement in secrecy performance. On the other hand, assuming multiple interferes towards the destination, the effects of eavesdroppers on system performance are evaluated in [42]. Hence, in [43], the authors examined a RIS-assisted multi-user system, demonstrating the pivotal influence of atmospheric conditions and fading parameters in increasing secrecy performance.

B. MOTIVATION AND CONTRIBUTIONS

Since new wireless networks emerged, the physical properties of the wireless medium in order to design secure systems have been increasingly focused on by researchers. Based on the studies mentioned, the current literature mainly focuses on utilizing a single-hop RIS-assisted configuration and almost all previous research has used the Gamma-Gamma distribution in the FSO path, which is only suitable for certain aperture sizes. While extensive research has been conducted on PLS analysis in RIS-assisted wireless networks [34], [35], [36], [37], [38], [39], [40], the majority of studies have predominantly concentrated on single-hop wireless systems. Different from the current literature, in this study, the secrecy performance of a novel RIS-aided combined RF-FSO system employing the variable gain relaying mechanism is investigated, where confidential information is transmitted from a source in the presence of an unexpected eavesdropper to the receiver. A relay is positioned between the source and destination receiver, which accepts RF signals from the source and turns them into signals in optical form, re-transmitting them via the FSO link to the destination. It is worth pointing out that the eavesdropper can intercept information from the same RIS which is used to transmit data toward the relay.Nakagami-*m* fading distributions are assumed to be followed by all the RF links, while the FSO link experiences Málaga turbulence with pointing error. We assume the Nakagami-*m* distribution in our model as it has the ability to represent a large range of fading conditions, from severe fading to non-fading channels. On the other hand, the generalized Málaga distribution is considered due to the ability to explain the atmospheric turbulence effects on the FSO communication network perfectly. Finally, we may shorten the main contribution of this research as follows,

1) In this research paper, the security performance of a RIS-aided RF-FSO combined system is investigated in the presence of three eavesdropping scenarios (i.e., RF eavesdropper, FSO eavesdropper, and simultaneous RF and FSO eavesdroppers), with the goal of enhancing secrecy. To the best of our knowledge, this study is the first to examine the impact of RIS technology on the secrecy performance for such configurations. It is noteworthy that prior studies [44], [45] have investigated the secrecy performance within RF-FSO mixed models. However, it is essential to highlight that these analyses did not encompass the integration of RIS, a crucial distinction from our proposed model. Conversely, the authors of [46] focused on underwater optical communication in the second hop, thus deviating from the scope and application of our suggested model.
2) Firstly, a new cumulative distribution function (CDF) for the suggested RF-FSO combined system is developed by using the individual probability density functions (PDFs) and CDFs. From the newly derived CDF, the closed-form expressions for various secrecy performance metrics are obtained, including the secrecy outage probability (SOP), average secrecy capacity (ASC), probability of strictly positive secrecy capacity (SPSC), and effective secrecy throughput (EST). It is worth noting that these expressions are said to be novel and any of the existing literature has not addressed them, as our proposed model is significantly different from previous ones.
3) To evaluate the performance of potential eavesdropper attacks, numerical results are presented from the obtained expressions for the ASC, SOP, SPSC, and EST metrics. Our findings indicate that factors such as fading parameters, weather conditions, and receiver detection techniques play a crucial role in ensuring secure mixed RF-FSO configurations. Finally, Monte Carlo simulations are employed in order to verify the precision of our analytical and asymptotic expressions.

C. ORGANIZATION

This paper is organized into several sections. The mixed RF-FSO system model is presented in Section II, while Section III discusses the statistical characteristics of each link. The performance metrics such as ASC, SOP, probability of SPSC, and EST analysis are derived in Section IV. Section V presents the results of Monte Carlo simulations and numerical analysis. Finally, the paper concludes by summarizing our findings in Section VI.

II. SYSTEM MODEL

As shown in Fig. 1, a conventional dual-hop RIS-assisted RF-FSO system is comprised of a source $\mathcal{S}$ (i.e., ground control station, smartphone, etc.), an interim relay $\mathcal{R}$, one RIS $\mathcal{I}_{\mathcal{S}}$, and a destination user $\mathcal{D}$ (i.e., drone, satellite ground station, smartphone, etc.) who is distant from the source. We may assume that the distance between $\mathcal{S}$ and $\mathcal{R}$ is very far, and because of the way the environment is set up between these two nodes, there is no exact connection between $\mathcal{S}$ and $\mathcal{R}$. So, the signal directed from $\mathcal{S}$ first goes to $\mathcal{I}_{\mathcal{S}}$, which then sends it towards $\mathcal{R}$. It is assumed that the $\mathcal{I}_{\mathcal{S}}$ can obtain the channel phases related to $\mathcal{S}-\mathcal{I}_{\mathcal{S}}$ and $\mathcal{I}_{\mathcal{S}}-\mathcal{R}$ links, which is then utilized to boost the SNR at $\mathcal{R}$ by inducing proper phases at the meta-surfaces of $\mathcal{I}_{\mathcal{S}}$. The unauthorized users are known as eavesdroppers (i.e., drones, smartphones, etc.) denoted by $\mathcal{E}_r$ and $\mathcal{E}_d$ attempt to overhear the confidential data which is being forwarded from the $\mathcal{S}$ to $\mathcal{D}$. Such types of mixed models demonstrate their versatility and advantages in a range of applications, including industrial sensor networks [47], aerial surveillance

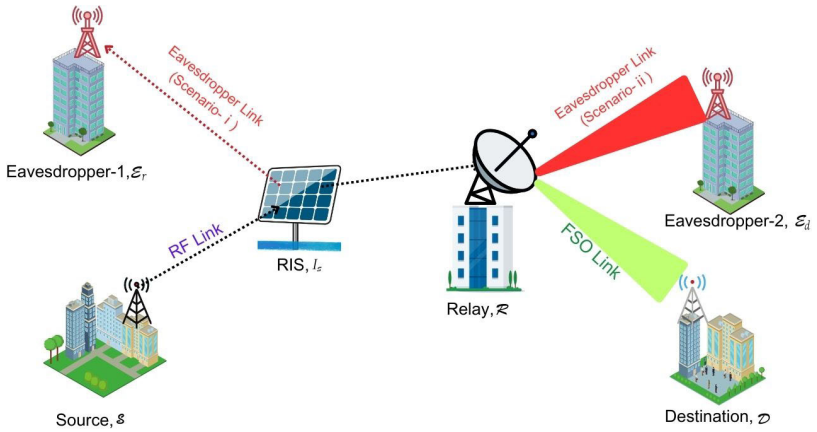

FIGURE 1. The combined RF-FSO relaying system having a source ($\mathcal{S}$), relay ($\mathcal{R}$), RIS surface ($\mathcal{I}_\mathcal{S}$), destination ($\mathcal{D}$), and eavesdroppers ($\mathcal{E}_r$, $\mathcal{E}_d$).

drones [20], military and satellite communications [48], and IoT-enabled smart buildings [12], [47]. This underscores the effectiveness of integrating RF and FSO technologies to address various communication requirements. In accordance with the location of eavesdroppers, three distinct cases are considered.

- In Scenario$-i$, the FSO link (i.e., $\mathcal{R}-\mathcal{D}$) is thought to be extremely secure. As a result, eavesdropper, $\mathcal{E}_r$ uses the RF link only to intercept. Similar to the $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{R}$ link, the $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{E}_r$ link is subjected to Nakagami-m fading channels.
- In Scenario$-ii$, the RF link (i.e., $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{R}$) is considered as secured whereas eavesdropper, $\mathcal{E}_d$ attempts to eavesdrop exclusively over the FSO link (i.e., $\mathcal{R}-\mathcal{D}$). It is assumed that $\mathcal{R}-\mathcal{E}_d$ link undergoes Málaga turbulence same as $\mathcal{R}-\mathcal{D}$ link.
- In Scenario$-iii$, neither of the links is safe from eavesdropping. Hence, both eavesdroppers (i.e., $\mathcal{E}_r$ and $\mathcal{E}_d$) simultaneously attempt to intercept the $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{R}$ and $\mathcal{R}-\mathcal{D}$ links, respectively.

It is assumed that $\mathcal{D}$ has only one photodetector for reception of optical wave, while the $\mathcal{I}_\mathcal{S}$ has N reflecting elements. Due to the fact that $\mathcal{S}$ is not straightly linked to $\mathcal{D}$, we consider that transmission takes up two hops. The system model offers that in the initial hop, $\mathcal{S}$ will transfer signals to $\mathcal{R}$ empowered by $\mathcal{I}_\mathcal{S}$ by means of the $\mathcal{S}$- $\mathcal{I}_\mathcal{S}$-$\mathcal{R}$ link. The $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$-$\mathcal{R}$ and $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$-$\mathcal{E}_r$ links (all the RF links) are subjected to Nakagami-m fading distribution. In the last hop, the incoming RF signal is transformed by the relay $\mathcal{R}$ into optical form before forwarding it towards $\mathcal{D}$. The FSO links ($\mathcal{R}$-$\mathcal{D}$ and $\mathcal{R}$-$\mathcal{E}_d$) undergo Málaga turbulence.

A. SNRs OF RIS-AIDED RF (MAIN AND EAVESDROPPER) LINKS

Let's the channel gains of $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$, $\mathcal{I}_\mathcal{S}$-$\mathcal{R}$ and $\mathcal{I}_\mathcal{S}$-$\mathcal{E}_r$ links are denoted as $h_{s,i}$, $g_{i,r}$ and $n_{i,er}$, respectively. So, the expressions of the signals received at $\mathcal{R}$ and $\mathcal{E}_r$ are given as

$$y_r = \left[\sum_{i=1}^{N} h_{s,i} e^{j\zeta_{i,r}} g_{i,r}\right] x_s + z_r, \tag{1}$$

$$y_{er} = \left[\sum_{i=1}^{N} h_{s,i} e^{j\theta_{i,er}} n_{i,er}\right] x_s + z_{er}, \tag{2}$$

respectively, where $h_{s,i} = \alpha_{s,i} e^{-j\varrho_{s,i}}$, $g_{i,r} = \beta_{i,r} e^{-j\vartheta_{i,r}}$ and $n_{i,er} = \delta_{i,er} e^{-j\phi_{i,er}}$, the Nakagami-$m$ distributed random variables (RVs) are $\alpha_{s,i}$, $\beta_{i,r}$, and $\delta_{i,er}$. $\varrho_{s,i}$, $\vartheta_{i,r}$ and $\phi_{i,er}$ denote the channel phases, adjustable phases induced at the i-th reflecting element of $\mathcal{I}_\mathcal{S}$ are denoted as $\zeta_{i,r}$ and $\theta_{i,er}$. The transmitted signal from $\mathcal{S}$ is symbolized as x_s having power P_s, and the Additive White Gaussian Noise (AWGN) samples are denoted as $z_r \sim \tilde{\mathcal{N}}(0, N_r)$, $z_{er} \sim \tilde{\mathcal{N}}(0, N_{er})$ with N_r, N_{er} presenting the noise powers. The maximum instantaneous SNRs at $\mathcal{R}$ and $\mathcal{E}_r$ are obtained considering the optimal choice of $\zeta_{i,r}$ and $\theta_{i,er}$ by eliminating the channel phases as $\zeta_{i,r} = \varrho_{s,i} + \vartheta_{i,r}$ and $\theta_{i,er} = \varrho_{s,i} + \phi_{i,er}$. Hence, the corresponding SNRs are given by

$$\gamma_r = \bar{\gamma}_r \left(\sum_{i=0}^{N} \alpha_{s,i}\beta_{i,r}\right)^2 \text{ and } \gamma_{er} = \bar{\gamma}_{er} \left(\sum_{i=0}^{N} \alpha_{s,i}\delta_{i,er}\right)^2, \tag{3}$$

where the average SNR of $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{R}$ link is defined as $\bar{\gamma}_r = \frac{P_s}{N_r}$ and the average SNR of $\mathcal{S}-\mathcal{I}_\mathcal{S}-\mathcal{E}_r$ link is defined as $\bar{\gamma}_{er} = \frac{P_s}{N_{er}}$. Again, gain of the channels $\mathcal{R}-\mathcal{D}$ and $\mathcal{R}-\mathcal{E}_d$ links are given as $h_{r,d} \in \mathbb{C}^{1\times 1}$ and $h_{r,ed} \in \mathbb{C}^{1\times 1}$, respectively. So, the signal received at $\mathcal{D}$ and $\mathcal{E}_d$ is stated as

$$y_d = h_{r,d} y_r + z_d, \tag{4}$$

$$y_{ed} = h_{r,ed} y_r + z_{ed}, \tag{5}$$

where $z_d \sim \tilde{\mathcal{N}}(0, N_d)$ and $z_{ed} \sim \tilde{\mathcal{N}}(0, N_{ed})$ illustrates optical noises arriving at $\mathcal{D}$ with a power N_d and N_{ed}, respectively. The related SNR is expressed as

$$\gamma_d = \frac{P_r}{N_d} \left\|h_{r,d}\right\|^2 = \bar{\gamma}_d \left\|h_{r,d}\right\|^2, \tag{6}$$

$$\gamma_{ed} = \frac{P_r}{N_{ed}} \left\|h_{r,ed}\right\|^2 = \bar{\gamma}_{ed} \left\|h_{r,ed}\right\|^2, \tag{7}$$

where the average SNR of $\mathcal{R}-\mathcal{D}$ and $\mathcal{R}-\mathcal{E}_d$ links are expressed as $\bar{\gamma}_d$ and $\bar{\gamma}_{ed}$, respectively. The power transmitted from $\mathcal{R}$ is denoted by P_r.

The SNR expression for the combined RIS-aided RF-FSO system when employing the AF variable gain relaying scheme is given as [49, Eq. (4)]

$$\gamma_{Eq} = \frac{\gamma_r \gamma_d}{\gamma_r + \gamma_d + 1} \cong \min\{\gamma_r, \gamma_d\}. \tag{8}$$

III. CHANNELS REALIZATION

A. PDF AND CDF OF RF LINKS

The PDF of γ_j, where $j \in (r, er)$ is expressed as [50, Eq. (2)]

$$f_{\gamma_j}(\gamma) = \frac{(\frac{\gamma}{\bar{\gamma}_j})^{\frac{a_j}{2}} e^{-(\frac{1}{b_j}\frac{\gamma}{\bar{\gamma}_j})}}{2b_j^{a_j+1}\Gamma(a_j+1)\sqrt{\gamma\bar{\gamma}_j}}, \tag{9}$$

where

$$a_j = \frac{m_i m_j N \Gamma(m_i)^2 \Gamma(m_j)^2}{m_i m_j \Gamma(m_i)^2 \Gamma(m_j)^2 - \Gamma\left(m_i+\frac{1}{2}\right)^2 \Gamma\left(m_j+\frac{1}{2}\right)^2},$$

$$b_j = \frac{m_i m_j \Gamma(m_i)^2 \Gamma(m_j)^2 - \Gamma\left(m_i+\frac{1}{2}\right)^2 \Gamma\left(m_j+\frac{1}{2}\right)^2}{\sqrt{\frac{m_i}{\Omega_i}}\Gamma(m_i)\Gamma\left(m_i+\frac{1}{2}\right)\sqrt{\frac{m_j}{\Omega_j}}\Gamma(m_j)\Gamma\left(m_j+\frac{1}{2}\right)}.$$

m_i and Ω_i denote the fading severity and scale parameters of $\mathcal{S}-\mathcal{I}_\mathcal{S}$ link, for $\mathcal{I}_\mathcal{S}-\mathcal{R}$ and $\mathcal{I}_\mathcal{S}-\mathcal{E}_r$ links, those are denoted as m_j and Ω_j, respectively, and the Gamma operator is signified by $\Gamma(.)$. The CDF of γ_j is stated as

$$F_{\gamma_j}(\gamma) = \frac{\gamma(a_j+1, \frac{\sqrt{\frac{\gamma}{\bar{\gamma}_j}}}{b_j})}{\Gamma(a_j+1)}, \tag{10}$$

where $\gamma(\cdot,\cdot)$ indicating the lower incomplete Gamma function as given in [51, Eq. (8.350.1)].

B. PDF AND CDF OF FSO LINKS

We assume the FSO links undergo Málaga turbulence with pointing error impairments. Fundamentally, this turbulence model is a physical system made up of a line-of-sight (LOS) communication (U_L), a component distributed by edges on the propagation axis and coupled to the LOS (U_S^C), and a free component dissipated with the aid of off-axis eddies (U_S^G). Moreover, it is regarded as one of the popular generalized optical turbulence models that can incorporate several conventional turbulence models, e.g. Lognormal, Rice-Nakagami, Gamma, etc. as special cases. The PDF of γ_k, where $k \in (d, ed)$ is expressed as [44, Eq. (12)]

$$f_{\gamma_k}(\gamma) = \frac{\epsilon_k^2 A_k}{2^r \gamma} \sum_{q_k=1}^{\beta_k} b_{q_k} G_{1,3}^{3,0}\left[B_k\left(\frac{\gamma}{\mu_{k,r}}\right)^{\frac{1}{r}} \middle| \begin{matrix}\epsilon_k^2+1 \\ \epsilon_k^2, \alpha_k, q_k\end{matrix}\right], \tag{11}$$

where

$$A_k = \frac{2\alpha_k^{\frac{\alpha_k}{2}}}{g^{1+\frac{\alpha_k}{2}}\Gamma(\alpha_k)}\left(\frac{g\beta_k}{g\beta_k+\Omega'}\right)^{\beta_k+\frac{\alpha_k}{2}},$$

$$B_k = \frac{\epsilon_k^2 \alpha_k \beta_k (g+\Omega')}{(\epsilon_k^2+1)(g\beta_k+\Omega')},$$

$$b_{q_k} = a_k\left(\frac{\alpha_k\beta_k}{g\beta_k+\Omega'}\right)^{-\frac{\alpha_k+q_k}{2}},$$

$$a_k = \binom{\beta_k-1}{q_k-1}\frac{(g\beta_k+\Omega')^{1-\frac{q_k}{2}}}{(q_k-1)!}\left(\frac{\Omega'}{g}\right)^{q_k-1}\left(\frac{\alpha_k}{\beta_k}\right)^{\frac{q_k}{2}}.$$

Here, the number of large-scale cells spread over the whole process is denoted by α_k, the fading parameter is β_k, and ϵ_k is the pointing error at the destination for $\mathcal{R}-\mathcal{D}$ or $\mathcal{R}-\mathcal{E}_d$ links. r indicates the detection technique used on the receiver side, i.e., the heterodyne detection(HD) technique is denoted by $r = 1$ and the intensity modulation/direct detection (IM/DD) approach is defined by $r = 2$ where $\mu_{k,r}$ ($\mu_{k,1} = \bar{\gamma}_k$ and $\mu_{k,2} = \frac{\alpha_k\epsilon_k^2(\epsilon_k^2+1)^{-2}(\epsilon_k^2+2)(g+\Omega')}{(\alpha_k+1)\left[2g(g+2\Omega')+\Omega'^2(1+\frac{1}{\beta_k})\right]}\bar{\gamma}_k$). The scattering component's average received power by off-axis eddies is given by $g = \mathbb{E}[|U_S^G|^2] = 2b_k(1-\rho)$, the average power of all scattered components are denoted as $2b_k = \mathbb{E}[|U_S^C|^2 + |U_S^G|^2]$, the measure of scattering power to the LOS component is expressed as ρ ($0 \le \rho \le 1$), the average power of coherent contributions is defined as $\Omega' = \Omega + 2b_k\rho + 2\sqrt{2b_k\rho\Omega}cos(\phi_a - \phi_b)$, the average power of the LOS component is denoted by $\Omega = \mathbb{E}[|U_L|^2]$, ϕ_a and ϕ_b are the phases of the LOS communication, and $\mathbf{G}[\cdot]$ is the Meijer's G-function defined in [51, Eq. (9.301)]. Therefore, the CDF of γ_k is expressed as

$$F_{\gamma_k}(\gamma) = D_k \sum_{q_k=1}^{\beta_k} c_{q_k} G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_k}{\mu_{k,r}}\gamma \middle| \begin{matrix}1, s_k \\ t_k, 0\end{matrix}\right], \tag{12}$$

where $D_k = \frac{\epsilon_k^2 A_k}{2^r(2\pi)^{r-1}}$, $c_{q_k} = b_{q_k} r^{\alpha_k+q_k-1}$, $\chi_k = \frac{B_k^r}{r^{2r}}$, $s_k = \Delta(r, \epsilon_k^2+1)$ including r number of terms, $t_k = \Delta(r, {\epsilon_k}^2), \Delta(r, \alpha_k), \Delta(r, q_k)$ that incorporates $3r$ number of terms, and $\Delta(x, a) = \frac{a}{x}, \frac{a+1}{x}, \ldots, \frac{a+x-1}{x}$.

C. CDF FOR DUAL-HOP RF-FSO LINK

According to (8), we can express the CDF of γ_{Eq} as

$$\begin{aligned} F_{Eq}(\gamma) &= \Pr\{\min\{\gamma_r, \gamma_d\} < \gamma\} \\ &= F_{\gamma_r}(\gamma) + F_{\gamma_d}(\gamma) - F_{\gamma_r}(\gamma)F_{\gamma_d}(\gamma). \end{aligned} \tag{13}$$

Substituting (10) and (12) into (13), the CDF of γ_{Eq} can be deduced finally as

$$\begin{aligned} F_{Eq}(\gamma) = {} & \frac{\gamma(a_r+1, \frac{\sqrt{\frac{\gamma}{\bar{\gamma}_r}}}{b_r})}{\Gamma(a_r+1)} + D_d \sum_{q_d=1}^{\beta_d} c_{q_d} \\ & \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\gamma \middle| \begin{matrix}1, s_d \\ t_d, 0\end{matrix}\right] \\ & \times \left(1 - \frac{\gamma(a_r+1, \frac{\sqrt{\frac{\gamma}{\bar{\gamma}_r}}}{b_r})}{\Gamma(a_r+1)}\right). \end{aligned} \tag{14}$$

IV. PERFORMANCE METRICS

In this section, we illustrate how the different performance metrics, such as the lower bound of SOP and the probability of SPSC, ASC, and EST, can be expressed analytically and asymptotically.

A. SECRECY OUTAGE PROBABILITY (SOP)

Scenario$-i$**:** The probability that instantaneous secrecy capacity (C_s) falls below a predetermined threshold known as the target secrecy rate (T_s) is defined as SOP. However, it is mathematically stated as [19, Eq. (22)]

$$\begin{aligned} SOP_1 &= \Pr\left\{C_s\left(\gamma_{Eq}, \gamma_{er}\right) \leq T_s\right\} \\ &= \Pr\left\{\gamma_{Eq} \leq \Theta\left(\gamma_{er}+1\right)-1\right\} \\ &= \int_0^{\infty} F_{Eq}\left(\Theta\left(\gamma+1\right)-1\right) f_{\gamma_{er}}\left(\gamma\right) d\gamma, \end{aligned} \tag{15}$$

where $\Theta = 2^{T_s}$ and the predefined rate, $T_s > 0$. However, the computation of the SOP using (15) can be challenging, as it involves complex mathematical derivations that may not be feasible in certain scenarios. Therefore, to address this issue, we may demonstrate the lower bound of SOP which can be mathematically expressed as

$$\begin{aligned} SOP_1 &= \Pr\{\gamma_{Eq} \leq \Theta(\gamma_{er}+1)-1\} \\ \geq SOP_1^L &= \Pr\{\gamma_{Eq} \leq \Theta\gamma_{er}\} \\ &= \int_0^{\infty} F_{Eq}(\Theta\gamma) f_{\gamma_{er}}(\gamma) d\gamma. \end{aligned} \tag{16}$$

The lower bound of SOP may eventually be expressed by substituting (9) and (14) into (16) as

$$SOP_1 = \sum_{n_1=0}^{\infty} \mathcal{J}_1 \mathcal{Y}_1 + \sum_{q_d=1}^{\beta_d} \mathcal{J}_2 \mathcal{Y}_2 - \sum_{n_1=0}^{\infty} \sum_{q_d=1}^{\beta_d} \mathcal{J}_3 \mathcal{Y}_3, \tag{17}$$

where

$$\mathcal{J}_1 = \frac{(-1)^{n_1} \Theta^{\frac{1}{2}(a_r+a_{er}+n_1)} \bar{\gamma}_r^{-\frac{1}{2}(a_r+n_1+1)} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+1)}}{(2b_{er})^{a_{er}+1} n_1! (a_r+n_1+1)\Gamma(a_r+1)\Gamma(a_{er}+1)},$$

$$\mathcal{J}_2 = \frac{D_d c_{q_d} \Theta^{-\frac{1}{2}(a_{er}+1)} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+1)}}{(2b_{er})^{a_{er}+1}\Gamma(a_{er}+1)} \text{ and}$$

$$\mathcal{J}_3 = \frac{D_d c_{q_d} (-1)^{n_1} \Theta^{\frac{1}{2}(a_r+a_{er}+n_1)} \bar{\gamma}_r^{-\frac{1}{2}(a_r+n_1+1)} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+1)}}{n_1! (2b_{er})^{a_{er}+1} (a_r+n_1+1)\Gamma(a_r+1)\Gamma(a_{er}+1)}.$$

Here the three integral parts are $\mathcal{Y}_1$, $\mathcal{Y}_2$, and $\mathcal{Y}_3$ that are deduced as follows.

1) DERIVATION OF $\mathcal{Y}_1$

$\mathcal{Y}_1$ is given as

$$\mathcal{Y}_1 = \int_0^{\infty} \gamma^{\frac{1}{2}(a_r+a_{er}+n_1)} e^{-\left(\frac{1}{b_{er}}\sqrt{\frac{\gamma}{\bar{\gamma}_{er}}}\right)} d\gamma. \tag{18}$$

Utilizing the integration as [52, Eq. (3.326.2)], $\mathcal{Y}_1$ may be stated as

$$\mathcal{Y}_1 = \Gamma(F_1)\left(b_{er}\sqrt{\bar{\gamma}_{er}}\right)^{F_1}, \tag{19}$$

where $F_1 = a_r + a_{er} + n_1 + 2$.

2) DERIVATION OF $\mathcal{Y}_2$

$\mathcal{Y}_2$ is written as

$$\begin{aligned} \mathcal{Y}_2 &= \int_0^{\infty} \gamma^{\frac{1}{2}(a_{er}-1)} e^{-\left(\frac{1}{b_{er}}\sqrt{\frac{\Theta\gamma}{\bar{\gamma}_{er}}}\right)} \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\Theta \middle| \begin{matrix} 1, s_d \\ t_d, 0 \end{matrix}\right] d\gamma \\ &= \int_0^{\infty} \gamma^{\frac{1}{2}(a_{er}-1)} G_{0,1}^{1,0}\left[\frac{\sqrt{\frac{\Theta\gamma}{\bar{\gamma}_{er}}}}{b_{er}} \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\Theta \middle| \begin{matrix} 1, s_d \\ t_d, 0 \end{matrix}\right] d\gamma. \end{aligned} \tag{20}$$

The exponential function is turned into Meijer's G function here using [53, Eq. (8.4.3.1)]. Therefore, utilizing the identity of [53, Eq. (2.24.1.1)], $\mathcal{Y}_2$ can be written finally as

$$\begin{aligned} \mathcal{Y}_2 &= \left(\frac{1}{b_{er}}\sqrt{\frac{\Theta}{\bar{\gamma}_{er}}}\right)^{-\frac{1}{2}(a_{er}+1)} \\ &\quad \times G_{r+2,3r+2}^{3r,2}\left[\frac{\chi_d\sqrt{\bar{\gamma}_{er}}}{\mu_{d,r}b_{er}}\Theta \middle| \begin{matrix} 1, v_1, s_d \\ t_d, v_1, 0 \end{matrix}\right], \end{aligned} \tag{21}$$

where $v_1 = \Delta\left(1, \frac{a_{er}}{2} - \frac{1}{2}\right)$.

3) DERIVATION OF $\mathcal{Y}_3$

$\mathcal{Y}_3$ is expressed as

$$\begin{aligned} \mathcal{Y}_3 &= \int_0^{\infty} \gamma^{(z_1+1)} e^{-\left(\frac{1}{b_{er}}\sqrt{\frac{\Theta\gamma}{\bar{\gamma}_{er}}}\right)} \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\Theta \middle| \begin{matrix} 1, s_d \\ t_d, 0 \end{matrix}\right] d\gamma \\ &= \int_0^{\infty} \gamma^{(z_1+1)} G_{0,1}^{1,0}\left[\frac{\sqrt{\frac{\Theta\gamma}{\bar{\gamma}_{er}}}}{b_{er}} \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\Theta \middle| \begin{matrix} 1, s_d \\ t_d, 0 \end{matrix}\right] d\gamma, \end{aligned} \tag{22}$$

where $z_1 = a_r + a_{er} + n_1$. Now, using the identity of [53, Eq. (2.24.2.1)], $\mathcal{Y}_3$ can be obtained as

$$\begin{aligned} \mathcal{Y}_3 &= \left(\frac{1}{b_{er}}\sqrt{\frac{\Theta}{\bar{\gamma}_{er}}}\right)^{-\frac{1}{2}(z_1+2)} \\ &\quad \times G_{r+2,3r+2}^{3r,2}\left[\frac{\chi_d\sqrt{\bar{\gamma}_{er}}}{\mu_{d,r}b_{er}}\Theta \middle| \begin{matrix} 1, v_2, s_d \\ t_d, v_2, 0 \end{matrix}\right], \end{aligned} \tag{23}$$

where $v_2 = \Delta\left(1, -\frac{z_1}{2} - \frac{1}{2}\right)$.

Asymptotic Analysis: With the use of [54, Eq. (20)], the Meijer's G function is expanded, and as a consequence, the asymptotic expression due to the lower bound of SOP_1 may be expressed as (24), shown at the bottom of the next page, where $\Lambda_{p,q}$ denotes the qth-term of Λ_p, $\Lambda_1 = [1, v_1, s_d]$, $\Lambda_2 = [t_d, v_1, 0]$, $\Lambda_3 = [1, v_2, s_d]$, and $\Lambda_4 = [t_d, v_2, 0]$.

Scenario$-ii$**:** The SOP can be expressed in the presence of an eavesdropper at the FSO link as [55]

$$\begin{aligned} SOP_2 &= \Pr\{C_s \le T_s\} = \Pr\left\{\gamma_{Eq} \le \Theta\gamma_{ed} + \Theta - 1\right\} \\ &= \int_0^\infty \int_{\Theta\gamma+\Theta-1}^\infty f_{\gamma_{Eq}}(\gamma) f_{\gamma_{ed}}(\gamma) d\gamma_{Eq} d\gamma \\ &= \int_0^\infty F_{\gamma_d}(\Theta\gamma + \Theta - 1) f_{\gamma_{ed}}(\gamma) d\gamma \\ &\quad \times \left(1 - F_{\gamma_r}(\Theta - 1)\right) + F_{\gamma_r}(\Theta - 1). \end{aligned} \tag{25}$$

It is difficult to compute the closed-form equation for exact SOP. As a consequence, we have the lower bound of SOP, which can be written as [54, Eq. (18)]

$$\begin{aligned} SOP_2 \ge SOP_2^L &= \Pr\left\{\gamma_{Eq} \le \Theta\gamma_{ed}\right\} \\ &= \int_0^\infty F_{\gamma_d}(\Theta\gamma) f_{\gamma_{ed}}(\gamma) d\gamma \\ &\quad \times \left(1 - F_{\gamma_r}(\Theta - 1)\right) + F_{\gamma_r}(\Theta - 1). \end{aligned} \tag{26}$$

With the substitution of (10), (11) and (12) into (26) and also using [53, Eq. (2.24.1.1)] results in

$$\begin{aligned} SOP_2 = 1 - \mathcal{J}_4 \Bigg(& \mathcal{J}_5 \sum_{q_d=1}^{\beta_d} \sum_{q_{ed}=1}^{\beta_{ed}} c_{q_d} b_{q_{ed}} \\ & \times G_{4r+1,4r+1}^{3r+1,3r} \left[\frac{\mu_{d,r}}{\mu_{ed,r}} \Theta \middle| \begin{matrix} 1 - t_d, 1, s_{ed} \\ t_{ed}, 0, 1 - s_d \end{matrix} \right] \Bigg) + \mathcal{J}_4, \end{aligned} \tag{27}$$

where $\mathcal{J}_4 = \frac{\gamma(a_r+1, \frac{1}{b_r}\sqrt{\frac{(\Theta-1)}{\bar{\gamma}_r}})}{\Gamma(a_r+1)}$, $\mathcal{J}_5 = \frac{D_d \epsilon_{ed}^2 A_{ed}}{2^r}$, $s_{ed} = \Delta(r, \epsilon_{ed}^2 + 1)$ that includes r number of terms, $t_{ed} = \Delta(r, \epsilon_{ed}{}^2)$, $\Delta(r, \alpha_{ed})$, $\Delta(r, q_{ed})$ which includes $3r$ number of terms.

Asymptotic Analysis: With the use of [54, Eq. (20)], the Meijer's G function is expanded, and as a consequence, the asymptotic expression due to the lower bound of SOP_2 may be written as (28), shown at the bottom of the next page, where $\Psi_{p,q}$ illustrates the qth-term of Ψ_p, $\Psi_1 = [1 - t_d, 1, s_{ed}]$, $\Psi_2 = [t_{ed}, 0, 1 - s_d]$.

Scenario$-iii$**:** The lower bound of SOP for RIS-assisted mixed RF-FSO network under simultaneous eavesdropping attack across both the RF and FSO links is defined mathematically as

$$SOP_3 = 1 - (P_1 \times P_2)\,. \tag{30}$$

where

$$P_1 = 1 - \int_0^\infty F_{\gamma_r}(\Theta\gamma) f_{\gamma_{er}}(\gamma) d\gamma, \tag{31}$$

$$P_2 = 1 - \int_0^\infty F_{\gamma_d}(\Theta\gamma) f_{\gamma_{ed}}(\gamma) d\gamma. \tag{32}$$

Now, replacing (9) and (10) into (31) and implementing the identity of [52, Eq. (3.326.2)] to obtain P_1 as

$$P_1 = 1 - \mathcal{J}_6 \sum_{m=0}^{\infty} \frac{(-1)^m \left(\frac{\sqrt{\Theta}}{b_r\sqrt{\bar{\gamma}_r}}\right)^{U_1} \left(b_{er}\sqrt{\bar{\gamma}_{er}}\right)^{U_2} \Gamma(U_2)}{m! U_1 \times \Gamma(a_r + 1)}, \tag{33}$$

where $\mathcal{J}_6 = \frac{\bar{\gamma}_{er}^{\frac{1}{2}(a_{er}+1)}}{2b_{er}^{a_{er}+1}\Gamma(a_{er}+1)}$, $U_1 = a_r + m + 1$ and $U_2 = a_r + a_{er} + m + 2$. Similarly, P_2 is derived by placing (11) and (12) into (32) and employing [53, Eq. (2.24.1.1)] to solve the integration as

$$\begin{aligned} P_2 = 1 - \Bigg(& \mathcal{J}_5 \sum_{q_d=1}^{\beta_d} \sum_{q_{ed}=1}^{\beta_{ed}} c_{q_d} b_{q_{ed}} \\ & \times G_{4r+1,4r+1}^{3r+1,3r} \left[\frac{\mu_{d,r}}{\mu_{ed,r}} \Theta \middle| \begin{matrix} 1 - t_d, 1, s_{ed} \\ t_{ed}, 0, 1 - s_d \end{matrix} \right] \Bigg). \end{aligned} \tag{34}$$

Asymptotic Analysis: The Meijer's G function can be expanded at the higher SNR using [54, Eq. (20)]. Therefore, the asymptotic representation for the lower bound of SOP_3 can be expressed as (29), shown at the bottom of the next page, where $\Phi_{p,q}$ illustrates the qth-term of Φ_p, $\Phi_1 = [1 - t_d, 1, s_{ed}]$, $\Phi_2 = [t_{ed}, 0, 1 - s_d]$.

B. STRICTLY POSITIVE SECRECY CAPACITY (SPSC)

To prevent eavesdropping, the secrecy capacity must be positive, and the probability of achieving a positive secrecy capacity is referred to as the SPSC. The mathematical expression for the probability of SPSC is [56, Eq. (25)]

$$\begin{aligned} SPSC &= \Pr(C_s \ge 0) \\ &= 1 - \Pr(C_s \le 0) \\ &= 1 - SOP|_{T_s=0}. \end{aligned} \tag{35}$$

SPSC can be demonstrated by the substitution of SOP formulations from (17), (27), and (30) into (35). Therefore,

$$SPSC_1 = 1 - SOP_1|_{T_s=0}\,, \text{ (Scenario}-i\text{)} \tag{36}$$

$$\begin{aligned} SOP_1(\infty) = & \sum_{n_1=0}^{\infty} \mathcal{J}_1 \mathcal{Y}_1 + \sum_{k=1}^{2} \sum_{q_d=1}^{\beta_d} \left(\frac{1}{b_{er}}\sqrt{\frac{\Theta}{\bar{\gamma}_{er}}}\right)^{-\frac{1}{2}(a_{er}+1)} \frac{\mathcal{J}_2 \prod_{l=1;l\neq k}^{2} \Gamma\left(\Lambda_{1,k} - \Lambda_{1,l}\right)}{\prod_{l=3}^{r+2} \Gamma\left(1 + \Lambda_{1,l} - \Lambda_{1,k}\right)} \frac{\prod_{l=1}^{3r} \Gamma\left(1 + \Lambda_{2,l} - \Lambda_{1,k}\right)}{\prod_{l=3r+1}^{3r+2} \Gamma\left(\Lambda_{1,k} - \Lambda_{2,l}\right)} \\ & \times \left(\frac{\chi_d \sqrt{\bar{\gamma}_{er}}\Theta}{\mu_{d,r} b_{er}}\right)^{\Lambda_{1,k}-1} - \sum_{n_1=0}^{\infty} \sum_{k=1}^{2} \sum_{q_d=1}^{\beta_d} \left(\frac{1}{b_{er}}\sqrt{\frac{\Theta}{\bar{\gamma}_{er}}}\right)^{-\frac{1}{2}(z_1+2)} \frac{\mathcal{J}_3 \prod_{l=1;l\neq k}^{2} \Gamma\left(\Lambda_{3,k} - \Lambda_{3,l}\right)}{\prod_{l=3}^{r+2} \Gamma\left(1 + \Lambda_{3,l} - \Lambda_{3,k}\right)} \\ & \times \frac{\prod_{l=1}^{3r} \Gamma\left(1 + \Lambda_{4,l} - \Lambda_{3,k}\right)}{\prod_{l=3r+1}^{3r+2} \Gamma\left(\Lambda_{3,k} - \Lambda_{4,l}\right)} \left(\frac{\chi_d \sqrt{\bar{\gamma}_{er}}\Theta}{\mu_{d,r} b_{er}}\right)^{\Lambda_{3,k}-1}. \end{aligned} \tag{24}$$

$$SPSC_2 = 1 - SOP_2|_{T_s=0}\,, (\text{ Scenario}-ii\,) \quad (37)$$
$$SPSC_3 = 1 - SOP_3|_{T_s=0}\,.(\text{ Scenario}-iii) \quad (38)$$

C. EFFECTIVE SECRECY THROUGHPUT (EST)

The EST is a crucial secrecy measure that takes into account the reliability as well as security restrictions of eavesdropper channels and quantifies the average rate at which confidential data can be transmitted from the source to the destination without being intercepted. As a result, the EST may be mathematically defined as [44, Eq. (50)]

$$EST = T_s(1 - SOP). \quad (39)$$

With the substitution of (17), (27), and (30) into (39), we can demonstrate the analytical expression of EST analysis. Hence,

$$EST_1 = T_s\big(1 - SOP_1\big), (\text{ Scenario}-i\,) \quad (40)$$
$$EST_2 = T_s\big(1 - SOP_2\big), (\text{ Scenario}-ii) \quad (41)$$
$$EST_3 = T_s\big(1 - SOP_3\big).(\text{ Scenario}-iii) \quad (42)$$

D. AVERAGE SECRECY CAPACITY (ASC)

ASC is a performance metric used in wireless communication systems that quantifies the average amount of secure information that can be transmitted over a communication channel while maintaining a certain level of secrecy. Because wireless channels are time-varying in nature, ASC is calculated as the average value of instantaneous secrecy capacity and may be expressed mathematically as [57, Eq. (31)]

$$ASC_1 = \int_0^\infty \frac{1}{1+\gamma} f_{\gamma_{er}}(\gamma)\left[1 - F_{Eq}(\gamma)\right] d\gamma. \quad (43)$$

With the substitution of (9) and (14) into (43), ASC is expressed as

$$ASC_1 = \sum_{n_2=0}^{\infty} \mathcal{L}_1\mathcal{H}_1 - \sum_{n_3=0}^{\infty}\sum_{n_4=0}^{\infty} \mathcal{L}_2\mathcal{H}_2 - \sum_{q_d=1}^{\beta_d}\sum_{n_5=0}^{\infty} \mathcal{L}_3\mathcal{H}_3 + \sum_{q_d=1}^{\beta_d}\sum_{n_6=0}^{\infty}\sum_{n_7=0}^{\infty} \mathcal{L}_4\mathcal{H}_4, \quad (44)$$

where

$$\mathcal{L}_1 = \frac{(-1)^{n_2} b_{er} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+n_2+1)}}{n_2!\,(a_{er}+n_2+1)\,\Gamma(a_{er}+1)},$$
$$\mathcal{L}_2 = \frac{(-1)^{n_3+n_4} b_r b_{er} \bar{\gamma}_r^{-\frac{1}{2}(a_r+n_3+1)} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+n_4+1)}}{n_3!(a_r+n_3+1)\,n_4!\,(a_{er}+n_4+1)\,\Gamma(a_r+1)\Gamma(a_{er}+1)},$$
$$\mathcal{L}_3 = \frac{(-1)^{n_5} D_d c_{q_d} b_{er} (\bar{\gamma}_{er})^{-\frac{1}{2}(a_{er}+n_5+1)}}{n_5!\,(a_{er}+n_5+1)\,\Gamma(a_{er}+1)} \text{ and}$$
$$\mathcal{L}_4 = \frac{(-1)^{n_6+n_7} D_d c_{q_d} b_r b_{er} \bar{\gamma}_r^{-\frac{1}{2}(a_r+n_6+1)} \bar{\gamma}_{er}^{-\frac{1}{2}(a_{er}+n_7+1)}}{n_6!(a_r+n_6+1)\,n_7!\,(a_{er}+n_7+1)\,\Gamma(a_r+1)\Gamma(a_{er}+1)}.$$

Here, the integral parts are $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$, and $\mathcal{H}_4$ which are computed as follows.

1) DETERMINATION OF $\mathcal{H}_1$

$\mathcal{H}_1$ is written as

$$\mathcal{H}_1 = \int_0^\infty \gamma^{\frac{1}{2}(a_{er}+n_2+1)}(1+\gamma)^{-1} d\gamma = \int_0^\infty \gamma^{\frac{1}{2}(a_{er}+n_2+1)} G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right] d\gamma. \quad (45)$$

Making use of the identity of [58, Eq. (24)], $\mathcal{H}_1$ can be derived finally as

$$\mathcal{H}_1 = \Gamma\left(\frac{z_2}{2}+1\right)\Gamma\left(-\frac{z_2}{2}-1\right), \quad (46)$$

where $z_2 = a_{er} + n_2$.

2) DETERMINATION OF $\mathcal{H}_2$

$\mathcal{H}_2$ is expressed as

$$\mathcal{H}_2 = \int_0^\infty \gamma^{z_3+2}(1+\gamma)^{-1} d\gamma = \int_0^\infty \gamma^{z_3+2} G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} 0 \\ 0 \end{matrix}\right] d\gamma. \quad (47)$$

$$SOP_2(\infty) = 1 - \mathcal{J}_4\Bigg[\sum_{q_d=1}^{\beta_d}\sum_{q_{ed}=1}^{\beta_{ed}}\sum_{k=1}^{2} \frac{c_{q_d} b_{q_{ed}} \mathcal{J}_5 \prod_{l=1;l\neq k}^{3r} \Gamma\left(\Psi_{1,k} - \Psi_{1,l}\right)}{\prod_{l=3r+1}^{4r+1} \Gamma\left(1 + \Psi_{1,l} - \Psi_{1,k}\right)} \frac{\prod_{l=1}^{3r+1} \Gamma\left(1 + \Psi_{2,l} - \Psi_{1,k}\right)}{\prod_{l=3r+2}^{4r+1} \Gamma\left(\Psi_{1,k} - \Psi_{2,l}\right)} \times \left(\frac{\mu_{d,r}}{\mu_{ed,r}}\Theta\right)^{\Psi_{1,k}-1}\Bigg] + \mathcal{J}_4, \quad (28)$$

$$SOP_3(\infty) = 1 - \Bigg[P_1 \times \Bigg(1 - \Bigg(\sum_{q_d=1}^{\beta_d}\sum_{q_{ed}=1}^{\beta_{ed}}\sum_{k=1}^{2} \frac{\mathcal{J}_5 c_{q_d} b_{q_{ed}} \prod_{l=1;l\neq k}^{3r} \Gamma\left(\Phi_{1,k} - \Psi_{1,l}\right)}{\prod_{l=3r+1}^{4r+1} \Gamma\left(1 + \Phi_{1,l} - \Phi_{1,k}\right)} \times \frac{\prod_{l=1}^{3r+1} \Gamma\left(1 + \Phi_{2,l} - \Phi_{1,k}\right)}{\prod_{l=3r+2}^{4r+1} \Gamma\left(\Phi_{1,k} - \Phi_{2,l}\right)} \left(\frac{\mu_{d,r}}{\mu_{ed,r}}\Theta\right)^{\Phi_{1,k}-1}\Bigg)\Bigg)\Bigg]. \quad (29)$$

where $z_3 = a_r + a_{er} + n_3 + n_4$. Now, similar to $\mathcal{H}_1$, using [58, Eq. (24)], $\mathcal{H}_2$ can be obtained as

$$\mathcal{H}_2 = \Gamma\left(\frac{z_3}{2}+1\right)\Gamma\left(-\frac{z_3}{2}-1\right). \tag{48}$$

3) DETERMINATION OF $\mathcal{H}_3$

$\mathcal{H}_3$ is stated as

$$\begin{aligned}\mathcal{H}_3 &= \int_0^\infty (1+\gamma)^{-1}\gamma^{\frac{1}{2}(z_4+1)} \\ &\quad\times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\gamma\,\middle|\,\begin{matrix}1, s_d\\ t_d, 0\end{matrix}\right]d\gamma \\ &= \int_0^\infty \gamma^{\frac{1}{2}(z_4+1)} G_{1,1}^{1,1}\left[\gamma\,\middle|\,\begin{matrix}0\\0\end{matrix}\right] \\ &\quad\times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\gamma\,\middle|\,\begin{matrix}1, s_d\\ t_d, 0\end{matrix}\right]d\gamma,\end{aligned} \tag{49}$$

where $z_4 = a_{er} + n_5$. Now, with the help of [53, Eq. (8.4.2.5)] and [53, Eq. (2.24.1.1)], $\mathcal{H}_3$ can be expressed as

$$\mathcal{H}_3 = G_{r+2,3r+3}^{3r+1,2}\left[\frac{\chi_d}{\mu_{d,r}}\,\middle|\,\begin{matrix}1, w_1, s_d\\ t_d, w_1, 0\end{matrix}\right], \tag{50}$$

where $w_1 = \Delta\left(1, -\frac{z_4}{2}-\frac{1}{2}\right)$.

4) DETERMINATION OF $\mathcal{H}_4$

$\mathcal{H}_4$ is expressed as

$$\begin{aligned}\mathcal{H}_4 &= \int_0^\infty (1+\gamma)^{-1}\gamma^{\frac{1}{2}(z_5+2)} \\ &\quad\times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\gamma\,\middle|\,\begin{matrix}1, s_d\\ t_d, 0\end{matrix}\right]d\gamma \\ &= \int_0^\infty \gamma^{\frac{1}{2}(z_5+2)} G_{1,1}^{1,1}\left[\gamma\,\middle|\,\begin{matrix}0\\0\end{matrix}\right] \\ &\quad\times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_d}{\mu_{d,r}}\gamma\,\middle|\,\begin{matrix}1, s_d\\ t_d, 0\end{matrix}\right]d\gamma,\end{aligned} \tag{51}$$

where $z_5 = a_r + a_{er} + n_6 + n_7$. Now, similar to $\mathcal{H}_3$, using [53, Eq. (8.4.2.5)] and [53, Eq. (2.24.1.1)], $\mathcal{H}_4$ can be written finally as

$$\mathcal{H}_4 = G_{r+2,3r+3}^{3r+1,2}\left[\frac{\chi_d}{\mu_{d,r}}\,\middle|\,\begin{matrix}1, w_2, s_d\\ t_d, w_2, 0\end{matrix}\right], \tag{52}$$

where $w_2 = \Delta\left(1, \frac{z_5}{2}-\frac{1}{2}\right)$.

Asymptotic Analysis: The Meijer's G function is expanded in (44) with the help of [54, Eq. (20)]. The final expression of the asymptotic expression of ASC_1 may be seen in (53), shown at the bottom of the page, where $\Xi_{x,y}$ defines the yth term of Ξ_x, $\Xi_1 = [1, w_1, s_d]$, $\Xi_2 = [t_d, w_1, 0]$, $\Xi_3 = [1, w_1, s_d]$, and $\Xi_4 = [t_d, w_2, 0]$.

Significance of the Derived Expressions: In this paper, the derived expressions pertaining to metrics such as ASC, SOP, SPSC, and EST serve as precise quantitative benchmarks for evaluating the system's secrecy performance. These analytical formulations not only corroborate the accuracy of the proposed theoretical framework but also impart a more profound comprehension of the intricate interplay between secrecy metrics and system parameters. Through these expressions, it is apparent how factors such as fading characteristics, turbulence conditions, pointing errors, and attack scenarios exert discernible influences on the system's secrecy performance. This comprehensive analysis yields invaluable insights into the system's capacity to uphold secure communication, thereby enhancing its practical viability. Moreover, these expressions furnish pertinent guidance for network architects, proffering clear directives for design considerations and optimization strategies.

V. NUMERICAL RESULTS

This section highlights how various system parameters such as the number of reflecting elements, fading, electrical SNR, detection techniques, atmospheric turbulence, pointing error, etc., can affect the RIS-assisted RF-FSO system's performance in terms of security. This is demonstrated through numerical examples and figures generated using expressions from (17), (27), (30), (36)-(38) and (40)-(42). Besides, secrecy performance is also examined at a high SNR regime using (24), (28), (29) and (53) to gain more useful insights. It is noteworthy that the derived expressions include infinite series, but after a few terms, all of those series converge quickly. To get the analytical results, we take into account the first 100 terms. By averaging 100,000 random channel samples with MATLAB, Monte Carlo simulations are used to further verify the correctness of the generated analytical results. The following system parameters are chosen: $m_i = m_r = m_{er} = 2$, $N = 2$, $\Omega_i = \Omega_r = \Omega_{er} = 1$, $r = 1$, $\bar{\gamma}_{er} = 0$dB, $\bar{\gamma}_d = \bar{\gamma}_{ed} = 10$dB, $\epsilon_d = \epsilon_{ed} = \epsilon = 1.1$, unless specified otherwise.

$$\begin{aligned}ASC_1(\infty) &= \sum_{n_2=0}^{\infty}\mathcal{L}_1 h_1 - \sum_{n_3=0}^{\infty}\sum_{n_4=0}^{\infty}\mathcal{L}_2 h_2 - \sum_{k=1}^{2}\sum_{q_d=1}^{\beta_d}\sum_{n_5=0}^{\infty}\frac{\mathcal{L}_3\prod_{l=1}^{2}\Gamma\left(\Xi_{1,k}-\Xi_{1,l}\right)}{\prod_{l=3}^{r+2}\Gamma\left(1+\Xi_{1,l}-\Xi_{1,k}\right)} \\ &\quad\times\frac{\prod_{l=1}^{3r+1}\Gamma\left(1+\Xi_{2,l}-\Xi_{1,k}\right)}{\prod_{l=3r+2}^{3r+3}\Gamma\left(\Xi_{1,k}-\Xi_{2,l}\right)}\left(\frac{\chi_d}{\mu_{d,r}}\right)^{\Xi_{1,k}-1} + \sum_{k=1}^{2}\sum_{q_d=1}^{\beta_d}\sum_{n_6=0}^{\infty}\sum_{n_7=0}^{\infty}\frac{\mathcal{L}_4\prod_{l=1}^{2}\Gamma\left(\Xi_{3,k}-\Xi_{3,l}\right)}{\prod_{l=3}^{r+2}\Gamma\left(1+\Xi_{3,l}-\Xi_{3,k}\right)} \\ &\quad\times\frac{\prod_{l=1}^{3r+1}\Gamma\left(1+\Xi_{4,l}-\Xi_{3,k}\right)}{\prod_{l=3r+2}^{3r+3}\Gamma\left(\Xi_{3,k}-\Xi_{4,l}\right)}\left(\frac{\chi_d}{\mu_{d,r}}\right)^{\Xi_{3,k}-1}.\end{aligned} \tag{53}$$

A. IMPACT OF RF LINK PARAMETERS

1) FADING SEVERITY

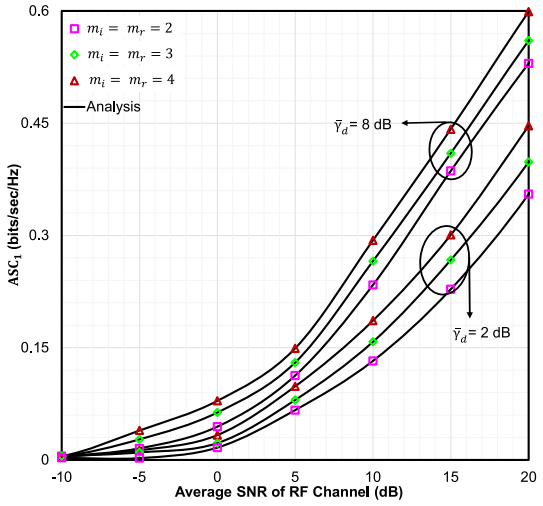

FIGURE 2. The ASC against $\bar{\gamma}_r$ for certain values of m_i, m_r, and $\bar{\gamma}_d$.

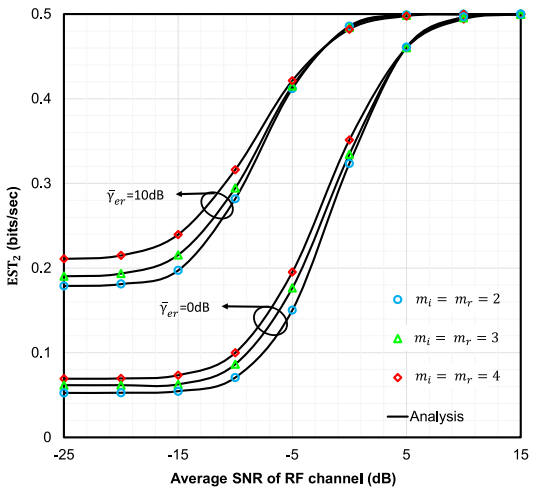

FIGURE 3. The EST against $\bar{\gamma}_r$ for selected values of m_i, m_r, and $\bar{\gamma}_{er}$.

To examine the impact of the shape parameters on secrecy performance, the ASC_1, EST_2, and SOP_1 are plotted against $\bar{\gamma}_r$ for chosen values of various fading parameters (i.e., m_i, m_r, and m_{er}) in Figs. 2, 3, and 4. Any equal rise in m_i and m_r raises the ASC (Fig. 2) and the EST (Fig. 3) for scenario-i and scenario-ii as the fading parameters (i.e., m_i and m_r) having a larger value of $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$-$\mathcal{R}$ link causes the entire fading of the associated connection to be reduced by improving the received SNR at $\mathcal{R}$, as said in [59]. The absolute similarity between the simulated and analytical outcomes assures that our generated expressions are flawless. Figure 4 is depicted to experience the effect m_i and m_{er}. It is noted that the rise in values of the fading parameters of the $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$-$\mathcal{E}_r$ link results in reduced system secrecy which is given by lower outage performance. In that particular scenario, increasing m_i and m_{er} leads to a better eavesdropper link, hence the SOP increases. A similar result is also experienced in [59]. The impact of Average SNRs of the eavesdropper and FSO links can also be seen in Figs. 2, 3, and 4, where it is noticed that the secrecy performance is enhanced with increasing $\bar{\gamma}_d$ as well as decreasing $\bar{\gamma}_{er}$. This is because the main link improves for the former case and the wiretap link improves for the latter one.

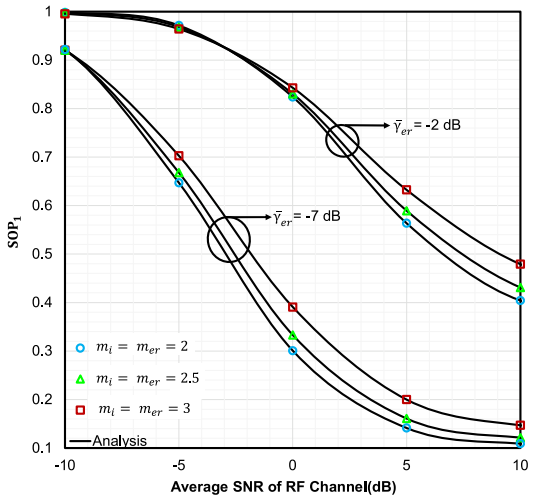

FIGURE 4. The SOP against $\bar{\gamma}_r$ for specific values of m_i, m_{er}, and $\bar{\gamma}_{er}$.

2) SCALE PARAMETERS

Scale parameters (i.e., Ω_i and Ω_r), in addition to the fading parameters, as shown in Figs. 5 and 6 (scenario-i) also play an important role in improving the system's secrecy performance and functioning, where EST_1 and $SPSC_1$ is plotted versus $\bar{\gamma}_r$. It was clearly observed in Fig. 5 that equal increases in Ω_i and Ω_r improve the EST performance as a fact of the main RF link being better due to a reduction in fading. Figure 6 displays almost similar results about the effects of scale parameters as the previous figure which reveals that an equal decrease in Ω_i, and Ω_{er} enhances the SPSC value, hence better secrecy output is obtained. This occurs since lower Ω_i and Ω_{er} signifies a weaker $\mathcal{S}$-$\mathcal{I}_\mathcal{S}$-$\mathcal{E}_r$ link.

3) NUMBER OF REFLECTING ELEMENTS

To determine the influence of the total number of reflecting elements (i.e., N) in $\mathcal{I}_\mathcal{S}$, the ASC_1 (scenario$-i$) and the $SPSC_3$ (scenario$-iii$) are plotted against $\bar{\gamma}_r$ in Fig. 7 and Fig. 8. It can be seen that with a greater value of N, system performance in terms of ASC and SPSC improves reasonably as N helps to reflect the incoming signals in a manner that enhances the signal strength, making it possible to extend the range of communication or improve the signal quality enabling the formation of directional beams. System security cannot be improved until a sufficient amount of reflecting elements are present in $\mathcal{I}_\mathcal{S}$ for $\mathcal{S} - \mathcal{I}_\mathcal{S} - \mathcal{R}$ link. It is noteworthy that, the RIS system is passive, hence it does not need any

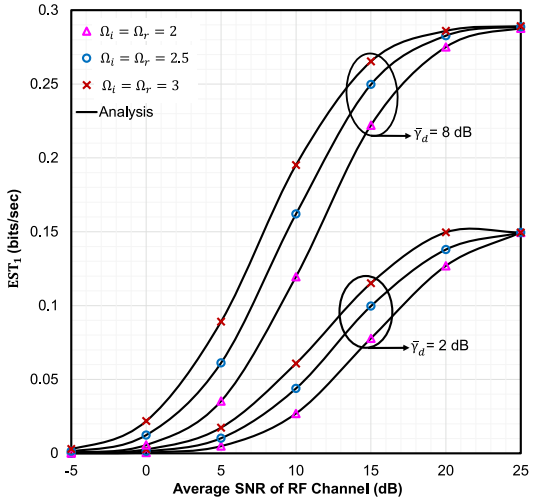

FIGURE 5. The EST against $\bar{\gamma}_r$ for certain values of Ω_i, Ω_r, and $\bar{\gamma}_d$.

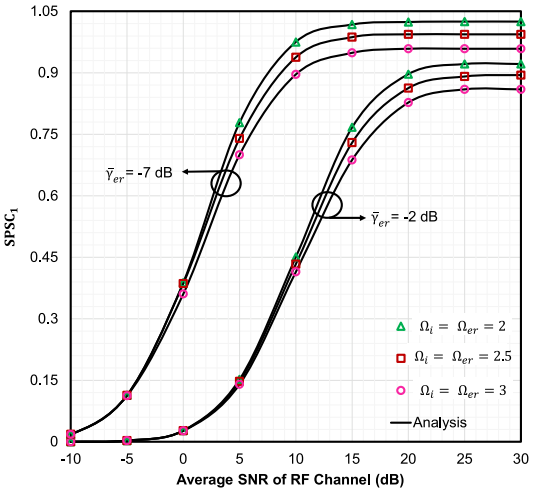

FIGURE 6. The SPSC over $\bar{\gamma}_r$ for selected values of Ω_i, Ω_{er}, and $\bar{\gamma}_{er}$.

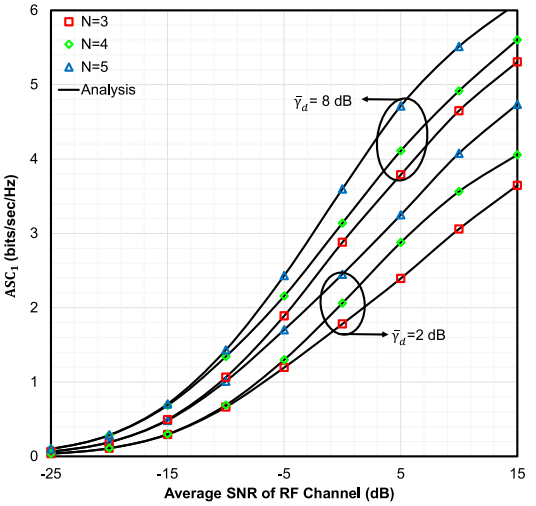

FIGURE 7. The ASC against $\bar{\gamma}_r$ for specific values of N and $\bar{\gamma}_d$.

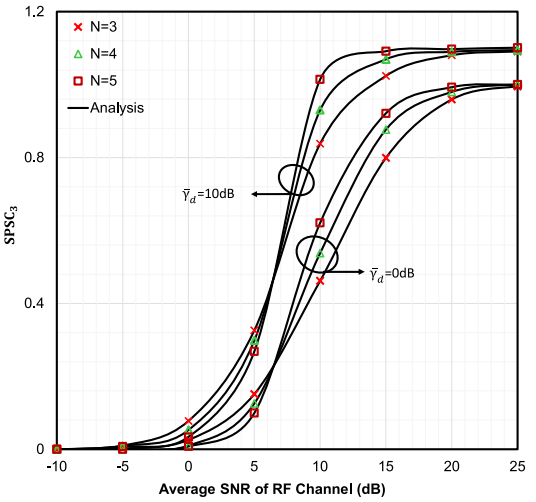

FIGURE 8. The SPSC against $\bar{\gamma}_r$ for the selected values of N and $\bar{\gamma}_d$.

additional power supply, making it highly energy efficient for our suggested model.

B. SECURITY AND EFFICIENCY TRADE-OFF

The EST_1 and EST_3 are plotted against T_s in Fig. 9 and 10 for scenario$-i$ and scenario$-iii$ respectively, to observe the impact of target secrecy rate changes on the secrecy performance of the system which also represents the trade-off between the resources required to maintain security and the rate at which secured information may be transmitted over a communication system. It is observed in Figs. 9 and 10 that the curve has a concave down shape, i.e., EST may increase or decrease with T_s. When T_s is lower, the desired secrecy level can be maintained with lower resources which results in a higher EST. As T_s rises, the desired degree of security will need more resources to encounter increasing secrecy threats, causing the EST to fall. To sum up, the graph represents the reduced benefits from stronger security measures and the decreasing gain in terms of EST.

C. IMPACTS OF FSO LINK PARAMETERS

1) POINTING ERROR

In order to conduct secure communication, the directional property of the beam must be maintained so that the transmitted beam can be prevented from spreading in an unintended propagation path. Since the transmitting and receiving apertures are misaligned, there occurs a pointing error, the beam deviates from its actual propagation direction, leading to a portion of the information being leaked to eavesdroppers, which is observed in Fig. 11-12 by plotting SOP_1, SOP_2 and in Fig. 13 by showing EST_1 against $\bar{\gamma}_d$. It is noted that the secrecy performance is greatly influenced by a strong pointing error ($\epsilon = 1.1$) compared to a weaker pointing error ($\epsilon = 6.7$) which is also testified in [44]. As the pointing error increases, more information

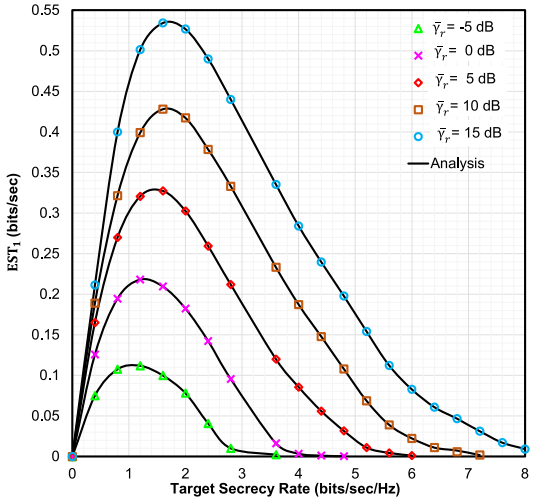

FIGURE 9. The EST over T_S for some specific values of $\bar{\gamma}_r$.

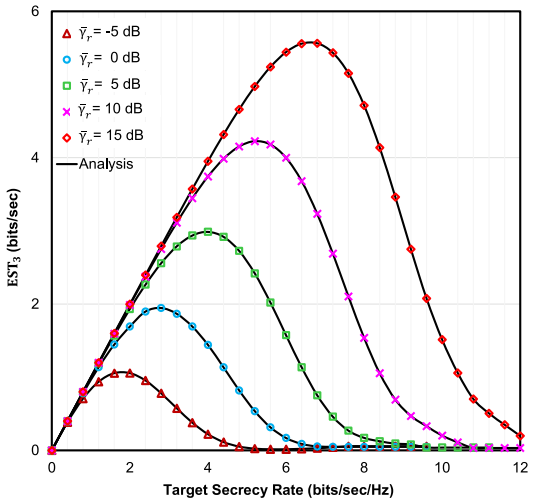

FIGURE 10. The EST over T_S for some specific values of $\bar{\gamma}_r$.

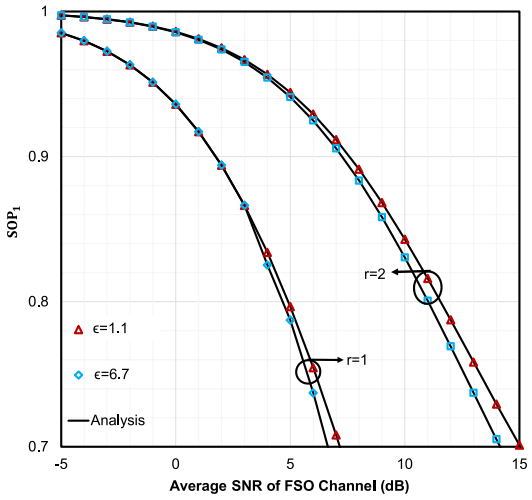

FIGURE 11. The SOP against $\bar{\gamma}_d$ for different values of ϵ and r.

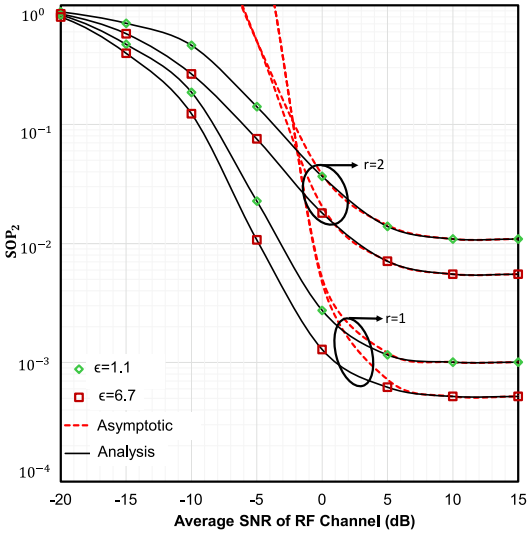

FIGURE 12. The SOP versus $\bar{\gamma}_r$ under different values of ϵ and r.

is leaked, thereby the secrecy performance is degraded of the system. Asymptotic SOP analysis is also carried out in Fig. 12, demonstrating significant agreement between all of the outcomes at high SNR ranges when the signal power dominates over the noise power.

2) DETECTION TECHNIQUES

The impacts of the two detection techniques are also shown in Fig. 11, 12 and 13 in terms of SOP_1, SOP_2 and EST_1 which indicate a better-achieved secrecy capacity utilizing the HD technique ($r = 1$) as opposed to the IM/DD technique ($r = 2$). It can be said that the HD method is capable of shifting the frequency of the signal to a higher frequency range for which the received SNR at $\mathcal{D}$ will also be high with reduced interference effects and a lower bit error rate. Hence, eavesdroppers will find it hard to wiretap confidential information. However, the IM/DD method includes the transmission of the signal at the original frequency, thereby wiretapping becomes much easier for the eavesdroppers.

3) ATMOSPHERIC TURBULENCE

The impact of different turbulence conditions (i.e. strong ($\alpha = 2.29, \beta = 2$), moderate ($\alpha = 4.2, \beta = 3$), and weak ($\alpha = 8.1, \beta = 4$)) turbulence are respectively shown in Figs.14, and 15 by plotting SOP_1 and $SPSC_1$ against $\bar{\gamma}_r$ and $\bar{\gamma}_d$. We may notice that the security of the system degrades with the growing turbulence level. This is due to atmospheric turbulence being responsible for the intensity and phase changes of the transmitted light signal resulting in significant degradation of the SNR at $\mathcal{D}$. Furthermore, the transmitted signal spreads and scatters around a wide area, and eavesdroppers can easily wiretap this portion of the signal followed by a deteriorated secrecy performance. In addition to analytical and simulation results, asymptotic

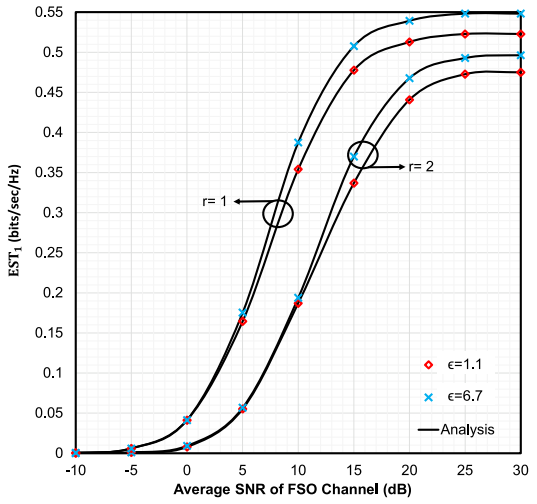

FIGURE 13. The EST versus $\bar{\gamma}_d$ for certain values of ϵ and r.

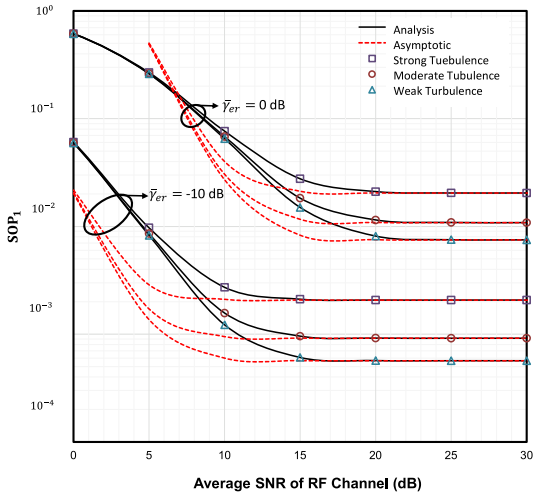

FIGURE 14. The SOP over $\bar{\gamma}_r$ showing different turbulence conditions.

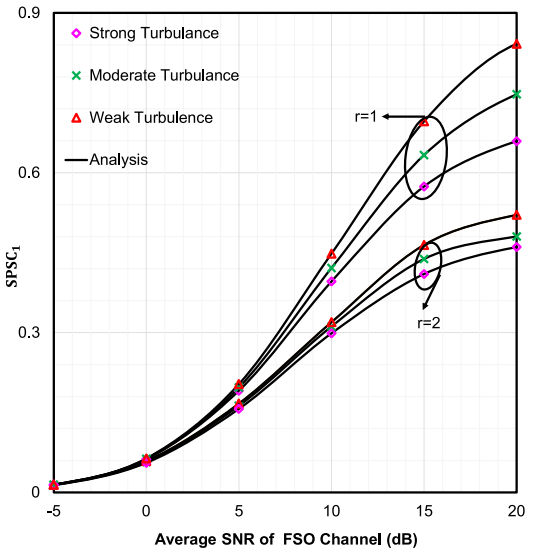

FIGURE 15. The SPSC vs. $\bar{\gamma}_d$ showing various turbulence conditions and receiver detection techniques (r).

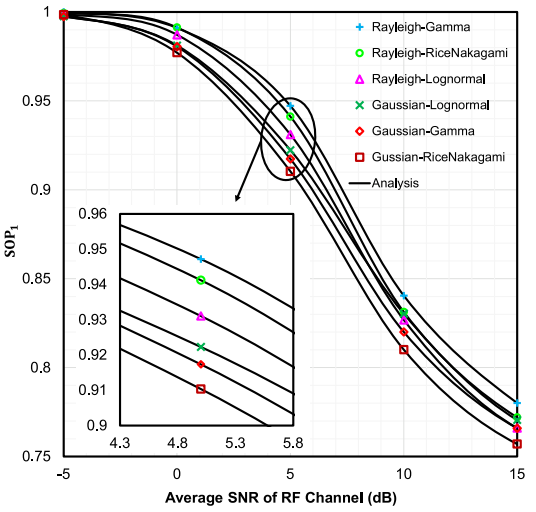

FIGURE 16. The SOP against $\bar{\gamma}_r$ showing the generalized nature of the proposed model.

SOP analysis is also performed in Fig. 14 indicating a good agreement between all of the results at high SNR regime where the signal power dominates over the noise power, and the noise contribution becomes relatively insignificant. As a result, the system behavior is mainly determined by the signal characteristics. Such analysis can focus on the dominant signal components, leading to simpler and more accurate approximations. Besides, at high SNR, the impact of the channel fading or impairments can be diminished and the channel conditions become more deterministic, allowing the use of simplified channel models.

Comparison with Existing Related Literature: By plotting the SOP_1 against $\bar{\gamma}_r$ using the generalized properties of our considered channel models, as shown in Figure 16, we can observe that our proposed model provides a unified performance analysis for a wide range of RIS-aided RF-FSO mixed models under various fading distributions. Our models can also transform various other popular channels as shown in Fig. 16. To analyze the complete security of a RIS-aided system, we consider three different scenarios. For this reason, the novel asymptotic and closed-form expressions of key performance metrics including ASC, the lower bound of SOP, the probability of SPSC, and EST are deduced. These expressions, different from existing literature, reflect our deepened understanding of the system. Utilizing these expressions, a fair comparison of scenario$-i$, scenario$-ii$ and scenario$-iii$ in terms of SOP for our suggested system model are demonstrated in Fig. 17. An FSO link is typically believed to be more secure and less vulnerable to eavesdropping than an RF link [60]. This conclusion is justified by our research in Fig.17, where SOP_2 (scenario$-ii$) has the lowest outage probability in between the three scenarios. Given that an RF link tends to be more susceptible to eavesdropping than an

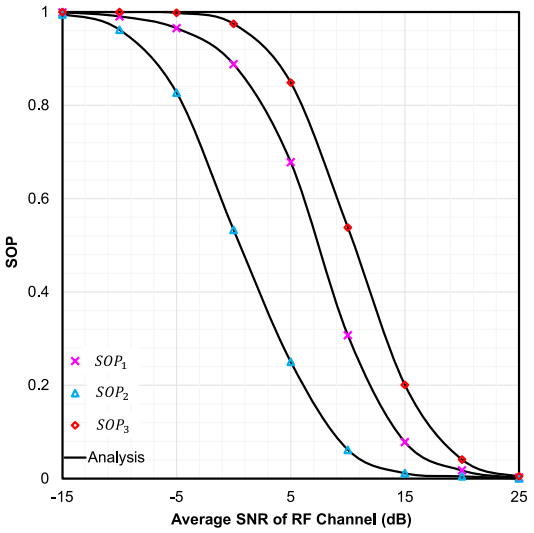

FIGURE 17. The SOP against $\bar{\gamma}_r$ showing the comparison between proposed scenarios.

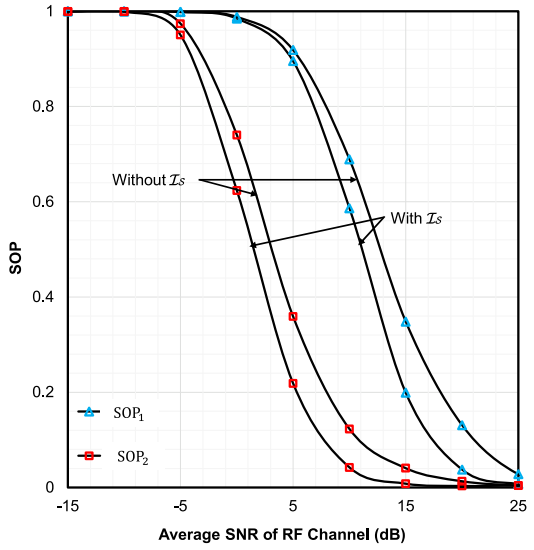

FIGURE 18. The SOP against $\bar{\gamma}_r$ showing the comparison of secrecy performance with and without the presence of $\mathcal{I}_{\mathcal{S}}$.

FSO link which is demonstrated by SOP_1 (scenario$-i$) being greater than SOP_2 (scenario$-ii$). The worst-case scenario in terms of secrecy is shown as SOP_3 (scenario$-iii$) due to the reason of simultaneous eavesdropping.

In Fig. 18, we examine the influence of RIS on secrecy performance. To this end, we plot the SOP against $\bar{\gamma}_r$ under scenario$-i$ and scenario$-ii$. It is evident that, in both instances (RF and FSO eavesdropping), the integration of RIS within the RF-FSO mixed system yields superior secrecy performance. This is attributed to the RIS elements' capability to concentrate and steer electromagnetic waves, resulting in heightened SNR and expanded coverage areas. Consequently, this enhancement translates to an overall improvement in secrecy performance.

VI. CONCLUSION

The study assessed the security performance of a dual-hop RIS-aided system using both RF and FSO connections in an effort to prevent any unauthorized access. To accomplish this task, the asymptotic and closed-form expressions for the ASC, lower bound SOP, probability of SPSC, and EST are derived by the authors. Monte-Carlo simulations confirmed the accuracy of these expressions. The influence of the system parameters being carefully observed, such as fading severity, atmospheric conditions, detection techniques at the receiver, etc., on the system performance, revealed that the proposed model can effectively secure confidential information. The numerical results also give significant insight into the efficiency of RIS in enhancing security in wireless communications which is useful for the design engineers in modeling RIS-empowered secure networks.

REFERENCES

[1] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334–366, 2021.

[2] Y. Zhou, L. Tian, L. Liu, and Y. Qi, "Fog computing enabled future mobile communication networks: A convergence of communication and computing," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 20–27, May 2019.

[3] M. K. Ghosh, M. K. Kundu, M. Ibrahim, A. S. M. Badrudduza, M. S. Anower, I. S. Ansari, A. A. Shaikhi, and M. A. Mohandes, "Secrecy outage analysis of energy harvesting relay-based mixed UOWC-RF network with multiple eavesdroppers," 2023, *arXiv:2302.10257*.

[4] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[5] T. Wang, G. Chen, M.-A. Badiu, and J. P. Coon, "Performance analysis of RIS-assisted large-scale wireless networks using stochastic geometry," *IEEE Trans. Wireless Commun.*, early access, Mar. 8, 2023, doi: 10.1109/TWC.2023.3250667.

[6] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021.

[7] Z. Lu, X. Yue, S. Chen, and W. Ma, "Performance analysis of RIS aided NOMA networks with hardware impairments," *IET Commun.*, vol. 16, no. 13, pp. 1606–1616, Aug. 2022.

[8] Y. Zhang, J. Zhang, M. D. Renzo, H. Xiao, and B. Ai, "Performance analysis of RIS-aided systems with practical phase shift and amplitude response," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4501–4511, May 2021.

[9] L. Yang, F. Meng, J. Zhang, M. O. Hasna, and M. D. Renzo, "On the performance of RIS-assisted dual-hop UAV communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10385–10390, Sep. 2020.

[10] T. N. Do, G. Kaddoum, T. L. Nguyen, D. B. da Costa, and Z. J. Haas, "Multi-RIS-aided wireless systems: Statistical characterization and performance analysis," *IEEE Trans. Commun.*, vol. 69, no. 12, pp. 8641–8658, Dec. 2021.

[11] D. Selimis, K. P. Peppas, G. C. Alexandropoulos, and F. I. Lazarakis, "On the performance analysis of RIS-empowered communications over Nakagami-*m* fading," *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2191–2195, Jul. 2021.

[12] P. Xu, W. Niu, G. Chen, Y. Li, and Y. Li, "Performance analysis of RIS-assisted systems with statistical channel state information," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 1089–1094, Jan. 2022.

[13] L. Yang, P. Li, Y. Yang, S. Li, I. Trigui, and R. Ma, "Performance analysis of RIS-aided networks with co-channel interference," *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 49–53, Jan. 2022.

[14] A. Bhowal and S. Aïssa, "RIS-aided communications in indoor and outdoor environments: Performance analysis with a realistic channel model," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13356–13360, Dec. 2022.

[15] A. Hemanth, K. Umamaheswari, A. C. Pogaku, D.-T. Do, and B. M. Lee, "Outage performance analysis of reconfigurable intelligent surfaces-aided NOMA under presence of hardware impairment," *IEEE Access*, vol. 8, pp. 212156–212165, 2020.

[16] Z. Liu, X. Yue, C. Zhang, Y. Liu, Y. Yao, Y. Wang, and Z. Ding, "Performance analysis of reconfigurable intelligent surface assisted two-way NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13091–13104, Dec. 2022.

[17] T. Wang, M.-A. Badiu, G. Chen, and J. P. Coon, "Outage probability analysis of STAR-RIS assisted NOMA network with correlated channels," *IEEE Commun. Lett.*, vol. 26, no. 8, pp. 1774–1778, Aug. 2022.

[18] R. P. Naik and W.-Y. Chung, "Evaluation of reconfigurable intelligent surface-assisted underwater wireless optical communication system," *J. Lightw. Technol.*, vol. 40, no. 13, pp. 4257–4267, Jul. 1, 2022.

[19] A. S. M. Badrudduza, M. Ibrahim, S. M. R. Islam, M. S. Hossen, M. K. Kundu, I. S. Ansari, and H. Yu, "Security at the physical layer over GG fading and mEGG turbulence induced RF-UOWC mixed system," *IEEE Access*, vol. 9, pp. 18123–18136, 2021.

[20] L. Qu, G. Xu, Z. Zeng, N. Zhang, and Q. Zhang, "UAV-assisted RF/FSO relay system for space-air-ground integrated network: A performance analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 6211–6225, Aug. 2022.

[21] Z. Zhang, Q. Sun, M. López-Benítez, X. Chen, and J. Zhang, "Performance analysis of dual-hop RF/FSO relaying systems with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4965–4976, May 2022.

[22] A. Asgari-Forooshani, M. Aghabozorgi, E. Soleimani-Nasab, and M. A. Khalighi, "Performance analysis of mixed RF/FSO cooperative systems with wireless power transfer," *Phys. Commun.*, vol. 33, pp. 187–198, Apr. 2019.

[23] B. Ashrafzadeh, E. Soleimani-Nasab, A. Zaimbashi, and M. Uysal, "Outage performance of mixed RF-FSO systems over DGG and Nakagami-*m* channels," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2135–2139, Dec. 2020.

[24] K. O. Odeyemi, G. Aiyetoro, P. A. Owolawi, and O. O. Olakanmi, "Performance analysis of reconfigurable intelligent surface in a dual-hop DF relay empowered asymmetric RF/FSO networks," *Opt. Quantum Electron.*, vol. 53, no. 11, Nov. 2021.

[25] L. Yang, W. Guo, and I. S. Ansari, "Mixed dual-hop FSO-RF communication systems through reconfigurable intelligent surface," *IEEE Commun. Lett.*, vol. 24, no. 7, pp. 1558–1562, Jul. 2020.

[26] S. Li, L. Yang, D. B. da Costa, M. D. Renzo, and M.-S. Alouini, "On the performance of RIS-assisted dual-hop mixed RF-UWOC systems," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 2, pp. 340–353, Jun. 2021.

[27] H. Wang, Z. Zhang, B. Zhu, J. Dang, and L. Wu, "Performance analysis of hybrid RF-reconfigurable intelligent surfaces assisted FSO communication," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13435–13440, Dec. 2022.

[28] A. Sikri, A. Mathur, and G. Kaddoum, "Signal space diversity-based distributed RIS-aided dual-hop mixed RF-FSO systems," *IEEE Commun. Lett.*, vol. 26, no. 5, pp. 1066–1070, May 2022.

[29] M. P. Ninos, P. Mukherjee, C. Psomas, and I. Krikidis, "Dual-hop full-duplex DF relay channel with parallel hybrid RF/FSO links," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[30] K. O. Odeyemi, P. A. Owolawi, and O. O. Olakanmi, "On the performance of reconfigurable intelligent surface in cooperative decode-and-forward relaying for hybrid RF/FSO systems," *Prog. Electromagn. Res. M*, vol. 110, pp. 157–169, 2022.

[31] M. Ibrahim, M. Z. I. Sarkar, A. S. M. Badrudduza, M. K. Kundu, and S. Dev, "Impact of correlation on the security in multicasting through κ-μ shadowed fading channels," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Jun. 2020, pp. 1396–1399.

[32] L. Yang, W. Zhang, P. S. Bithas, H. Liu, M. O. Hasna, T. A. Tsiftsis, and D. W. K. Ng, "Covert transmission and secrecy analysis of RS-RIS-NOMA-aided 6G wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10659–10670, Aug. 2023.

[33] K. An, T. Liang, X. Yan, and G. Zheng, "On the secrecy performance of land mobile satellite communication systems," *IEEE Access*, vol. 6, pp. 39606–39620, 2018.

[34] 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.

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

[36] I. Trigui, W. Ajib, and W.-P. Zhu, "Secrecy outage probability and average rate of RIS-aided communications using quantized phases," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1820–1824, Jun. 2021.

[37] F. Zhou, X. Li, M. Alazab, R. H. Jhaveri, and K. Guo, "Secrecy performance for RIS-based integrated satellite vehicle networks with a UAV relay and MRC eavesdropping," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 2, pp. 1676–1685, Feb. 2023.

[38] 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.

[39] X. Li, Y. Zheng, M. Zeng, Y. Liu, and O. A. Dobre, "Enhancing secrecy performance for STAR-RIS NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684–2688, Feb. 2023.

[40] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks," *IEEE Access*, vol. 9, pp. 42583–42592, 2021.

[41] X. Zhao and J. Sun, "Secure reconfigurable intelligent surface aided heterogeneous VLC-RF cooperative NOMA networks," *Opt. Commun.*, vol. 511, May 2022, Art. no. 127983.

[42] M. R. A. Ruku, M. Ibrahim, A. S. M. Badrudduza, and I. S. Ansari, "Effects of co-channel interference on RIS empowered wireless networks amid multiple eavesdropping attempts," 2023, *arXiv:2302.10876*.

[43] 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.

[44] M. Ibrahim, A. S. M. Badrudduza, Md. S. Hossen, M. K. Kundu, I. S. Ansari, and I. Ahmed, "On effective secrecy throughput of underlay spectrum sharing α-μ/Málaga hybrid model under interference-and-transmit power constraints," *IEEE Photon. J.*, vol. 15, no. 2, pp. 1–13, Apr. 2023.

[45] S. H. Islam, A. S. M. Badrudduza, S. M. R. Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, and H. Yu, "Impact of correlation and pointing error on secure outage performance over arbitrary correlated Nakagami-*m* and $\mathcal{M}$-turbulent fading mixed RF-FSO channel," *IEEE Photon. J.*, vol. 13, no. 2, pp. 1–17, Apr. 2021.

[46] T. Hossain, S. Shabab, A. S. M. Badrudduza, M. K. Kundu, and I. S. Ansari, "On the physical layer security performance over RIS-aided dual-hop RF-UOWC mixed network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2246–2257, Feb. 2023.

[47] E. Erdogan, I. Altunbas, N. Kabaoglu, and H. Yanikomeroglu, "A cognitive radio enabled RF/FSO communication model for aerial relay networks: Possible configurations and opportunities," *IEEE Open J. Veh. Technol.*, vol. 2, pp. 45–53, 2021.

[48] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "A weather-dependent hybrid RF/FSO satellite communication for improved power efficiency," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 573–577, Mar. 2022.

[49] M. Ibrahim, A. S. M. Badrudduza, M. S. Hossen, M. K. Kundu, and I. S. Ansari, "Enhancing security of TAS/MRC-based mixed RF-UOWC system with induced underwater turbulence effect," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5584–5595, Dec. 2022.

[50] M. H. Samuh, A. M. Salhab, and A. H. A. El-Malek, "Performance analysis and optimization of RIS-assisted networks in Nakagami-*m* environment," 2020, *arXiv:2010.07841*.

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

[52] D. Zwillinger and A. Jeffrey, *Table of Integrals, Series, and Products*. Amsterdam, The Netherlands: Elsevier, 2007.

[53] A. P. Prudnikov, Y. A. Brychkov, O. I. Marichev, and R. H. Romer, *Integrals and Series*. College Park, MD, USA: American Association of Physics Teachers, 1988.

[54] S. H. Islam, A. Badrudduza, S. R. Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, and H. Yu, "Impact of correlation and pointing error on secure outage performance over arbitrary correlated Nakagami-*m* and turbulent fading mixed RF-FSO channel," *IEEE Photon. J.*, vol. 13, no. 2, pp. 1–17, 2021.

[55] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, pp. 1–17, Dec. 2020.
[56] S. H. Islam, A. S. M. Badrudduza, S. M. Riazul Islam, F. I. Shahid, I. S. Ansari, M. K. Kundu, S. K. Ghosh, M. B. Hossain, A. S. M. S. Hosen, and G. H. Cho, "On secrecy performance of mixed generalized gamma and Málaga RF-FSO variable gain relaying channel," *IEEE Access*, vol. 8, pp. 104127–104138, 2020.
[57] N. H. Juel, A. S. M. Badrudduza, S. M. R. Islam, S. H. Islam, M. K. Kundu, I. S. Ansari, M. M. Mowla, and K.-S. Kwak, "Secrecy performance analysis of mixed α-μ and exponentiated Weibull RF-FSO cooperative relaying system," *IEEE Access*, vol. 9, pp. 72342–72356, 2021.
[58] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, Jul. 1990, pp. 212–224.
[59] A. K. Yadav, S. Yadav, A. Pandey, and A. Silva, "On the secrecy performance of RIS-enabled wireless communications over Nakagami-*m* fading channels," *ICT Exp.*, vol. 9, no. 3, pp. 452–458, Jun. 2023.
[60] N. A. Sarker, A. S. M. Badrudduza, M. K. Kundu, I. S. Ansari, and I. Ahmed, "Effects of eavesdropper on the performance of mixed η-μ and DGG cooperative relaying system," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4627–4638, Sep. 2023.

TAHMID AHMED is currently pursuing the Bachelor of Science (B.Sc.) degree in electronics and telecommunication engineering (ETE) with the Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh. His research interests include FSO communication and physical layer security.

A. S. M. BADRUDDUZA (Member, IEEE) received the Bachelor of Science (B.Sc.) and Master of Science (M.Sc.) degrees in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh, in 2016 and 2019, respectively. From September 2016 to July 2017, he was a Lecturer with the Department of EEE, Bangladesh Army University of Engineering & Technology (BAUET), Natore, Rajshahi. From July 2017 to June 2020, he was a Lecturer with the Department of Electronics and Telecommunication Engineering (ETE), RUET, where he has been an Assistant Professor with the Department of ETE, since June 2020. He has been affiliated with IEEE, since 2020. He is an active reviewer for several IEEE journals and transactions. He has authored/coauthored more than 40 international journals/conference publications. His research interests include physical layer security in multicast, cellular and cooperative networks, free space optics (FSO), underwater optics (UWO), and NOMA systems.

Mr. Badrudduza was a recipient of two EEE Association Awards (Student of the Year Award) from RUET for his outstanding academic performances in the first and fourth-year examinations, while pursuing the B.Sc. degree in engineering and three Best Paper Awards for three different research papers from IEEE Region 10 Symposium (TENSYMP2020), IEEE Third International Conference on Telecommunication and Photonics (ICTP2019), and International Conference on Electrical, Computer and Communication Engineering (ECCE 2023).

S. M. RIAZUL ISLAM (Senior Member, IEEE) received the Ph.D. degree in information engineering. He is currently an Associate Professor (a Senior Lecturer) in computing science with the University of Aberdeen, U.K. Before that, he was with the University of Huddersfield as a Senior Lecturer in computer science. His academic journey also includes the role of an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, South Korea, from 2017 to 2022. His prior affiliations were with Inha University as a Postdoctoral Fellow, Samsung Research and Development Institute as a Senior Engineer, and University of Dhaka as an Assistant Professor in EEE. His research interests include applied artificial intelligence (AI), digital health, machine learning, data science, and the IoT & security. He has authored more than 100 publications in peer-reviewed international journals.

He received the Distinguished Research Professor Award 2020 from Sejong University. He is a fellow of the Higher Education Academy (FHEA).

SHEIKH HABIBUL ISLAM received the bachelor's degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering & Technology (RUET), Bangladesh. He is currently pursuing the Ph.D. degree with University of Massachusetts Lowell, USA. His research interests include machine learning-based full-duplex wireless communication, alongside his continued investigations into FSO communication, physical layer security, and NOMA systems. With this multidisciplinary research agenda, he showcases his dedication to advancing various areas of wireless communication.

MD. IBRAHIM (Graduate Student Member, IEEE) received the Bachelor of Science (B.Sc.) degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh, in 2021. From September 2021 to December 2021, he was a Lecturer with the Department of EEE, Varendra University (VU), Rajshahi. He has been a Lecturer with the Institute of Information and Communication Technology (ICT), RUET, since December 2021. He has been affiliated with IEEE, since 2022. He is an active reviewer for several IEEE journals. His current research interests include free-space optics communication, physical layer security, underwater communications, cognitive radio networks, and NOMA systems.

M. ABDULLAH-AL-WADUD (Member, IEEE) received the B.S. degree in computer science and the M.S. degree in computer science and engineering from the University of Dhaka, Bangladesh, in 2003 and 2004, respectively, and the Ph.D. degree in computer engineering from Kyung Hee University, South Korea, in 2009. He was a Faculty Member with the Department of Industrial and Management Engineering, Hankuk University of Foreign Studies, South Korea, from 2009 to 2014. He was also a Lecturer with the Faculty of Sciences and Information Technology, Daffodil International University, Bangladesh, in 2003, and the Faculty of Sciences and Engineering, East West University, Bangladesh, in 2004. He is currently an Associate Professor with the Department of Software Engineering, King Saud University, Saudi Arabia. His research interests include pattern recognition, optimization, computer vision, cloud computing, recommender systems, sensor, and ad hoc networks.

IMRAN SHAFIQUE ANSARI (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer engineering from the King Fahd University of Petroleum and Minerals (KFUPM), in 2009, and the M.Sc. and Ph.D. degrees from the King Abdullah University of Science and Technology (KAUST), in 2010 and 2015, respectively.

Since August 2018, he has been a Lecturer (an Assistant Professor) with the University of Glasgow, Glasgow, U.K. Prior to this, from November 2017 to July 2018, he was a Lecturer (an Assistant Professor) with the Global College of Engineering and Technology (GCET) (affiliated with University of the West of England (UWE), Bristol, U.K.). From April 2015 to November 2017, he was a Postdoctoral Research Associate (PRA) with Texas A&M University at Qatar (TAMUQ). From May 2009 to August 2009, he was a Visiting Scholar with Michigan State University (MSU), East Lansing, MI, USA, and from June 2010 to August 2010, he was a Research Intern with Carleton University, Ottawa, ON, Canada. He has authored/coauthored more than 100 journals and conference publications. He has co-organized the GRASNET'2016, 2017, and 2018 workshops in conjunction with IEEE WCNC'2016, 2017, and IEEE GLOBECOM 2018. His current research interests include free-space optics (FSO), underwater communications, physical layer secrecy issues, full duplex systems, and secure D2D applications for 5G+ systems, among others.

Dr. Ansari has been affiliated with IEEE and IET, since 2007. He has served in various capacities. He was served on the IEEE Nominations and Appointments (N&A) Committee (2020–2021) and IEEE Communication Society Young Professionals (ComSoc YP) Board, since April 2016. He has been a part of the IEEE 5G Tech Focus Publications Editorial Board, since February 2017. He was served as the Past-Chair for the IET Young Professionals Communities Committee (YPCC), from October 2020 to September 2021. He has served on the IET Satellites Technical Network (TN), from March 2016 to September 2020. He has served on the IET CC-EMEA (Communities Committee-Europe, Middle-East and Africa) for two complete terms, from October 2015 to September 2018 and from October 2010 to September 2013. He is an active reviewer for various IEEE TRANSACTIONS and various other journals. He has served as a TPC for various IEEE conferences. He was a recipient of appreciation of an Exemplary Reviewer of IEEE TRANSACTION ON COMMUNICATIONS, in 2018 and 2016, a recipient of appreciation of an Exemplary Reviewer of IEEE WIRELESS COMMUNICATIONS LETTERS, in 2017 and 2014, a recipient of TAMUQ ECEN Research Excellence Award, in 2016 and 2017, a recipient of Recognized Reviewer Certificate by *Optics Communications* (Elsevier), in 2015, a recipient of Recognized Reviewer Certificate by OSA Publishing, in 2014, a recipient of Postdoctoral Research Award (PDRA) (first cycle) with Qatar National Research Foundation (QNRF), in 2014, a recipient of KAUST Academic Excellence Award (AEA), in 2014, and a recipient of IEEE Richard E. Merwin Student Scholarship Award, in July 2013.