IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2020, accepted July 6, 2020, date of publication July 13, 2020, date of current version July 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009026

Secrecy Performance Analysis of Mixed Hyper-Gamma and Gamma-Gamma Cooperative Relaying System

NOOR AHMAD SARKER[1], A. S. M. BADRUDDUZA[1], S. M. RIAZUL ISLAM[2], (Member, IEEE), SHEIKH HABIBUL ISLAM[3], IMRAN SHAFIQUE ANSARI[4], (Member, IEEE), MILTON KUMAR KUNDU[5], (Member, IEEE), MST. FATEHA SAMAD[1], MD. BIPLOB HOSSAIN[6], AND HEEJUNG YU[7], (Member, IEEE)

[1]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology (RUET), Rajshahi 6204, Bangladesh
[2]Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
[3]Department of Electrical and Electronic Engineering, RUET, Rajshahi 6204, Bangladesh
[4]James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.
[5]Department of Electrical and Computer Engineering, RUET, Rajshahi 6204, Bangladesh
[6]Department of Electrical and Electronic Engineering, Jashore University of Science and Technology (JUST), Jashore 7408, Bangladesh
[7]Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea

Corresponding authors: A. S. M. Badrudduza (asmb.kanon@gmail.com) and Heejung Yu (heejungyu@korea.ac.kr)

(Noor Ahmad Sarker, A. S. M. Badrudduza, and S. M. Riazul Islam are co-first authors.)

This work was supported in part by the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT under Grant 2019R1A2C1083988, and in part by the Ministry of Science and ICT (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program supervised by the Institute for Information and communications Technology Promotion (IITP) under Grant IITP-2020-2016-0-00313.

ABSTRACT In this paper, we investigate a secure dual-hop radio frequency-free space optical (RF-FSO) mixed variable gain relaying framework in the presence of a single eavesdropper. The RF and FSO links are modeled with hyper Gamma (HG) and Gamma-Gamma ($\Gamma\Gamma$) fading channels, respectively. We assume that the eavesdropper utilizes another HG fading channel to wiretap the transmitted confidential data from the RF link. Our key concern is to defend this information against passive eavesdropping. We carry out the secrecy measurements by deriving closed-form mathematical expressions of average secrecy capacity (ASC), secure outage probability (SOP), and strictly positive secrecy capacity (SPSC), all in terms of Meijer's G function. Capitalizing on the derived expressions, we analyze the impacts of atmospheric turbulence and pointing errors on the secrecy capacity and outage performance of the proposed scenario. For gaining more insights, we also analyze the asymptotic outage behaviour for high signal-to-noise ratio. Two detection techniques i.e. heterodyne (HD) and the intensity modulation with direct detection (IM/DD) are taken into consideration and our results demonstrate that HD technique notably outperforms the IM/DD scheme. The supremacy and novelty of the model is demonstrated via utilizing generic properties of the HG fading channel. Finally, we provide a justification of the derived expressions via Monte-Carlo simulations.

INDEX TERMS Gamma-Gamma fading, eavesdropper, Hyper-Gamma fading, physical layer security, pointing error, variable gain relay.

I. INTRODUCTION

A. BACKGROUND AND RELATED WORKS

Free space optical (FSO) communication is experiencing a widespread concern as part of the next generation of wireless networks due to a large number of motives such as high security, comparatively larger bandwidth, lesser physical effect relative to radio-wave or microwave in the human body etc. Moreover, FSO environment offers a wide range of license-free spectrum that makes this system cost effective. Simultaneously, this technology also paves the way to solve the spectrum scarcity problem, which is one of the major concerns of the researchers in recent times.

Over the last few years, researchers have performed ample amounts of work on the FSO system [1]–[10] whereas first analysis of FSO communication was performed in [1]

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

revealing that the spatial diversity can appreciably overcome the turbulence-induced fading. Besides this technique, error control coding was also considered as a good approach by the authors of [2], [3] for correlated K distribution and Gamma-Gamma ($\Gamma\Gamma$) turbulence models. A turbulent atmosphere with multiple receive and transmit apertures was modeled in [4] considering the presence of shot and background noises. The authors obtained an improvement in ergodic capacity (EC) when the signal-to-background ratio is low. The concept of series and parallel relaying system in FSO communication was introduced in [5] deriving the closed-form expression of outage probability (OP). The authors in [6] used the concepts of maximal ratio combining (MRC) and selective combining (SC) techniques over the FSO links and obtained the outage Shannon capacity to examine the effect of the scintillation index (SI) and number of diversity branches. In [7], the authors investigated a turbulence induced $\Gamma\Gamma$ fading FSO channel with intensity modulation and direct detection (IM/DD) technique using bit error rate (BER) expressions. The authors in [8] assumed a multiple-input multiple-output (MIMO) FSO system for multiple transmitters and receivers with misalignment and atmospheric fading. The expression of OP was demonstrated to show that if both fading are absent, then the diversity gain is directly proportional to the number of transmitters and receivers. The EC was analyzed in [9] for a FSO link with nonzero boresight pointing errors with IM/DD and heterodyne detection (HD) techniques. The authors in [10] derived the exact expressions of OP, EC, SI, average error rate (for both M-ary and binary modulation), and also asymptotic expression of EC to analyze the functioning of a Málaga turbulent FSO network. Recently, FSO is found compatible with other 5G paradigms such as advanced radio access techniques [11], [12].

Despite having huge benefits, FSO link is remarkably sensitive to pointing errors and atmospheric turbulence. To overcome these problems, the concept of mixed radio frequency (RF)-FSO system was introduced that inspired a lot of researchers around the world to investigate the behaviour of such mixed systems [13]–[33]. In a RF-FSO framework, the critical long-distanced part is generally covered by RF channel whereas the short-distanced line-of-sight (LoS) portion is covered with FSO link. The performance of a Nakagami-m-double generalized Gamma (DGG) RF-FSO communication link was considered in [13] based on both closed-form and asymptotic expressions of OP. This network was extended in [14] considering multiple amplify-and-forward (AF) relays with partial relay selection (PRS) protocol. For further extension, the impact of co-channel interference (CCI) was included in a two way relaying (TWR) system in [15]. A multihop RF-FSO link with Rician-$\Gamma\Gamma$ distribution was also analyzed in terms on OP and ergodic achievable rates in [16]. Another multihop system with low altitude aerial platform (LAP) relaying technique was designed in [17] for outage analysis. The authors in [18] modeled a RF-FSO link with a single-input multiple-output (SIMO) Nakagami-m RF link, and unified $\Gamma\Gamma$ and generalized K FSO links. They used the expressions of symbol error probability (SEP), OP, and EC to determine the effects of number of RF links. A Rayleigh-$\Gamma\Gamma$ fading communication model was taken into account in [19]–[21] obtaining expressions of average OP, BER, and EC whereas the authors of [21] adopted a TWR scheme. The authors found that EC can be almost doubled by using TWR scheme. A RF-FSO system with multiple variable gain AF relays was employed in [23]. The authors considered a Rayleigh- Málaga turbulent fading channel with pointing errors and derived the OP for PRS scheme. In [24], the performance of $\eta - \mu$-Málaga fading framework was evaluated utilizing expressions of OP, BER, and EC for both fixed and variable gain relaying schemes. The authors proved that the diversity order depends on the channel parameters, number of users, and pointing error of the FSO link. The expressions of EC and OP were obtained in [25]–[27] considering a Nakagami-m-Málaga turbulent fading channel where in [27], the authors made an extension with CCI to imply that the performance of the RF-FSO system depends on the number and power of CCI. Diversity and coding gain of a $\kappa - \mu$/Inverse Gaussian fading (IG) system was analyzed in [28] where the authors deduced the EC and BER expressions for different binary modulations. In [29], a RF-FSO scenario was modeled with multiple sources containing decode-and-forward (DF) relaying scheme. The FSO hop was backed-up with a virtual MIMO system that enhanced the system performance notably. The authors in [30] modeled the optical channels with double Weibull fading distribution employing PRS protocol for both AF and DF relaying techniques. The system performance was analyzed in terms of OP, EC, and SER for both HD and IM/DD techniques. The authors in [31] presented a DF protocol based RF-FSO system where Beaulieu-Xie fading was considered for RF path and Málaga turbulent fading with pointing errors was considered for FSO path. The authors also provided asymptotic analysis of OP, BER, and EC. An underlay cognitive RF-FSO system with multiple relays adopting PRS strategy was designed by the authors in [32]. In [33], a multiple-input single-output (MISO) RF-FSO underlay cognitive system was shown to reduce the OP based on a proposed power allocation model.

Recently, due to the vulnerability of wireless mediums to eavesdropping, physical layer security (PLS) has become a vital issue for the researchers as it can perfectly ensure a secure communication making use of time varying nature of wireless networks without utilization of any secrecy key [34], [35]. A RF-FSO system also suffers from security threat [36]–[45]. In recent times, a secure turbulent FSO link was analyzed in [36] by deriving the expression of probability of strictly positive secrecy capacity (SPSC). In [37], the authors evaluated the Málaga atmospheric turbulence impacts on the secrecy performance with an IM/DD method by determining the expressions of average secrecy capacity (ASC), secrecy outage probability (SOP), and SPSC. The authors in [38] performed the secrecy analysis of a

Nakagami-m-ΓΓ fading RF-FSO model by determining the expressions of lower bound of SOP and ASC in closed-form while considering pointing error, and HD and IM/DD techniques at the FSO receiver. The same channels were used in [39] considering multiuser scenario and in [40] considering a simultaneous wireless information and power transfer (SWIPT) system. A Nakagami-m-Málaga faded SWIPT system was employed in [41]. The authors derived the expressions of ASC and lower bound of SOP to examine the effect of multiple antennas, energy harvesting, pointing error, and detection techniques. Secrecy performance of a CCI affected multiuser RF/FSO system was analyzed in [42] for a single DF relay with opportunistic user scheduling based on the expression of OP. The SOP with imperfect CSI and error of misalignment was analyzed in [43]. The PLS employing $\eta - \mu$-Málaga fading channel was analyzed in [44] for both fixed and variable gain relaying schemes. The authors derived the expressions of SOP and average secrecy rate (ASR). The authors in [45] analyzed a secure network over Rayleigh-ΓΓ fading channels and derived the expressions of the lower bound of SOP and SPSC.

B. MOTIVATION AND CONTRIBUTIONS

The aforementioned literature disclose that PLS contemplating generalized fading channels in the RF links are very infrequent. Since the wireless channels vary frequently with time, hence assuming generalized channels in the RF link will provide more realistic secrecy analysis of wireless RF-FSO systems rather than the existing RF multipath models. On the other hand, ΓΓ fading model can also accurately make intelligible outcomes amid intense atmospheric turbulence and pointing error impairment circumstances. Inspired by these conveniences of mixed RF-FSO networks with generalized RF channels, we present a secure scenario over hyper Gamma (HG)-ΓΓ mixed RF-FSO fading channel. We also assume an eavesdropper can wiretap transmitted data utilizing RF links only. In summary:

1) We first obtain the cumulative distribution function (CDF) and probability density function (PDF) of dual-hop RF-FSO system using CDF and PDF of each individual hop. These expressions of PDF and CDF are novel compared to the existing works as HG fading is not reported in the existing RF-FSO literature. Again, some existing scenarios [38], [46] can also be achieved as our special cases because investigation of HG distribution unifies the performance evaluation of Rayleigh and Nakagami-m distributions [47].
2) We analyze the secrecy characteristics utilizing popular secrecy metrics and deduce novel expressions for ASC, SOP, and SPSC. Subsequently, we exploit these expressions to derive the numerical results with selected figures which are further verified via utilizing Monte-Carlo simulations. Besides exact expression of SOP, we also provide asymptotic expression of SOP for obtaining better insights into the outage behaviour.
3) Although in [36]–[46] similar types of secure structures are used, we demonstrate the supremacy of our analysis over these existing works. Simultaneously, we also prove with numerical and simulation results that [38] and [46] can directly be obtained as our special cases.
4) As our suggested model ascertains security at the physical layer, we exhibit all consequences regarding impacts of each parameter of the system e.g. fading, atmospheric turbulence, pointing error etc. We also offer a comparative analysis between HD and IM/DD detection methods and realize that HD outmatches the IM/DD method within secrecy performance.

The rest of the parts are organized with following arrangement. Section-II illustrates the proposed framework initiating formulation of mathematical model. Expression of the performance parameters (ASC, SOP, and SPSC) are derived in Section-III. Numerical results are explained in Section-IV. Finally, a conclusion of the whole work is provided in Section-V.

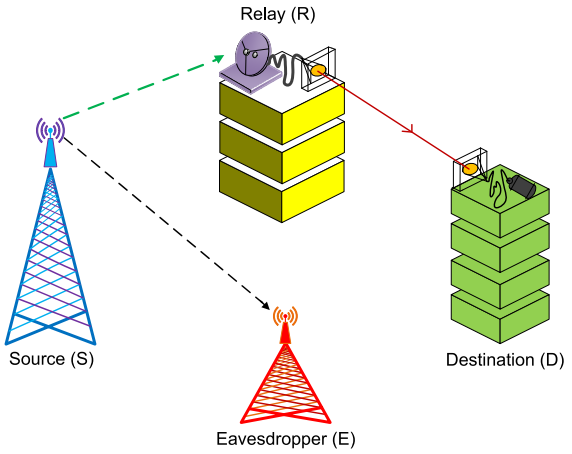


FIGURE 1. System model incorporating the source (S), relay (R), eavesdropper (E), and destination (D).

II. SYSTEM MODEL AND PROBLEM FORMULATION

We assume a mixed RF-FSO relaying system in Fig. 1, where the defined source, S (legitimate transmitter), and the destination, D, are connected with each other through a passable intermediate relay, R. We consider AF-based variable gain relaying system for our proposed framework. An eavesdropper, E, is also introduced in this model that tries to overhear the secret transmission between S and D. S has one transmit antenna whereas the relay as well as the eavesdropper have one receive antenna. For FSO communication, R has one transmit aperture and D has one receive aperture. This full communication process can be briefed into two parts of transmission. In the first part, the confidential information is sent from S to R through the radio-wave link, where E tries to intercept that information through another similar type of link. Both of the links experience independently and identically distributed (i.i.d.) HG fading. The second part of

the transmission is between R and D through FSO link which experiences ΓΓ fading turbulence with pointing error. For FSO transmission, R first converts the received RF signal into optical form and then transmit to D via FSO link.

A. SNR OF EACH LINK

We denote the instantaneous signal-to-noise ratios (SNRs) of $S-R$, $R-D$, and $S-E$ links as γ_r, γ_f, and γ_e, respectively. Mathematically, we express the SNRs as $\gamma_r = \phi_{kr}\|\alpha_r\|^2$, $\gamma_f = \phi_f\|\alpha_f\|^2$, and $\gamma_e = \phi_{ke}\|\alpha_e\|^2$, where α_r, α_f, and α_e are the channel gains, and ϕ_{kr}, ϕ_f, and ϕ_{ke} are the average SNRs of the $S-R$, $R-D$, and $S-E$ links, respectively. To find out the received SNR of the combined RF-FSO channel, the information of channel state with the approach of assisted relaying is utilized in the intermediate relay. So, the SNR for end-to-end system is given by [48, Eq. (5)]

$$\gamma_{dn} = \frac{\gamma_r\gamma_f}{\gamma_r+\gamma_f+1} \cong min\left\{\gamma_r, \gamma_f\right\}. \tag{1}$$

B. SECRECY CAPACITY

In order to maintain an uninterrupted secure transmission between S and D through R, we must transmit at secrecy rate (i.e. the rate at which the eavesdropper is unable to decrypt the confidential message). Mathematically, secrecy capacity is defined as [49, Eq. (3)]

$$\mathcal{C}_{sc} = \begin{cases} \log_2(1+\gamma_{dn}) - \log_2(1+\gamma_e), & \text{if } \gamma_{dn} > \gamma_e \\ 0, & \text{if } \gamma_{dn} \leq \gamma_e. \end{cases} \tag{2}$$

C. PDF AND CDF OF SNR FOR RF MAIN CHANNEL

Considering HG fading distribution in the link between S and R, the PDF of this channel is expressed as [47, Eq. (3)]

$$f_r(\gamma_r) = \sum_{kr=0}^{n} \frac{\zeta_{kr}}{\Gamma(P_{kr})} \mathcal{A}^{P_{kr}} {\gamma_r}^{P_{kr}-1} e^{-\mathcal{A}\gamma_r}, \tag{3}$$

where $\mathcal{A} = \frac{P_{kr}}{\phi_{kr}}$. The parameters P_{kr}, ζ_{kr}, and ϕ_{kr} denote fading severity, accruing factor of kr-th fading situation among n possible fading samples, and the average SNR of the main RF channel, respectively. For a specific condition with $1 \leq kr \leq n$, the limits of these parameters are given by $P_{kr} \geq 0.5$, $\phi_{kr} > 0$, and $0 \leq \zeta_{kr} \leq 1$. The HG is a generic model that unifies the performance of Rayleigh fading, Nakagami-m fading, and one-sided Gaussian channels. Table 1 indicates the special cases containing different multipath fadings [47]. As a result, a wide variety of channel conditions including LOS / NLOS link, symmetric / asymmetric, stationary / non-stationary etc. situations can be easily realized utilizing this channel that proves this model to be a promising option for the researchers. The CDF of γ_r is defined as

$$F_r(\gamma_r) = \int_0^{\gamma_r} f_r(y)dy. \tag{4}$$

TABLE 1. Special cases of HG fading channel.

Channels	HG Fading Parameters
One-sided Gaussian	$P_{kr} = 0.5$
Rayleigh	$P_{kr} = 1$
Nakagami-m	$P_{kr} = 2$
Nakagami-m	$P_{kr} = 3$

Substituting (3) into (4), utilizing [50, Eq. (3.351.1)] and performing integration, (4) is derived as

$$F_r(\gamma_r) = 1 - \sum_{kr=0}^{n}\sum_{v=0}^{P_{kr}-1} \frac{\zeta_{kr}}{v!}\mathcal{A}^v e^{-\mathcal{A}\gamma_r}{\gamma_r}^v. \tag{5}$$

D. PDF AND CDF OF SNR FOR FSO MAIN CHANNEL

Considering the FSO link experiences ΓΓ turbulence fading including pointing error, the PDF of γ_f is given as [10, Eq. (10)]

$$f_f(\gamma_f) = \frac{\mathcal{B}_1}{\gamma_f} G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_f}{\mu_s}\right)^{\frac{1}{s}} \middle| \begin{matrix}\epsilon^2+1 \\ \epsilon^2, a, b\end{matrix}\right], \tag{6}$$

where $\mathcal{B}_1 = \frac{\epsilon^2}{s\Gamma(a)\Gamma(b)}$, ϵ is known as the ratio between the equivalent beam radius of the wave and standard deviation of the pointing error displacement at the side of receiver [10], b and a both are scintillation / fading parameters that are related to the condition of atmospheric turbulence [51], s denotes the type of detection at the side of receiver i.e. $s = 1$ indicates HD technique and $s = 2$ indicates IM/DD method, $t = \frac{\epsilon^2}{\epsilon^2+1}$, $\Gamma(.)$ symbolizes Gamma operator [50, Eq. (8.310)], μ_s is the electrical SNR that is related to the average SNR of the FSO link denoted as ϕ_f, $\mu_1 = \phi_f$ is defined for HD method and $\mu_2 = \frac{\phi_f ab\epsilon^2(\epsilon^2+2)}{(a+1)(b+1)(\epsilon^2+1)^2}$ indicates for IM/DD technique. The expression of Meijer's G function [50, Eq. (9.301)] is expressed as $G_{p,q}^{m,n}\left[x\middle|\begin{matrix}\alpha_1,\ldots,\alpha_p \\ \beta_1,\ldots,\beta_q\end{matrix}\right]$. The CDF for FSO link is expressed as [51, Eq. (2)]

$$F_f(\gamma_f) = \mathcal{B}_2 G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_f \middle| \begin{matrix}1, l_1 \\ l_2, 0\end{matrix}\right], \tag{7}$$

where $\mathcal{B}_2 = \frac{\epsilon^2\, s^{a+b-2}}{(2\pi)^{s-1}\Gamma(a)\,\Gamma(b)}$ and $\mathcal{B}_3 = \frac{tab}{s^{2s}}$. The series l_1 and l_2 can be described as

$$l_1 = \Delta(s, \epsilon^2+1),$$
$$l_2 = \Delta(s, \epsilon^2), \Delta(s, a), \Delta(s, b),$$

and the notation $\Delta(\mathcal{L}, c)$ that includes $\mathcal{L}$ terms, is defined as

$$\Delta(\mathcal{L}, c) = \frac{c}{\mathcal{L}}, \frac{c+1}{\mathcal{L}}, \ldots\ldots, \frac{c+\mathcal{L}-1}{\mathcal{L}}.$$

E. PDF AND CDF OF SNR FOR EAVESDROPPER CHANNEL

Similar to the $S-R$ link, the link between S and E experiences HG fading. The PDF of the eavesdropper channel is expressed as [47, Eq. (3)]

$$f_e(\gamma_e) = \sum_{ke=0}^{n} \frac{\zeta_{ke}}{\Gamma(P_{ke})} \mathcal{C}^{P_{ke}} {\gamma_e}^{P_{ke}-1} e^{-\mathcal{C}\gamma_e}, \tag{8}$$

where $\mathcal{C} = \frac{P_{ke}}{\phi_{ke}}$. For a specific condition $1 \leq ke \leq n$, the limit of the fading severity parameter, the accruing factor of ke-th fading situation among n possible fading samples, and the average SNR of the eavesdropper channel are expressed as $P_{ke} \geq 0.5$, $0 \leq \zeta_{ke} \leq 1$, and $\phi_{ke} > 0$, respectively. Similar to (5), for eavesdropper channel, the CDF of γ_e is expressed as

$$F_e(\gamma_e) = 1 - \sum_{ke=0}^{n} \sum_{w=0}^{P_{ke}-1} \frac{\zeta_{ke}}{w!} \mathcal{C}^w e^{-\mathcal{C}\gamma_e} \gamma_e^w. \tag{9}$$

F. PDF AND CDF OF SNR FOR DUAL-HOP RF-FSO LINK

The CDF of γ_{dn} is expressed as by using order statistics [52, Eq. (5)]

$$\begin{aligned} F_{dn}(\gamma_{dn}) &= Pr\left\{min(\gamma_r, \gamma_f) < \gamma\right\} \\ &= F_r(\gamma_{dn}) + F_f(\gamma_{dn}) - F_r(\gamma_{dn}) F_f(\gamma_{dn}). \end{aligned} \tag{10}$$

Placing (5) and (7) into (10) and performing some mathematical manipulations for further simplifications, the CDF of γ_{dn} is written as

$$\begin{aligned} F_{dn}(\gamma_{dn}) = 1 - \sum_{kr=0}^{n} \sum_{v=0}^{P_{kr}-1} \frac{\zeta_{kr}}{v!} \mathcal{A}^v e^{-\mathcal{A}\gamma_{dn}} \gamma_{dn}^v \\ \times \left(1 - \mathcal{B}_2 G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn} \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right]\right). \end{aligned} \tag{11}$$

The PDF of SNR of the RF-FSO link is obtained by differentiating (11) with respect to γ_{dn} as [28, Eq. (4)]

$$\begin{aligned} f_{dn}(\gamma_{dn}) = f_r(\gamma_{dn}) + f_f(\gamma_{dn}) - f_r(\gamma_{dn}) F_f(\gamma_{dn}) \\ - f_f(\gamma_{dn}) F_r(\gamma_{dn}). \end{aligned} \tag{12}$$

Substituting (3), (5), (6), and (7) into (12) and further simplifying, the PDF of γ_{dn} is obtained as

$$\begin{aligned} f_{dn}(\gamma_{dn}) = \sum_{kr=0}^{n} \zeta_{kr} e^{-\mathcal{A}\gamma_{dn}} \Bigg(\mathcal{B}_1 \sum_{v=0}^{P_{kr}-1} \frac{\mathcal{A}^v}{v!} \gamma_{dn}^{v-1} \\ \times G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_{dn}}{\mu_s}\right)^{\frac{1}{s}} \middle| \begin{matrix} \epsilon^2 + 1 \\ \epsilon^2, a, b \end{matrix}\right] + \frac{\mathcal{A}^{P_{kr}}}{\Gamma(P_{kr})} \\ \times \mathcal{B}_2 {\gamma_{dn}}^{P_{kr}-1} G_{s+1,3s+1}^{3s+1,0}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn} \middle| \begin{matrix} l_1, 1 \\ 0, l_2 \end{matrix}\right]\Bigg). \end{aligned} \tag{13}$$

III. PERFORMANCE ANALYSIS

In this section, we derive novel expressions of SOP, ASC, and SPSC in closed-form. We also present asymptotic expression of SOP in high-SNR regime to obtain a better insight.

A. AVERAGE SECRECY CAPACITY

The ASC is one of the most important performance metric for the evaluation of secrecy performance in the presence of an eavesdropper. Mathematically, ASC is defined as [53, Eq. (15)], as shown at the bottom of the page,

$$ASC = \int_0^\infty \frac{F_e(\gamma)}{1+\gamma} \{1 - F_{dn}(\gamma)\} d\gamma. \tag{14}$$

Substituting (9) and (11) into (14), the expression of ASC is given by (15), wherein four integration terms can be found as follows:

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

Utilizing [54, eqs. (8.2.2.15), (8.4.2.5) and (8.4.3.1)] for expressing $\frac{\gamma^v}{1+\gamma}$ and $e^{-\mathcal{A}\gamma}$ in terms of Meijer's G function and integrating via utilizing [50, Eq. (7.811.1)], we obtain $\mathcal{R}_1$ as

$$\begin{aligned} \mathcal{R}_1 &= \int_0^\infty \frac{\gamma^v}{1+\gamma} e^{-\mathcal{A}\gamma} d\gamma \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} v \\ v \end{matrix}\right] G_{0,1}^{1,0}\left[\mathcal{A}\gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right] d\gamma \\ &= G_{1,2}^{2,1}\left[\mathcal{A} \middle| \begin{matrix} -v \\ 0, -v \end{matrix}\right]. \end{aligned} \tag{16}$$

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

Performing some simple mathematical calculation identical to (16) and utilizing [55, Eq. (20)] to perform integration, the term $\mathcal{R}_2$ is obtained as

$$\begin{aligned} \mathcal{R}_2 &= \int_0^\infty \frac{\gamma^v}{1+\gamma} e^{-\mathcal{A}\gamma} G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} v \\ v \end{matrix}\right] G_{0,1}^{1,0}\left[\mathcal{A}\gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma \\ &= \frac{1}{\mathcal{A}} G_{1,0:1,1:s+1,3s+1}^{1,0:1,1:3s,1}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} v \\ v \end{matrix} \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix} \middle| \frac{1}{\mathcal{A}}, \frac{\mathcal{B}_3}{\mu_s \mathcal{A}}\right], \end{aligned} \tag{17}$$

where, the term $G_{\alpha_1,\beta_1:\alpha_2,\beta_2:\alpha_3,\beta_3}^{p_1,q_1:p_2,q_2:p_3,q_3}[.]$ is defined as the extended generalized bivariate Meijer's G function (EGBMGF), which is introduced and explained in [56, Table 1].

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

Utilizing similar mathematical procedures as in $\mathcal{R}_1$, the term $\mathcal{R}_3$ is derived as

$$\mathcal{R}_3 = \int_0^\infty \frac{\gamma^z}{1+\gamma} e^{-\mathcal{D}\gamma} d\gamma$$

$$ASC = \sum_{kr=0}^{n} \sum_{v=0}^{P_{kr}-1} \frac{\zeta_{kr}}{v!} \mathcal{A}^v \left[\mathcal{R}_1 - \mathcal{B}_2 \mathcal{R}_2 - \sum_{ke=0}^{n} \sum_{w=0}^{P_{ke}-1} \frac{\zeta_{ke}}{w!} \mathcal{C}^w \left(\mathcal{R}_3 - \mathcal{B}_2 \mathcal{R}_4\right)\right]. \tag{15}$$

$$= \int_0^\infty G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} +w \\ +w \end{matrix}\right] G_{0,1}^{1,0}\left[\mathcal{D}\gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right] d\gamma$$
$$= G_{1,2}^{2,1}\left[\mathcal{D} \middle| \begin{matrix} -z \\ 0, -z \end{matrix}\right], \quad (18)$$

where $\mathcal{D} = \mathcal{A} + \mathcal{C}$ and $z = v + w$.

4) DERIVATION OF $\mathcal{R}_4$

Similar to (17), $\mathcal{R}_4$ is expressed as

$$\mathcal{R}_4 = \int_0^\infty \frac{\gamma^z}{1+\gamma} e^{-\mathcal{D}\gamma} G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma$$
$$= \int_0^\infty G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} +w \\ +w \end{matrix}\right] G_{0,1}^{1,0}\left[\mathcal{D}\gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right]$$
$$\times G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma$$
$$= \frac{1}{\mathcal{D}} G_{1,0:1,1:3s,1}^{1,0:1,1:3s,1}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} z \\ z \end{matrix} \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix} \middle| \frac{1}{\mathcal{D}}, \frac{\mathcal{B}_3}{\mu_s \mathcal{D}}\right]. \quad (19)$$

Note that all the system parameters are included in (15) and utilizing this expression provides useful insights into how the secrecy capacity performance is affected by the physical properties of the channel that can be easily analyzed. Again, (15) can be reduced to [38, Eq. (20)] for the condition ($P_{kr} = P_{ke} = 2$ and 3) considering Nakagami-m-ΓΓ distribution that indicates the generic nature of this expression over the existing works.

B. SECRECY OUTAGE PROBABILITY

If T_{sc} can be defined as the target secrecy rate, then the probability of occurring the secrecy outage event can be defined when the secrecy capacity falls below T_{sc}. So, the expression of SOP of combined RF-FSO channel can be described as [57, Eq. (14)]

$$SOP = Pr\{C_{sc} \le T_{sc}\}$$
$$= Pr\{\gamma_{dn} \le \varphi\gamma_e + \varphi - 1\}$$
$$= \int_0^\infty \int_{\varphi\gamma_e+\varphi-1}^\infty f_{dn}(\gamma_{dn}) f_e(\gamma_e) d\gamma_{dn} d\gamma_e$$
$$= \int_0^\infty F_{dn}(\varphi\gamma_e + \varphi - 1) f_e(\gamma_e) d\gamma_e, \quad (20)$$

where $\varphi = 2^{T_{sc}}$. It is mathematically difficult to define the exact expression of SOP in closed-form. Hence, we derive the expression of SOP at the lower-bound considering the variable gain relaying scheme as [58, Eq. (6)]

$$SOP \ge SOP_L = Pr\{\gamma_{dn} \le \varphi\gamma_e\}$$
$$= \int_0^\infty F_{dn}(\varphi\gamma_e) f_e(\gamma_e) d\gamma_e. \quad (21)$$

1) EXACT SOP

Substituting (8) and (11) into (21), the expression of SOP containing exact form of Meijer's G function is obtained as (22), shown at the bottom of the next page.

Here, utilizing [50, Eq.(3.351.3)] and performing integration, we can express the term S_1 as

$$S_1 = \int_0^\infty \gamma_e^{P_{ke}+v-1} e^{-\mathcal{E}\gamma_e} \varphi^v d\gamma_e = \frac{\varphi^v \Gamma(P_{ke}+v)}{(\mathcal{E})^{P_{ke}+v}}, \quad (24)$$

where $\mathcal{E} = \mathcal{A}\varphi + \mathcal{C}$. Similar to S_1, utilizing [54, eqs. (2.24.1.1) and (8.4.3.1)], S_2 is expressed as

$$S_2 = \int_0^\infty \gamma_e^{P_{ke}+v-1} e^{-\mathcal{E}\gamma_e} \varphi^v G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_e\varphi \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma_e$$
$$= \int_0^\infty \gamma_e^{P_{ke}+v-1} G_{0,1}^{1,0}\left[\mathcal{E}\gamma_e \middle| \begin{matrix} - \\ 0 \end{matrix}\right]$$
$$\times G_{s+1,3s+1}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_e\varphi \middle| \begin{matrix} 1, l_1 \\ l_2, 0 \end{matrix}\right] d\gamma_e$$
$$= \frac{\varphi^v}{\mathcal{E}^{P_{ke}+v}} G_{s+2,3s+1}^{3s,2}\left[\frac{\mathcal{B}_3\varphi}{\mu_s\mathcal{E}} \middle| \begin{matrix} 1, 1-P_{ke}-v, l_1 \\ l_2, 0 \end{matrix}\right]. \quad (25)$$

2) ASYMPTOTIC SOP

The exact SOP in (22) does not provide much insight into the secure outage performance of the proposed model. Hence, we also derive the asymptotic expression of SOP given in (23), as shown at the bottom of the next page. Herein, the Meijer's G term in S_2 is converted into asymptotic term in (23) by utilizing [59, Eq. (6.2.2)] and [10, Eq. (19)].

Similar to (15), the impact of all system parameters on the secure outage behaviour are demonstrated via (22) and (23). Additionally, for the conditions of considering Rayleigh-ΓΓ distribution ($P_{kr} = P_{ke} = 1$) and Nakagami-m-ΓΓ distribution ($P_{kr} = P_{ke} = 2$ and 3), our demonstrated results in (22) and (23) agree with [46, eqs. (15) and (22)] and [38, eqs. (13) and (15)], respectively.

C. STRICTLY POSITIVE SECRECY CAPACITY

To achieve a secure communication, the secrecy capacity must be a positive quantity that can be ensured in terms of an important secrecy measure such as SPSC. The SPSC is defined as [49]

$$\Pr(C_{sc} > 0) = \Pr(\gamma_{dn} > \gamma_e)$$
$$= \int_0^\infty \int_0^{\gamma_{dn}} f_{dn}(\gamma_{dn}) f_e(\gamma_e) d\gamma_e d\gamma_{dn}$$
$$= \int_0^\infty f_{dn}(\gamma_{dn}) F_e(\gamma_{dn}) d\gamma_{dn}. \quad (26)$$

This definition indicates that, a secure communication is possible if and only if $\gamma_{dn} > \gamma_e$. Substituting (9) and (13) into (26), and performing integration, we have (27), as shown at the bottom of the next page. The terms $\mathcal{T}_1$, $\mathcal{T}_2$, $\mathcal{T}_3$, and $\mathcal{T}_4$ are obtained as follows.

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

Utilizing [54, eqs. (2.24.1.1) and (8.4.3.1)] and performing some arithmetic calculations and simplifications, the term $\mathcal{T}_1$

is obtained as

$$\begin{aligned}\mathcal{T}_1 &= \int_0^\infty \mathcal{B}_2 \gamma_{dn}^{P_{kr}-1} e^{-\mathcal{A}\gamma_{dn}} G_{s+1,3s+1}^{3s+1,0}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn}\middle| \begin{matrix}1, l_1\\ l_2, 0\end{matrix}\right] d\gamma_{dn}\\ &= \int_0^\infty \mathcal{B}_2 \gamma_{dn}^{P_{kr}-1} G_{0,1}^{1,0}\left[\mathcal{A}\gamma_{dn}\middle| \begin{matrix}-\\ 0\end{matrix}\right]\\ &\quad\times G_{s+1,3s+1}^{3s+1,0}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn}\middle| \begin{matrix}1, l_1\\ l_2, 0\end{matrix}\right] d\gamma_{dn}\\ &= \mathcal{A}^{-P_{kr}}\mathcal{B}_2 G_{s+2,3s+1}^{3s+1,1}\left[\frac{\mathcal{B}_3}{\mu_s\mathcal{A}}\middle| \begin{matrix}1-P_{kr}, l_1, 1\\ 0, l_2\end{matrix}\right]. \end{aligned} \tag{28}$$

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

Similar to the derivation of $\mathcal{T}_1$, $\mathcal{T}_2$ is obtained as

$$\begin{aligned}\mathcal{T}_2 &= \int_0^\infty \mathcal{B}_1 \gamma_{dn}^{v-1} e^{-\mathcal{A}\gamma_{dn}} G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_{dn}}{\mu_s}\right)^{\frac{1}{s}}\middle| \begin{matrix}\epsilon^2+1\\ \epsilon^2, a, b\end{matrix}\right] d\gamma_{dn}\\ &= \int_0^\infty \mathcal{B}_1 \gamma_{dn}^{v-1} G_{0,1}^{1,0}\left[\mathcal{A}\gamma_{dn}\middle| \begin{matrix}-\\ 0\end{matrix}\right]\\ &\quad\times G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_{dn}}{\mu_s}\right)^{\frac{1}{s}}\middle| \begin{matrix}\epsilon^2+1\\ \epsilon^2, a, b\end{matrix}\right] d\gamma_{dn}\\ &= \mathcal{A}^{-v}\mathcal{B}_2 G_{s+1,3s}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s\mathcal{A}}\middle| \begin{matrix}1-v, l_1\\ l_2\end{matrix}\right]. \end{aligned} \tag{29}$$

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

The expression of $\mathcal{T}_3$ is deduced similarly as

$$\begin{aligned}\mathcal{T}_3 &= \int_0^\infty \mathcal{B}_2 \gamma_{dn}^{P_{kr}+w-1} e^{-\mathcal{D}\gamma_{dn}}\\ &\quad\times G_{s+1,3s+1}^{3s+1,0}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn}\middle| \begin{matrix}l_1, 1\\ 0, l_2\end{matrix}\right] d\gamma_{dn}\\ &= \int_0^\infty \mathcal{B}_2 \gamma_{dn}^{P_{kr}+w-1} G_{0,1}^{1,0}\left[\mathcal{D}\gamma_{dn}\middle| \begin{matrix}-\\ 0\end{matrix}\right]\\ &\quad\times G_{s+1,3s+1}^{3s+1,0}\left[\frac{\mathcal{B}_3}{\mu_s}\gamma_{dn}\middle| \begin{matrix}l_1, 1\\ 0, l_2\end{matrix}\right] d\gamma_{dn}\\ &= \mathcal{B}_2\mathcal{D}^{-P_{kr}-w} G_{s+2,3s+1}^{3s+1,1}\left[\frac{\mathcal{B}_3}{\mu_s\mathcal{D}}\middle| \begin{matrix}1-P_{kr}-w, l_1, 1\\ 0, l_2\end{matrix}\right]. \end{aligned} \tag{30}$$

4) DERIVATION OF $\mathcal{T}_4$

Following the similar procedures as in obtaining $\mathcal{T}_3$, $\mathcal{T}_4$ is obtained as

$$\begin{aligned}\mathcal{T}_4 &= \int_0^\infty \mathcal{B}_1 \gamma_{dn}^{z-1} e^{-\mathcal{D}\gamma_{dn}} G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_{dn}}{\mu_s}\right)^{\frac{1}{s}}\middle| \begin{matrix}\epsilon^2+1\\ \epsilon^2, a, b\end{matrix}\right] d\gamma_{dn}\\ &= \int_0^\infty \mathcal{B}_1 \gamma_{dn}^{z-1} G_{0,1}^{1,0}\left[\mathcal{D}\gamma_{dn}\middle| \begin{matrix}-\\ 0\end{matrix}\right]\\ &\quad\times G_{1,3}^{3,0}\left[tab\left(\frac{\gamma_{dn}}{\mu_s}\right)^{\frac{1}{s}}\middle| \begin{matrix}\epsilon^2+1\\ \epsilon^2, a, b\end{matrix}\right] d\gamma_{dn}\\ &= \mathcal{B}_2\mathcal{D}^{-z} G_{s+1,3s}^{3s,1}\left[\frac{\mathcal{B}_3}{\mu_s\mathcal{D}}\middle| \begin{matrix}1-z, l_1\\ l_2\end{matrix}\right]. \end{aligned} \tag{31}$$

It can be pointed out that all the system parameters e.g. pointing error, turbulence, fading etc. are incorporated in (27) and hence how these parameters affect SPSC can be easily obtained with it. For example Rayleigh-ΓΓ distribution can be obtained via $P_{kr} = P_{ke} = 1$ and Nakagami-m-ΓΓ distribution can be obtained via $P_{kr} = P_{ke} = 2$ and 3 in (27).

IV. NUMERICAL RESULTS

In this section, the impact of the system parameters on the secrecy behaviour of the proposed scheme is presented. For this purpose, several analytical results regarding the deduced expressions of SOP, ASC, and SPSC are illustrated with the help of Figures. We also present the simulation results to validate the analytical outcomes via Monte-Carlo simulations. We generate HG and Gamma-Gamma random variables in MATLAB and average 100,000 channel realizations to obtain each value of the secrecy parameters. The parametric analysis is performed considering $P_{kr} = P_{ke} = (1, 2, 3)$, $C_{sc} = 1$, $T_{sc} = 0.1$ bits/sec/Hz, $s = 1$ and 2, $(a, b) = (2.064, 1.342)$ for strong turbulence, (2.296, 1.822) for moderate turbulence, and (2.902, 2.510) for weak turbulence, and $\epsilon = 1$ and 6.7.

The impacts of P_{kr} on ASC and SOP are analyzed in Figs. 2 and 3, respectively. Numerical and simulation results are obtained by plotting these parameters against ϕ_{kr}. In each Figure, we consider two cases with $\phi_{ke} = -5dB$ and $5dB$. It is observed that for both cases, the secrecy capacity and secrecy outage behaviour improve with P_{kr}. Again, the worst the

$$SOP_{L,E} = 1 - \sum_{kr=0}^{n}\sum_{ke=0}^{n}\sum_{v=0}^{P_{kr}-1}\frac{\zeta_{kr}\zeta_{ke}}{v!\Gamma(P_{ke})}\mathcal{A}^v\mathcal{C}^{P_{ke}}(S_1 - \mathcal{B}_2 S_2). \tag{22}$$

$$SOP_{L,A} = 1 - \sum_{kr=0}^{n}\sum_{ke=0}^{n}\sum_{v=0}^{P_{kr}-1}\frac{\zeta_{kr}\zeta_{ke}}{v!\Gamma(P_{ke})}\mathcal{A}^v\mathcal{C}^{P_{ke}}\left[S_1 - \frac{\mathcal{B}_2\varphi^v}{\mathcal{E}^{P_{ke}+v}}\sum_{\kappa=1}^{3s}\frac{\Gamma(l_{2,\kappa})\prod_{p=1,p\neq\kappa}^{3s}\Gamma(l_{2,p}-l_{2,\kappa})}{\prod_{p=3}^{s+2}\Gamma(l_{1,p}-l_{2,\kappa})}\left(\frac{\mathcal{E}\mu_s}{\mathcal{B}_3\varphi}\right)^{-l_{2,\kappa}}\right]. \tag{23}$$

$$SPSC = \sum_{kr=0}^{n}\zeta_{kr}\left[\frac{\mathcal{A}^{P_{kr}}}{\Gamma(P_{kr})}\mathcal{T}_1 + \sum_{v=0}^{P_{kr}-1}\frac{\mathcal{A}^v}{v!}\mathcal{T}_2 - \sum_{ke=0}^{n}\sum_{w=0}^{P_{ke}-1}\frac{\zeta_{ke}}{w!}\mathcal{C}^w\left(\frac{\mathcal{A}^{P_{kr}}}{\Gamma(P_{kr})}\mathcal{T}_3 + \sum_{v=0}^{P_{kr}-1}\frac{\mathcal{A}^v}{v!}\mathcal{T}_4\right)\right]. \tag{27}$$

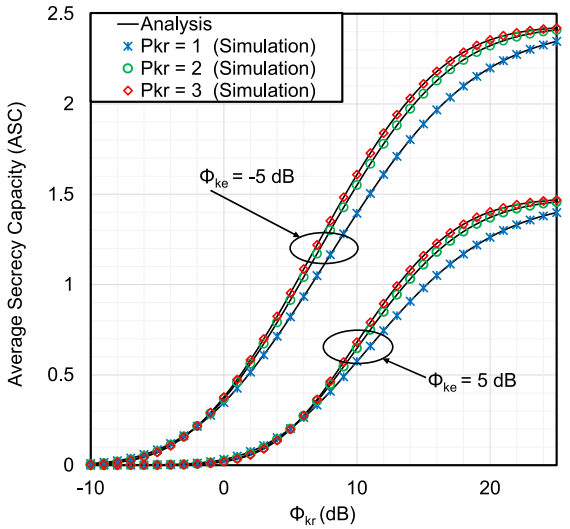


FIGURE 2. The ASC versus ϕ_{kr} for selected values of P_{kr} and ϕ_{ke} with $P_{ke} = 3$ $\mu_s = 15dB$, $\epsilon = 1$, $s = 1$, $a = 2.064$, and $b = 1.342$.

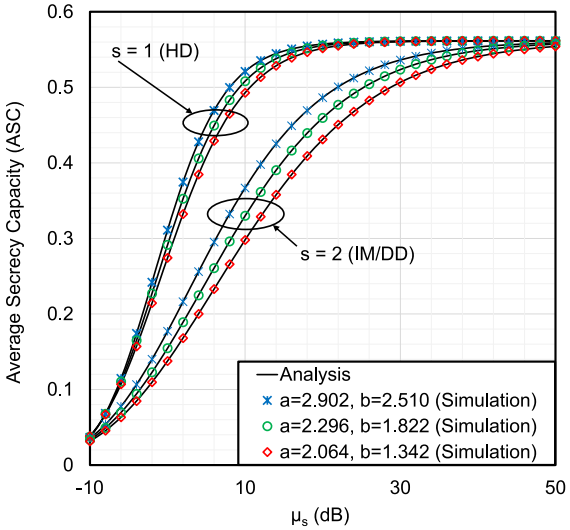


FIGURE 4. The ASC versus μ_s for selected values of s, a, and b with $P_{kr} = P_{ke} = 3$, $\phi_{kr} = 0dB$, $\phi_{ke} = -10dB$, and $\epsilon = 1$.

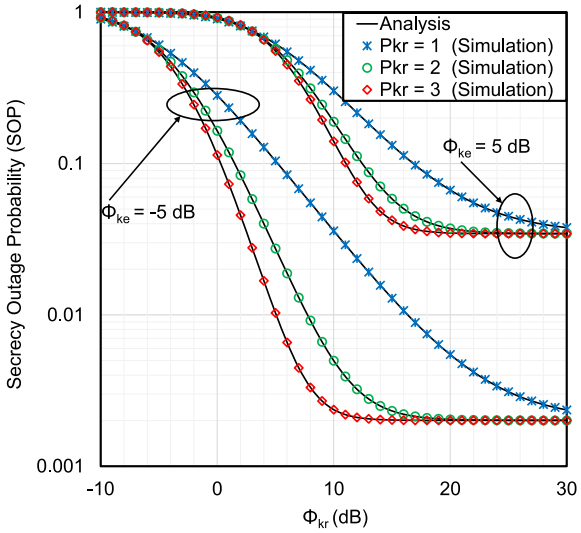


FIGURE 3. The SOP versus ϕ_{kr} for selected values of P_{kr} and ϕ_{ke} with $P_{ke} = 3$ $\mu_s = 20dB$, $\epsilon = 1$, $s = 1$, $a = 2.064$, and $b = 1.342$.

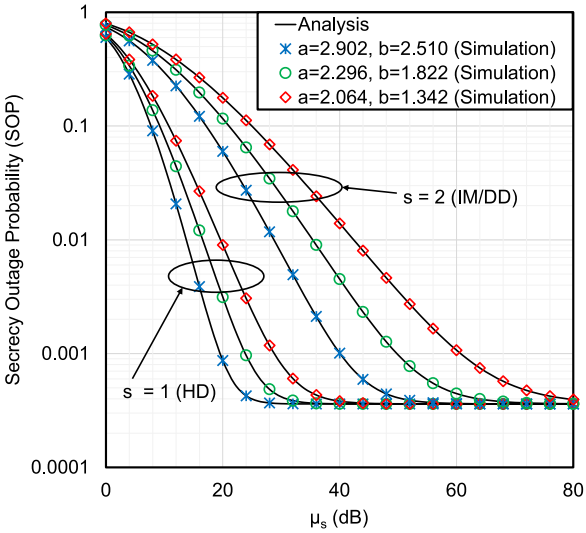


FIGURE 5. The SOP versus μ_s for selected values of s, a, and b with $P_{kr} = P_{ke} = 3$, $\phi_{kr} = 15dB$, $\phi_{ke} = 0dB$, and $\epsilon = 6.7$.

eavesdropper channel, the better the secrecy performance is. The fading of RF (main) links gradually decreases as the value of P_{kr} increases from zero to infinity and hence the system performance also enhances. Our results agree with the related outcomes of [47]. It is also noted that the simulation results perfectly matches with the analytical results that is a clear indication of the exactness of our deduced expressions.

The impacts of weak, moderate, and strong atmospheric turbulence on the secrecy behaviour of the proposed scheme are demonstrated in Figs. 4, 5, and 6. We consider two scenarios with $s = 1$ and $s = 2$ in each Figure. It is noted for both the scenarios that the weak turbulence exhibits better secrecy performance than the others, as testified in [38], [52]. This occurs because the atmospheric turbulence only affects the SNR at D remarkably. The gap-size between the curves of each detection scheme reveals that the turbulence affects the IM/DD scheme more significantly than the HD scheme.

Besides atmospheric turbulence, the influences of HD and IM/DD detection techniques employed at the receiver are also analyzed in Figs. 4, 5, and 6. The results demonstrate that enhanced secrecy performances is obtained in the case of HD technique ($s = 1$) rather than the IM/DD technique ($s = 2$). This happens because HD technique offers better SNR at the receiver compared to the IM/DD case. The authors of [38], [51], [52] also demonstrated similar results that strengthen the accuracy of our analysis.

The impact of pointing error on the secrecy performance is analyzed by plotting ASC, SOP, and SPSC against ϕ_{kr}

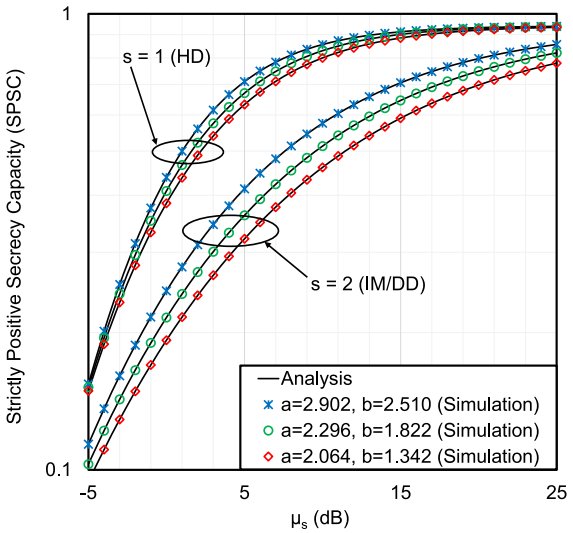


FIGURE 6. The SPSC versus μ_s for selected values of s, a, and b with $P_{kr} = P_{ke} = 3$, $\phi_{kr} = 5dB$, $\phi_{ke} = -1dB$, and $\epsilon = 1$.

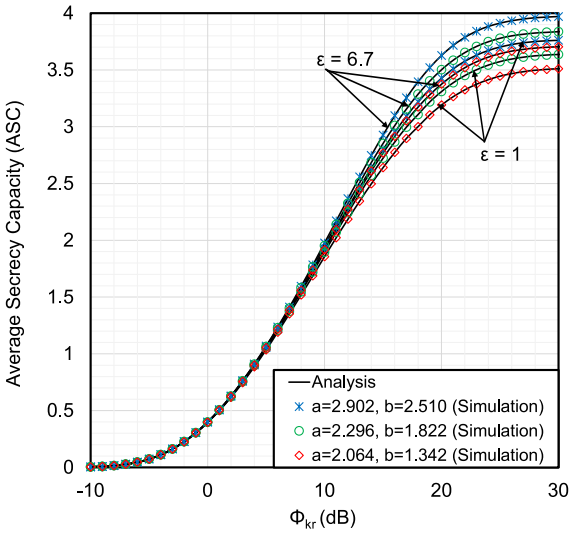


FIGURE 7. The ASC versus ϕ_{kr} for selected values of ϵ, a, and b with $P_{kr} = P_{ke} = 3$, $\mu_s = 20dB$, $\phi_{ke} = -5dB$, and $s = 1$.

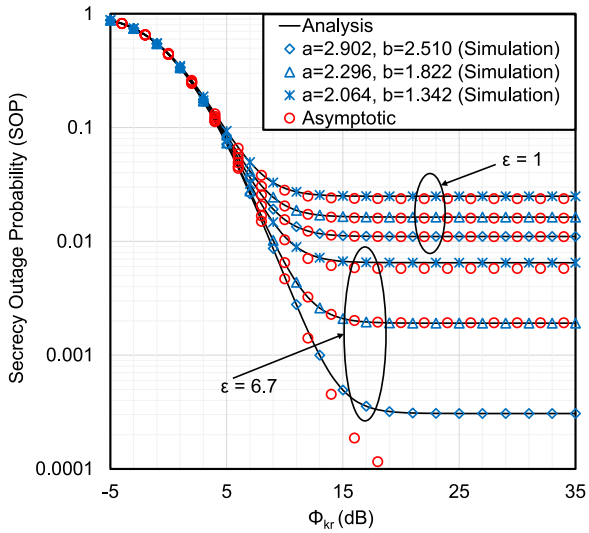


FIGURE 8. The SOP versus ϕ_{kr} for selected values of ϵ, a, and b with $P_{kr} = P_{ke} = 3$, $\mu_s = 20dB$, $\phi_{ke} = -1dB$, and $s = 1$.

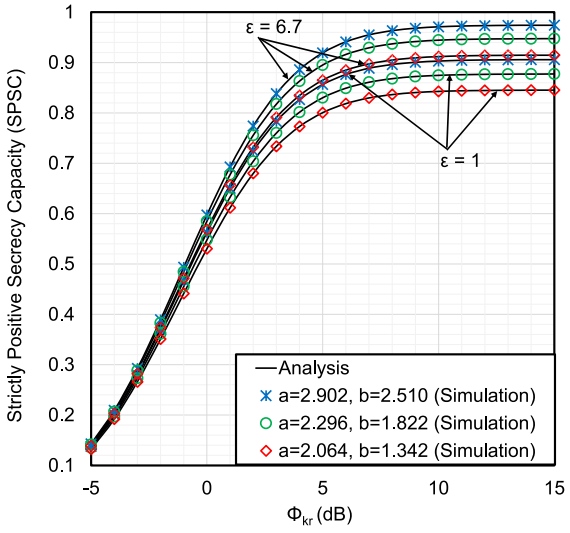


FIGURE 9. The SPSC versus ϕ_{kr} for selected values of ϵ, a, and b with $P_{kr} = P_{ke} = 3$, $\mu_s = 10dB$, $\phi_{ke} = -1dB$, and $s = 1$.

in Figs. 7, 8, and 9, respectively. It is observed that the SPSC and ASC increases, and SOP decreases if the value of ϵ is increased from 1 (i.e. severe pointing error) to 6.7 (i.e. negligible pointing error). The reason behind this observation is that the pointing authenticity also enhances with the increase of ϵ. The similar impact of pointing error is also encountered in the existing literature [38], [60]. To obtain more insights into the secrecy outage performance, asymptotic results are demonstrated in Fig. 8 besides the analytical and simulation results. We can see that the asymptotic SOP matches well with the exact results which indicates that at high SNR regime, a tight approximation of the exact results is obtained with the asymptotic SOP.

The SPSC is plotted as a function of ϕ_{kr} in Fig. 10 to investigate the effect of ϕ_{ke}. The results demonstrate that SPSC deteriorates as the value of ϕ_{ke} is increased from -10dB to 20dB. This phenomenon indicates that the stronger the eavesdropper channel, the weaker the secrecy performance is.

It is noted from Figs. 2-11 that a floor in SOP curves and a ceiling in SPSC and ASC curves are obtained. This is obvious due to the limit in performance of the $S - R$ link. We may improve the $R-D$ link, but due to the weaker $S-R$ link, $R-D$ link will be receiving somewhat weaker data for which the secrecy capacity will be constant. Hence the SOP will reach a floor, and SPSC and ASC will reach a ceiling.

Comparative analysis with existing related literature:

In our analysis, we assume Generalized HG fading channel at the RF links (main and eavesdropper) and ΓΓ fading channel at the FSO link. Note that ΓΓ is a popular and interesting FSO model that can describe fading, atmospheric turbulence,

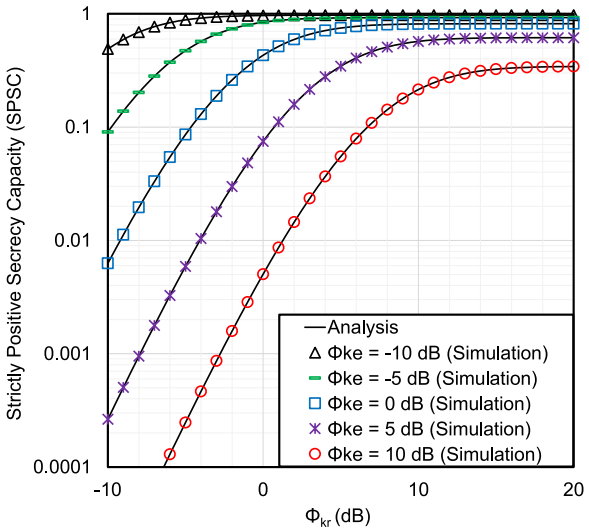


FIGURE 10. The SPSC versus ϕ_{kr} for selected values of ϕ_{ke} with $P_{kr} = P_{ke} = 3$, $\mu_s = 10dB$, $a = 2.064$, $b = 1.342$, $\epsilon = 1$, and $s = 1$.

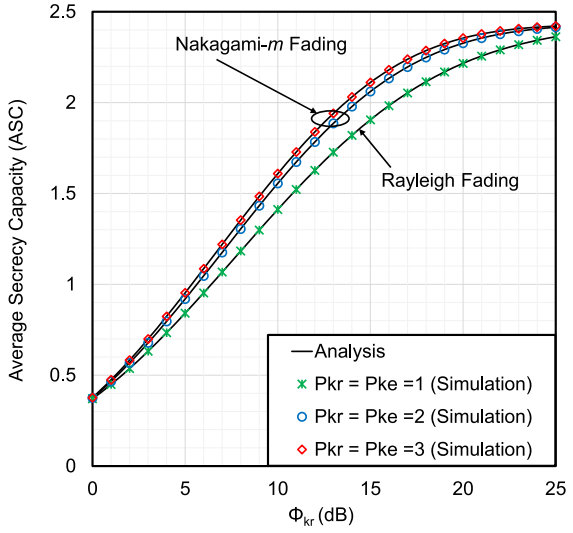


FIGURE 11. The ASC versus ϕ_{kr} for selected values of P_{kr} and P_{ke} with $\mu_s = 15dB$, $\phi_{ke} = -5dB$, $a = 2.064$, $b = 1.342$, $\epsilon = 1$, and $s = 1$.

and pointing error more accurately and precisely than any other existing FSO models. On the other hand, HG represents a generalized fading scenario from which some classical fading channels can be obtained as special cases [Table 1].

Our proposed model provides a unified performance evaluation of the aforementioned multipath [Table 1]-ΓΓ mixed fading scenarios that is more clearly explained in Fig. 11.

Hence, we can say that the existing works in [38], [43], [46], and [60] are the special cases of our model. This helps to decide that the originality of the proposed scheme is more distinct and exclusive than all the existing works.

V. CONCLUSION

This research centers on the assessment of a HG-ΓΓ RF-FSO mixed system's capabilities to defend against maleficent attacks of a passive eavesdropper. We execute the secrecy analysis by means of expressions of ASC, SOP, and SPSC in closed-form. We also demonstrate asymptotic expression for SOP of such framework to gain more useful insights. We, in addition, authenticate the analytical results utilizing Monte-Carlo simulations. Due to the HG fading channel at the RF link, the derived expressions are also general and responsible for analyzing the impacts of acute turbulent fading, pointing errors, and various detection methodologies (e.g. HD and IM/DD). It is noteworthy that, the evaluated SOP, SPSC, and ASC performance adopting IM/DD technique deteriorates considerably amid intense pointing errors and atmospheric turbulence conditions relative to the HD technique. At the end, we establish the supremacy of our analysis via utilizing generic physical properties of HG channel. In future, the authors' interest is to model RF-FSO networks with DF relay.

REFERENCES

[1] X. Zhu and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1293–1300, Aug. 2002.
[2] M. Uysal, S. M. Navidpour, and J. Li, "Error rate performance of coded free-space optical links over strong turbulence channels," *IEEE Commun. Lett.*, vol. 8, no. 10, pp. 635–637, Oct. 2004.
[3] M. Uysal, J. Li, and M. Yu, "Error rate performance analysis of coded free-space optical links over gamma-gamma atmospheric turbulence channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1229–1233, Jun. 2006.
[4] S. M. Haas and J. H. Shapiro, "Capacity of wireless optical communications," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 8, pp. 1346–1357, Oct. 2003.
[5] M. Safari and M. Uysal, "Relay-assisted free-space optical communication," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5441–5449, Dec. 2008.
[6] A. Belmonte and J. M. Kahn, "Capacity of coherent free-space optical links using diversity-combining techniques," *Opt. Express*, vol. 17, no. 15, pp. 12601–12611, 2009.
[7] E. Bayaki, R. Schober, and R. Mallik, "Performance analysis of MIMO free-space optical systems in gamma-gamma fading," *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3415–3424, Nov. 2009.
[8] A. A. Farid and S. Hranilovic, "Diversity gain and outage probability for MIMO free-space optical links with misalignment," *IEEE Trans. Commun.*, vol. 60, no. 2, pp. 479–487, Feb. 2012.
[9] I. S. Ansari, M.-S. Alouini, and J. Cheng, "Ergodic capacity analysis of free-space optical links with nonzero boresight pointing errors," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4248–4264, Aug. 2015.
[10] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Performance analysis of free-space optical links over Málaga ($\mathcal{M}$) turbulence channels with pointing errors," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 91–102, Jan. 2016.
[11] M. Najafi, V. Jamali, P. D. Diamantoulakis, G. K. Karagiannidis, and R. Schober, "Non-orthogonal multiple access for FSO backhauling," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
[12] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart., 2017.
[13] H. Arezumand, H. Zamiri-Jafarian, and E. Soleimani-Nasab, "Outage and diversity analysis of underlay cognitive mixed RF-FSO cooperative systems," *J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 909–920, Oct. 2017.
[14] E. Balti and M. Guizani, "Mixed RF/FSO cooperative relaying systems with co-channel interference," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4014–4027, Sep. 2018.
[15] A. Upadhya, V. K. Dwivedi, and M.-S. Alouini, "Interference-limited mixed MUD-RF/FSO two-way cooperative networks over double generalized gamma turbulence channels," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1551–1555, Sep. 2019.

[16] B. Makki, T. Svensson, M. Brandt-Pearce, and M.-S. Alouini, "On the performance of millimeter wave-based RF-FSO multi-hop and mesh networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7746–7759, Dec. 2017.

[17] L. Yang, J. Yuan, X. Liu, and M. O. Hasna, "On the performance of LAP-based multiple-hop RF/FSO systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 499–505, Jun. 2018.

[18] N. Singhal, A. Bansal, and A. Kumar, "Performance evaluation of decode-and-forward-based asymmetric SIMO-RF/FSO system with misalignment errors," *IET Commun.*, vol. 11, no. 14, pp. 2244–2252, Sep. 2017.

[19] N. Varshney and P. Puri, "Performance analysis of decode-and-forward-based mixed MIMO-RF/FSO cooperative systems with source mobility and imperfect CSI," *J. Lightw. Technol.*, vol. 35, no. 11, pp. 2070–2077, Jun. 1, 2017.

[20] B. Bag, A. Das, I. S. Ansari, A. Prokeš, C. Bose, and A. Chandra, "Performance analysis of hybrid FSO systems using FSO/RF-FSO link adaptation," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–17, Jun. 2018.

[21] Y. F. Al-Eryani, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Two-way multiuser mixed RF/FSO relaying: Performance analysis and power allocation," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 396–408, Apr. 2018.

[22] J. Vellakudiyan, V. Palliyembil, I. S. Ansari, P. Muthuchidambaranathan, and K. A. Qaraqe, "Performance analysis of the decode-and-forward relay-based RF-FSO communication system in the presence of pointing errors," *IET Signal Process.*, vol. 13, no. 4, pp. 480–485, Jun. 2019.

[23] M. I. Petkovic and Z. Trpovski, "Exact outage probability analysis of the mixed RF/FSO system with variable-gain relays," *IEEE Photon. J.*, vol. 10, no. 6, pp. 1–14, Dec. 2018.

[24] L. Yang, M. O. Hasna, and I. S. Ansari, "Unified performance analysis for multiuser mixed μ-η and $\mathcal{M}$-distribution dual-hop RF/FSO systems," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3601–3613, Aug. 2017.

[25] V. Palliyembil, J. Vellakudiyan, P. Muthuchidamdaranathan, and T. A. Tsiftsis, "Capacity and outage probability analysis of asymmetric dual-hop RF–FSO communication systems," *IET Commun.*, vol. 12, no. 16, pp. 1979–1983, Oct. 2018.

[26] O. M. S. Al-Ebraheemy, A. M. Salhab, A. Chaaban, S. A. Zummo, and M.-S. Alouini, "Precise performance analysis of dual-hop mixed RF/Unified-FSO DF relaying with heterodyne detection and two IM-DD channel models," *IEEE Photon. J.*, vol. 11, no. 1, pp. 1–22, Feb. 2019.

[27] Z. Wang, W. Shi, and W. Liu, "Two-way mixed RF/FSO relaying system in the presence of co-channel interference," *IEEE Photon. J.*, vol. 11, no. 2, pp. 1–16, Apr. 2019.

[28] J. Gupta, V. K. Dwivedi, and V. Karwal, "On the performance of RF-FSO system over Rayleigh and Kappa-Mu/inverse Gaussian fading environment," *IEEE Access*, vol. 6, pp. 4186–4198, 2018.

[29] Y. F. Al-Eryani, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Protocol design and performance analysis of multiuser mixed RF and hybrid FSO/RF relaying with buffers," *J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 309–321, Apr. 2018.

[30] E. Balti, M. Guizani, B. Hamdaoui, and B. Khalfi, "Aggregate hardware impairments over mixed RF/FSO relaying systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1110–1123, Mar. 2018.

[31] J. Hu, Z. Zhang, J. Dang, L. Wu, and G. Zhu, "Performance of decode-and-forward relaying in mixed Beaulieu-Xie and $\mathcal{M}$ dual-hop transmission systems with digital coherent detection," *IEEE Access*, vol. 7, pp. 138757–138770, 2019.

[32] H. Arezumand, H. Zamiri-Jafarian, and E. Soleimani-Nasab, "Exact and asymptotic analysis of partial relay selection for cognitive RF-FSO systems with non-zero boresight pointing errors," *IEEE Access*, vol. 7, pp. 58611–58625, 2019.

[33] A. H. A. El-Malek, M. A. Aboulhassan, A. M. Salhab, and S. A. Zummo, "Performance analysis and power optimization for spectrum-sharing mixed RF/FSO relay networks with energy harvesting," *IEEE Photon. J.*, vol. 11, no. 2, pp. 1–17, Apr. 2019.

[34] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[35] H. Yu, T. Kim, and H. Jafarkhani, "Wireless secure communication with beamforming and jamming in time-varying wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2087–2100, Aug. 2018.

[36] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[37] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, Feb. 2017.

[38] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photon. J.*, vol. 9, no. 4, pp. 1–14, Aug. 2017.

[39] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5904–5918, Sep. 2016.

[40] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6384–6395, Dec. 2018.

[41] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[42] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Effect of RF interference on the security-reliability tradeoff analysis of multiuser mixed RF/FSO relay networks with power allocation," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1490–1505, May 1, 2017.

[43] H. Lei, H. Luo, K.-H. Park, Z. Ren, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–13, Jun. 2018.

[44] L. Yang, T. Liu, J. Chen, and M. Alouini, "Physical-layer security for mixed η-μ and $\mathcal{M}$-distribution dual-hop RF/FSO systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12427–12431, Oct. 2018.

[45] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "On secrecy analysis of DF based dual hop mixed RF-FSO systems," *IEEE Access*, vol. 7, pp. 66725–66730, 2019.

[46] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[47] S. Ekin, F. Yilmaz, H. Celebi, K. A. Qaraqe, M.-S. Alouini, and E. Serpedin, "Achievable capacity of a spectrum sharing system over hyper fading channels," in *Proc. GLOBECOM IEEE Global Telecommun. Conf.*, Nov. 2009, pp. 1–6.

[48] M. O. Hasna and M.-S. Alouini, "A performance study of dual-hop transmissions with fixed gain relays," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, vol. 4, Apr. 2003, pp. 189–192.

[49] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745–6751, Dec. 2012.

[50] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*. Amsterdam, The Netherlands: Elsevier, 2007.

[51] E. Zedini, H. Soury, and M.-S. Alouini, "On the performance analysis of dual-hop mixed FSO/RF systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3679–3689, May 2016.

[52] E. Zedini, I. S. Ansari, and M. Alouini, "Performance analysis of mixed Nakagami-*m* and Gamma–Gamma dual-hop FSO transmission systems," *IEEE Photon. J.*, vol. 7, no. 1, pp. 1–20, Feb. 2015.

[53] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[54] A. Prudnikov, Y. Brychkov, and O. Marichev, *IIntegrals and Series: More Special Functions*, vol. 3. New York, NY, USA: Gordon and Breach Science Publishers, 1992.

[55] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO generalized-*k* fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[56] I. S. Ansari, S. Al-Ahmadi, F. Yilmaz, M.-S. Alouini, and H. Yanikomeroglu, "A new formula for the BER of binary modulations with dual-branch selection over Generalized-K composite fading channels," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2654–2658, Oct. 2011.

[57] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Performance analysis of physical layer security over generalized-*K* fading channels using a mixture gamma distribution," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 408–411, Feb. 2016.

[58] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized Gamma fading channels," *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1257–1260, Jul. 2015.

[59] M. D. Springer, *The Algebra of Random Variables*. New York, NY, USA: Wiley, Apr. 1979.
[60] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion," *Opt. Quantum Electron.*, vol. 50, no. 7, p. 298, Jul. 2018.

NOOR AHMAD SARKER is currently pursuing the B.Sc. degree in electronics and telecommunication engineering (ETE) with the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh. His research interests include physical layer security, cooperative communication, and FSO communication.

A. S. M. BADRUDDUZA received the B.Sc. and M.Sc. degrees in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Kajla, Rajshahi, 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 and 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 working as an Assistant Professor, since June 2020. His research interests include information-theoretic security in multicast, cellular and cooperative networks, physical layer security of RF/FSO, and NOMA systems. He has more than 24 technical articles in his research area.

Mr. Badrudduza was a recipient of two EEE Association Awards (Student of the Year Award) from RUET for his outstanding academic performances in the 1st and 4th year examinations while pursuing the B.Sc. engineering degree and two Best Paper Awards for two different research papers from IEEE Region 10 Symposium (TENSYMP 2020) and 3rd IEEE International Conference on Telecommunication and Photonics (ICTP 2019).

S. M. RIAZUL ISLAM (Member, IEEE) was with the University of Dhaka, Bangladesh, as an Assistant Professor, and a Lecturer with the Department of Electrical and Electronic Engineering, from 2005 to 2014. In 2014, he has worked with the Department of Solution Lab, Samsung Research and Development Institute Bangladesh (SRBD), as the Chief Engineer. From 2014 to 2017, he has worked with the Wireless Communications Research Centre, Inha University, South Korea, as a Postdoctoral Fellow. From 2016 to 2017, he was also affiliated with Memorial University, Canada, as a non-resident Postdoctoral Fellow. He has been working as an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, South Korea, since March 2017. He is also a Distinguished Professor with the Chongqing College of Electronic Engineering, China. His research interests include wireless communications, 5G and the IoT, wireless health, bioinformatics, and machine learning.

SHEIKH HABIBUL ISLAM is currently pursuing the B.Sc. degree in electrical and electronic engineering (EEE) with the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh. His research interests include FSO communication, physical layer security, and NOMA systems.

IMRAN SHAFIQUE ANSARI (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.

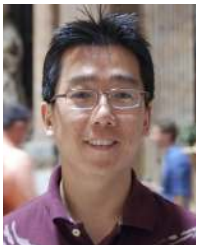
From May 2009 to August 2009, he was a Visiting Scholar with Michigan State University (MSU), East Lansing, MI, USA. From June 2010 to August 2010, he was a Research Intern with Carleton University, Ottawa, ON, Canada. From April 2015 to November 2017, he was a Postdoctoral Research Associate (PRA) with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

Dr. Ansari has served in various capacities. He has been serving on the IEEE Nominations and Appointments (N&A) Committee 2020–2021 and IEEE Communication Society Young Professionals (ComSoc YP) Board, since April 2016. He is an active reviewer for the various IEEE TRANSACTIONS and various other journals. He has served as a TPC for various IEEE conferences. He was a recipient of appreciation for an Exemplary Reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS, in 2016 and 2018, a recipient of appreciation for an Exemplary Reviewer for the IEEE WIRELESS COMMUNICATIONS LETTERS, in 2014 and 2017, a recipient of Postdoctoral Research Award (PDRA) (first cycle) with the Qatar National Research Foundation (QNRF), in 2014, and a recipient of the IEEE Richard E. Merwin Student Scholarship Award, in July 2013. He has co-organized the GRASNET'2016, 2017, 2018 workshops in conjunction with IEEE WCNC'2016, 2017, and IEEE Globecom 2018. He is a part of the IEEE 5G Tech Focus Publications Editorial Board, since February 2017.

MILTON KUMAR KUNDU (Member, IEEE) received the B.Sc. degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Bangladesh, in 2016, where he is currently pursuing the M.Sc. degree. He has been working as a Lecturer with the Department of Electrical and Computer Engineering (ECE), RUET, since February 2019. He is also the current Advisor of the IEEE RUET IAS Student Branch Chapter. His research interests include security aspects of cooperative and physical layer networks and wireless multicasting. He performed his duty as the Chair of the IEEE RUET Student Branch, from 2015 to 2016.

MST. FATEHA SAMAD received the B.Sc. degree in electronics and communication engineering from the Khulna University of Engineering and Technology, Bangladesh, in 2008, and the Ph.D. degree from the School of Engineering, Deakin University, Australia, in 2015. She is currently working as an Associate Professor with the Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology (RUET). She has been working in the area of nanotechnology, telecommunication, and biomedical engineering for last ten years. She has published a number of research articles on those fields. Her research interests include drug deliver systems, digital microfluidics, bio-sensor, lab-on-a-chip, wireless endoscopy, implantable antenna, deep brain stimulation, and wireless communication.

MD. BIPLOB HOSSAIN received the B.Sc. and M.Sc. degrees from the Rajshahi University of Engineering and Technology (RUET), in 2016 and 2019, respectively, all in electrical and electronic engineering (EEE). In 2016, he was appointed as a Lecturer with the Department of EEE, Bangladesh Army University of Engineering and Technology (BAUET), where he was from August 2016 to December 2018. From December 2018 to February 2020, he has worked as a Lecturer with the Department of Electrical and Electronic Engineering, Faculty of Engineering and Technology, Jashore University of Science and Technology (JUST), Jashore, Bangladesh, where he has been working as an Assistant Professor, since February 2020. He has authored or coauthored around 30 technical articles, including Elsevier, Springer, IEEE, ASP, Hindawi, DE GRUYTER, and SPIE publishers. His research interests include advanced optical sensors modeling for emerging applications, such as biomedical sensing, electric vehicles, power transformer, optical fiber-based SPR sensors for solid state transformer, surface plasmon resonance (SPR) sensors design and implementation for biomedical sensing, power transformer, wind turbine applications, and performance analysis of SPR sensors for biomedical sensing, electric vehicle, and power and solid state transformer. He had been awarded the University Technical Scholarship at RUET for his outstanding academic results, from 2012 to 2015. He has been got the Deanship of the Scientific Research (DSR) Fund from King Abdulaziz University (KAU), Jeddah, Saudi Arabia, from 2019 to 2020.



HEEJUNG YU (Member, IEEE) received the B.S. degree in radio science and engineering from Korea University, Seoul, South Korea, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2001 and 2011, respectively. From 2001 to 2012, he was with the Electronics and Telecommunications Research Institute (ETRI), Daejeon. From 2012 to 2019, he was with Yeungman University, South Korea. He is currently an Associate Professor with the Department of Electronics and Information Engineering, Korea University, Sejong, South Korea. His research interests include statistical signal processing and communication theory.