Received May 9, 2020, accepted May 20, 2020, date of publication May 29, 2020, date of current version June 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2998742

On Secrecy Performance of Mixed Generalized Gamma and Málaga RF-FSO Variable Gain Relaying Channel

SHEIKH HABIBUL ISLAM[1,*], A. S. M. BADRUDDUZA[2,*], S. M. RIAZUL ISLAM[3,*], (Member, IEEE), FARDIN IBNE SHAHID[1], IMRAN SHAFIQUE ANSARI[4], (Member, IEEE), MILTON KUMAR KUNDU[5], (Member, IEEE), SUBARTO KUMAR GHOSH[1], MD. BIPLOB HOSSAIN[6], A. S. M. SANWAR HOSEN[7], AND GI HWAN CHO[7]

[1]Department of Electrical and Electronic Engineering, Rajshahi University of Engineering and Technology (RUET), Rajshahi 6204, Bangladesh
[2]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology (RUET), Rajshahi 6204, Bangladesh
[3]Department of Computer Science and Engineering, Sejong University, Seoul 05006, South Korea
[4]James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K.
[5]Department of Electrical and Computer Engineering, Rajshahi University of Engineering and Technology (RUET), Rajshahi 6204, Bangladesh
[6]Department of Electrical and Electronic Engineering, Jashore University of Science and Technology (JUST), Jashore 7408, Bangladesh
[7]Division of Computer Science and Engineering, Jeonbuk National University, Jeonju 54896, South Korea

Corresponding authors: A. S. M. Badrudduza (asmb.kanon@gmail.com) and Gi Hwan Cho (ghcho@jbnu.ac.kr)

*S. H. Islam, A. S. M. Badrudduza, and S. M. R. Islam contributed equally to this work and co-first authors.

This work was supported in part by the Jeonbuk National University, in 2020, and in part by the Sejong University Research Faculty Program under Grant 20192021.

ABSTRACT The emergence of an array of new wireless networks has led researchers to evaluate the prospect of utilizing the physical properties of the wireless medium in order to design secure systems. In this paper, the physical layer secrecy performance of a mixed radio frequency-free space optical (RF-FSO) system with variable gain relaying scheme is investigated in the presence of an eavesdropper. We assume that the eavesdropper can wiretap the transmitted confidential data from the RF link only. It is further assumed that the main and eavesdropper RF links are modeled as generalized Gamma (GG) fading channel, and the free space optical (FSO) link experiences Málaga turbulence with pointing error impairment. Our primary concern is to protect this confidential information from being wiretapped. Besides pointing error, the atmospheric turbulence and two types of detection techniques (i.e. heterodyne detection and intensity modulation with direct detection) are also taken into consideration. Utilizing amplify-and-forward (AF) scheme, the novel mathematical closed-form expressions for average secrecy capacity, lower bound of secrecy outage probability, and strictly positive secrecy capacity are derived. As both the links (RF and FSO) undergo generalized fading channels, the derived expressions are also general. We present a unification of some existing works utilizing the proposed model to better clarify the novelty of this work. Finally, all the derived expressions are justified via Monte-Carlo simulations.

INDEX TERMS Physical layer security, generalized gamma fading, Málaga fading, variable gain relay, average secrecy capacity, strictly positive secrecy capacity, secrecy outage probability.

I. INTRODUCTION

A. BACKGROUND

Free space optical (FSO) communication is now growing a lot of interest among researchers due to its immunity to interference, lower cost, wider bandwidth, and higher capacity [1], [2]. This communication operates at an unlicensed optical spectrum, thus providing a solution to the scarcity of radio frequency (RF) resources [3]. This technology is applicable in underwater communication, 'last mile' access, military applications, disaster recovery, etc. [4]. However, in the case of long distance communication, some factors like pointing error and atmospheric turbulence deteriorate the overall performance of FSO networks significantly [5]–[7].

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

A dual-hop mixed RF-FSO system can be considered as a solution to those drawbacks of the FSO technology. In this system, the communication occurs in two hops. The source sends the information to the relay via RF link in the first hop. Subsequently, this signal is converted into optical signal via a relay. That optical signal is finally sent to the receiver via FSO link. The RF-FSO mixed scenario provides an extended cell coverage area. Besides, it also ensures improved received signal quality by employing spatial diversity. These are the main reasons behind widespread interest of the researchers in this technology and such similar systems.

B. LITERATURE SURVEY

Mixed RF-FSO frameworks have been investigated thoroughly in recent years because of its promising nature. The authors in [8] considered an amplify-and-forward (AF) fixed gain relaying technique over Rayleigh - Gamma-Gamma($\Gamma\Gamma$) fading channel and analyzed the performance of this model by deriving the closed-form expression for Outage probability (OP). In [9], the RF-FSO link was modelled with Nakagami-m and $\Gamma\Gamma$ fading channels. The authors here took both HD and IM/DD techniques into consideration and then derived the closed-form expressions for OP, bit error rate (BER), and ergodic capacity (EC). Fixed gain and channel state information (CSI) assisted relaying technique was considered by the authors in [10] for a dual hop mixed RF-FSO system. Here they examined the channels' performance by acquiring the closed-form expressions for OP and bit-error rate (BER). The expressions for OP and average BER for various modulation techniques, such as phase-shift keying (PSK), differential PSK (DPSK), and non-coherent frequency-shift keying (NCFSK), were derived in [11], where the authors used exponentiated-Weibull distribution to model the FSO link. The authors in [12] derived the closed form expressions for EC, OP, and BER over Rayleigh-kappa-mu/inverse Gaussian fading scenarios utilizing the expansion of moment generating function (MGF). The authors in [13] and [14] used identical channel models but different relaying techniques. In [13], closed-form expressions for OP, EC, and BER were obtained for two IM/DD models e.g. input-independent and cost-dependent, using decode-and-forward (DF) relaying, while in [14], OP and EC expressions were obtained for a multi-user scenario using AF relaying technique. The impact of non-zero bore-sight, caused by thermal expansion of the building, was investigated in [15] over Nakagami-m-Málaga mixed channels where the authors derived expressions for OP and average BER (ABER).

Traditional security measures, such as encryption technique is harder to implement in wireless networks consisting of intermediate terminals and relatively simpler end devices. So instead of relying on complicated upper layer security, secured data transmission can be ensured via utilizing the physical properties of the medium that have been proposed in [16]. As the wireless medium is random and inherently time-varying in nature, physical layer security (PLS) has proven to be effective in protecting the secret information from eavesdropping [17]–[20]. Taking advantage of the PLS features, the researchers have performed several analysis to evaluate the secrecy performance of FSO communication systems [21]–[23]. Similar analysis was also performed for mixed RF-FSO systems to show how PLS can protect data [24]–[31]. Considering variable gain relaying technique for both HD and IM/DD techniques, the authors of [24] derived the exact closed-form expression for average secrecy capacity (ASC) over Nakagami-m-Málaga fading model. In [25], a secure simultaneous wireless information and power transfer (SWIPT) system was analyzed over a Nakagami-m-$\Gamma\Gamma$ dual-hop RF-FSO scenario for various detection techniques. The authors derived expressions for secure OP (SOP) and showed that secrecy diversity order (SDO) is affected by the fading parameters, detection techniques, and the pointing error.

The authors in [26] took the effects of imperfect channel state information into consideration and examined its consequence on the SOP with variable and fixed gain relaying techniques. The expressions for average secrecy rate (ASR) and SOP were derived in [27], where the authors considered a highly secure optical link for communication. So the eavesdropper can wiretap only the RF link. The mathematical expressions for SOP and ASC were obtained in [28] for a mixed RF-FSO communication link. Authors also observed that, in case of variable gain relaying scheme, the RF link has little impact on the secrecy performance of the channel, and the HD technique outperforms the IM/DD technique. In [29], the presence of an eavesdropper was assumed to be in the relay-destination link, and the authors deduced the closed-form expressions for SOP and strictly positive secrecy capacity (SPSC) employing DF relaying scheme. In [30], a SWIPT scenario was proposed where the energy receiver acts as a potential eavesdropper. The authors investigated the secrecy capability of the proposed RF-FSO cooperative system with multiple antennas at the receiver by deriving the closed-form expressions for ASC and SOP. The authors in [31] considered a Nakagami-m fading and Málaga mixed two-way relaying (TWR) model with multiple eavesdroppers. Here they deduced the mathematical expressions for SOP and secrecy throughput (ST) to analyze the secrecy performance. Considering Nakagami-m-Málaga fading scenario, the effects of outdated CSI and transmit antenna selection scheme (TAS) were examined in [32]. The authors observed that a higher number of antennas at the source node doesn't substantially improve the secrecy performance.

C. MOTIVATION

The aforecited literature has revealed that the secrecy analysis over RF-FSO system has been performed considering mainly the multipath fading channels for the RF link. But in practice, generalized fading channels are more likely to be encountered during the data transmission as the wireless fading channels are time varying in nature. Hence, a secrecy analysis over a RF-FSO dual hop link, considering generalized fading channels for both the RF and FSO links, is still an open problem for the researchers. Motivated by aforementioned observations, in this work, a secure framework over generalized Gamma (GG)-Málaga fading mixed RF-FSO scenario is proposed in the presence of an eavesdropper. Here the eavesdropper is considered to be able to wiretap the confidential information via the RF link only, as the directivity of the optical beam in the FSO link is very high, and that's why it is highly unlikely that the eavesdropping will occur in the FSO link. We consider two generalized fading environments (GG and Málaga) because a number of famous classical distributions can be obtained as special cases of both fading distributions. For example Weibull, Nakagami-*m*, and Rayleigh fading channels can be obtained from GG fading environment and Málaga model includes Gamma-Rician, Log-Normal, ΓΓ, etc. distributions as its special cases [33], [34].

D. CONTRIBUTIONS

Our main contributions are summarized as follows.

- At first, we realize the probability density functions (PDF) for SNR of each individual hop of the proposed system and then derive the PDF and cumulative distribution function (CDF) of the dual-hop end-to-end SNR. We take atmospheric turbulence, pointing error, and two detection techniques (HD and IM/DD) into consideration.
- Secondly, we investigate the secrecy capability of the mixed RF-FSO system by deriving the closed-form expressions for SOP and SPSC in terms of Meijer's G function. Additionally, we also represent the ASC in terms of extended generalized bivariate Meijer's G function (EGBMGF). To the best of authors' knowledge bsaed on the open literature, these expressions are novel.
- We present some numerical outcomes based on the derived expressions of ASC, SOP, and SPSC. As both of our channels (RF and FSO) are generalized fading channels, the performance of our dual-hop mixed RF-FSO system unifies the secrecy performance of several existing models in the existing literature [35], [36]. This observation proves the novelty and superiority of our model over all the existing works.
- Finally, the accuracy of our analytical expressions are validated by Monte-Carlo simulations. Our analysis demonstrates that the secrecy performance worsens because of the increment in atmospheric turbulence and pointing error. The results also suggest that the HD technique shows better performance than the IM/DD scheme.

E. ORGANIZATION

The rest of the paper has been arranged in the following way. The system model has been described in an elaborate manner in Section II. Closed-form expressions for ASC, SOP, and SPSC are derived in Section III. Analytical and simulation results are presented in Section IV, and finally Section V presents the concluding remarks.

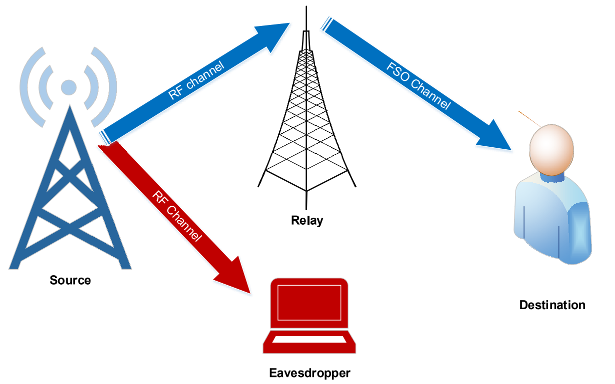


FIGURE 1. The mixed RF-FSO relaying system with source (P), relay (H), destination (K), and eavesdropper (W).

II. SYSTEM MODEL AND PROBLEM FORMULATION

A mixed RF-FSO system is considered in Fig. 1, where a single antenna source, P, is transmitting secret information to a legitimate receiver, K, via an intermediate relay, H. Here, H is equipped with a single transmit aperture and a single receive antenna, and K has one receive aperture. As the distance between P and K is very large, there is no direct link between them, and the communication occurs only through the relay. A single antenna eavesdropper, W, is also present in the network and trying to decode the confidential information from the source. The channel between P and K is the main channel, and the one between P and W is denoted as the eavesdropper channel. The total communication takes place in two separate phases. In the first phase, P transmits confidential information to H via RF link. The relay then converts the RF signal to optical signal and re-transmits this optical signal via FSO link to K in the second phase. The eavesdroppers are assumed passive and can decode information via RF links only. The RF links of main and eavesdropper channel experience independent and identically distributed (i.i.d.) GG fading while the FSO link undergoes the Málaga turbulence.

We denote the channel gains between P and H as $g_{ph} \in \mathbb{C}^{1\times 1}$ and that between P and W as $l_{pw} \in \mathbb{C}^{1\times 1}$, so the signals at H and W can be expressed in the following manner:

$$t_h = g_{ph}\, z + n_h, \tag{1}$$

$$t_w = l_{pw}\, z + m_w, \tag{2}$$

respectively. Here, the signal transmitted from P is denoted as $z \sim \widetilde{\mathcal{N}}(0, P_p)$, the imposed additive white Gaussian noises (AWGN) at H and W are given by $n_h \sim \widetilde{\mathcal{N}}(0, P_h)$ and $m_w \sim \widetilde{\mathcal{N}}(0, P_w)$, respectively, and the terms P_h and P_w symbolize the noise powers.

A. PDF AND CDF OF SNR FOR RF MAIN CHANNEL

The instantaneous signal-to-noise ratio (SNR) of the main RF channel is denoted by $\Psi_R = \frac{P_p}{P_h}\|g_{ph}\|^2$. The PDF of Ψ_R can be expressed as [37, Eq. (2)]

$$f_R(\Psi_R) = M_1 \Psi_R^{M_2} e^{-M_3 \Psi_R^{\tilde{\lambda}_r}}, \tag{3}$$

where $M_1 = \frac{\tilde{\lambda}_r c_r^{c_r}}{\Psi_k^{\tilde{\lambda}_r c_r}\Gamma(c_r)}$, $M_2 = \tilde{\lambda}_r c_r - 1$, $M_3 = c_r \Psi_k^{-\tilde{\lambda}_r}$, $\tilde{\lambda}_r = \frac{\lambda_r}{2}$, λ_r is the fading severity parameter, and c_r is the

TABLE 1. Special cases of GG distribution model.

Envelop distribution	c_r	$\tilde{\lambda}_r$
Rayleigh	1	1
Nakagami-m		1
Weibull	1	
Gamma		1/2
Exponential	1	1/2
Half-normal	1/2	1
AWGN	∞	1
Lognormal	∞	0

TABLE 2. Special cases of Málaga distribution model [34, Table 1].

Envelop distribution	parameters
ΓΓ	$\rho = 1$, then $g_p = 0, \Omega' = 1$
Lognormal	$\rho = 0, g_p \to 0$
Rice-Nakagami	$\rho = 0$
Gamma	$\rho = 0, g_p = 0$

normalized variance. The average SNR of main RF channel is denoted by Ψ_k and $\Gamma(.)$ is the Gamma operator. Utilizing [38, Eq. (3.381.8)], the CDF of Ψ_R is given by [37, Eq. (3)]

$$F_R(\Psi_R) = \frac{\gamma(c_r, M_3 M_2^{\tilde{\lambda}_r})}{\Gamma(c_r)}. \tag{4}$$

Utilizing [38, Eq. (8.352.6)] into (4), the CDF of Ψ_R can be expressed as

$$F_R(\Psi_R) = 1 - e^{-M_3 \Psi_R^{\tilde{\lambda}_r}} \sum_{p_1=0}^{c_r-1} \frac{M_3{}^{p_1} \Psi_R{}^{\tilde{\lambda}_r p_1}}{p_1!}. \tag{5}$$

We consider our RF channels (both main and eavesdropper) experiencing GG distribution due to its flexibility of modeling several well-known small scale fading channels, which are its special cases. This makes it more popular to the researchers to utilize relative to the other conventional models. For instance, some classical distributions modeled from GG Distribution are included in Table 1 [39].

B. PDF AND CDF OF SNR FOR FSO CHANNEL

The Málaga turbulence model is a well-known generalized model that includes some classical turbulence models as its special cases as shown in Table 2. We consider the FSO link experiencing Málaga turbulence with pointing error impairments.

Hence, the PDF of instantaneous SNR of the FSO channel denoted by Ψ_o is expressed as [33]

$$f_o(\Psi_o) = \frac{\epsilon^2 U}{2^r \Psi_o} \sum_{m=1}^{\beta_o} v_m G_{1,3}^{3,0}\left[V \left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \epsilon^2+1 \\ \epsilon^2, \alpha_o, m \end{matrix} \right], \tag{6}$$

where

$$U = \frac{2\alpha_o^{\frac{\alpha_o}{2}}}{g_p^{1+\frac{\alpha_o}{2}} \Gamma(\alpha_o)} \left(\frac{g_p \beta_o}{g_p \beta_o + \Omega'}\right)^{\beta_o + \frac{\alpha_o}{2}},$$

$$V = \frac{\epsilon^2 \alpha_o \beta_o (g_p + \Omega')}{(\epsilon^2+1)(g_p \beta_o + \Omega')},$$

$$v_m = u_m \left(\frac{\alpha_o \beta_o}{g_p \beta_o + \Omega'}\right)^{-\frac{\alpha_o + m}{2}},$$

$$u_m = \binom{\beta_o - 1}{m-1} \frac{(g_p \beta_o + \Omega')^{1-\frac{m}{2}}}{(m-1)!} \left(\frac{\Omega'}{g_p}\right)^{m-1} \left(\frac{\alpha_o}{\beta_o}\right)^{\frac{m}{2}},$$

β_o denotes the fading parameter, α_o denotes a parameter which is related to the effective number of large-scale cells of the scattering process, ϵ is utilized to refer to the ratio of the equivalent beam radius to the pointing error displacement standard deviation (jitter) at the receiver [40], the electrical SNR is denoted by μ_r, r refers to the detection technique utilized i.e. for HD technique ($r = 1$), $\mu_1 = \mathbb{E}(\Psi_o) = \bar{\Psi}_{10}$ which is the average SNR of HD technique and for IM/DD technique ($r = 2$), $\mu_2 = \frac{\alpha_o \epsilon^2 (\epsilon^2+1)^{-2} (\epsilon^2+2)(g_p+\Omega')}{(\alpha_o+1)[2 g_p(g_p+2\Omega')+\Omega'^2(1+1/\beta_o)]} \bar{\Psi}_{20}$ with $\bar{\Psi}_{20}$ being the average SNR of IM/DD technique, the average power of scattering component received by off-axis eddies is denoted by $g_p = \mathbb{E}[|U_S^G|^2] = 2\, b_o(1-\rho)$, the average power of the total scattered components is denoted by $2\, b_o = \mathbb{E}[|U_S^C|^2 + |U_S^G|^2]$, the amount of coupled scattering power to the LOS component is represented by $0 \le \rho \le 1$ parameter, the average power in regard of the coherent contributions is denoted by $\Omega' = \Omega + 2\, b_o \rho + 2\sqrt{2\, b_o \rho \Omega} cos(\phi_A - \phi_B)$, the average power of the LOS component is represented by $\Omega = \mathbb{E}[|U_L|^2]$, the deterministic phases of the LOS are ϕ_A and ϕ_B and G[.] refers to the the Meijer's G function as defined in [38]. The CDF of Ψ_o is expressed as [33, Eq. (11)]

$$F_o(\Psi_o) = R \sum_{m=1}^{\beta_o} w_m G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r} \Psi_o \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix} \right], \tag{7}$$

where $R = \frac{\epsilon^2 U}{2^r (2\pi)^{r-1}}$, $w_m = v_m r^{\alpha_o + m - 1}$, $\chi = \frac{V^r}{r^{2\,r}}$, $s_1 = \left\{\frac{\epsilon^2+1}{r}, \ldots, \frac{\epsilon^2+r}{r}\right\}$ that incorporates r number of terms and $s_2 = \left\{\frac{\epsilon^2}{r}, \ldots, \frac{\epsilon^2+r-1}{r}, \frac{\alpha_o}{r}, \ldots, \frac{\alpha_o+r-1}{r}, \frac{m}{r}, \ldots, \frac{m+r-1}{r}\right\}$ that incorporates $3r$ number of terms.

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

The end-to-end instantaneous SNR of the dual-hop RF-FSO channel considering variable gain relaying is given by [28, Eq. (7)]

$$\Psi_D = \frac{\Psi_o \Psi_R}{\Psi_o + \Psi_R + 1} \approx \min\{\Psi_R, \Psi_o\}. \tag{8}$$

The CDF of Ψ_D can be expressed as [15, Eq. (15)]

$$F_D(\Psi_D) = P_r\{\min\{\Psi_R, \Psi_o\} < \Psi_D\} = F_R(\Psi_D) + F_o(\Psi_D) - F_R(\Psi_D) F_o(\Psi_D). \tag{9}$$

Substituting (5) and (7) into (9), and utilizing some algebraic manipulations, the CDF of Ψ_D is obtained as

$$F_D(\Psi_D) = 1 - e^{-M_3 \Psi_D^{\tilde{\lambda}_r}} \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1} \Psi_D^{\tilde{\lambda}_r p_1}}{p_1!} \times \left[1 - R \sum_{m=1}^{\beta} w_m G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r} \Psi_D \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix} \right]\right]. \tag{10}$$

The PDF of equivalent SNR at the destination for the dual-hop system can be derived by differentiating (9) with respect to Ψ_D as [41, Eq. (12)]

$$\begin{aligned} f_D(\Psi_D) &= \frac{d}{d\Psi_D}[F_D(\Psi_D)] \\ &= f_R(\Psi_D) + f_o(\Psi_D) - f_R(\Psi_D) F_o(\Psi_D) \\ &\quad - f_o(\Psi_D) F_R(\Psi_D) \end{aligned} \tag{11}$$

By substituting (3), (5), (6), and (7) into (11), and utilizing [42, Eq. (2.24.2.3)] and after some algebraic manipulations and simplifications, the PDF of Ψ_D is expressed as

$$\begin{aligned} f_D(\Psi_D) &= M_1 \Psi_D^{M_2} e^{-M_3 \Psi_D^{\tilde{\lambda}_r}} \\ &\quad \times R \sum_{m=1}^{\beta_o} w_m G_{r+1,3r+1}^{3r+1,0}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} s_1, 1 \\ 0, s_2 \end{matrix} \right] \\ &\quad + e^{-M_3 \Psi_D^{\tilde{\lambda}_r}} \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1} \Psi_D^{\tilde{\lambda}_r p_1}}{p_1!} \frac{\epsilon^2 U}{2^r \Psi_o} \\ &\quad \times \sum_{m=1}^{\beta_o} v_m G_{1,3}^{3,0}\left[V\left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \epsilon^2+1 \\ \epsilon^2, \alpha_o, m \end{matrix} \right]. \end{aligned} \tag{12}$$

D. PDF AND CDF OF SNR FOR EAVESDROPPER CHANNEL

The instantaneous SNR of the eavesdropper channel is denoted by $\Psi_E = \frac{P_p}{P_w}\|h_{pw}\|^2$. Similar to (3), the PDF of Ψ_E can be expressed as (3)

$$f_E(\Psi_E) = N_1 \Psi_E^{N_2} e^{-N_3 \Psi_E^{\tilde{\lambda}_e}}, \tag{13}$$

where $N_1 = \frac{\tilde{\lambda}_e c_e^{c_e}}{\Psi_e^{\tilde{\lambda}_e c_e}\Gamma(c_e)}$, $N_2 = \tilde{\lambda}_e c_e - 1$, $N_3 = c_e \Psi_e^{-\tilde{\lambda}_e}$, $\tilde{\lambda}_e = \lambda_e/2$, λ_e is the fading amplitude, c_e is the normalized variance, and the average SNR of eavesdropper channel is Ψ_e. Like (5), the CDF of Ψ_E is expressed as

$$F_E(\Psi_E) = 1 - e^{-N_3 \Psi_E^{\tilde{\lambda}_e}} \sum_{q_1=0}^{c_e-1} \frac{N_3^{q_1} \Psi_E^{\tilde{\lambda}_e q_1}}{q_1!}. \tag{14}$$

III. PERFORMANCE ANALYSIS

A. AVERAGE SECRECY CAPACITY (ASC) ANALYSIS

As the wireless channels are time-varying in nature, ASC is computed as the the average value of instantaneous secrecy capacity that is expressed as [24, Eq. (12)]

$$ASC = \int_0^\infty \frac{1}{1+\Psi_D} F_E(\Psi_D)\left[1 - F_D(\Psi_D)\right] d\Psi_D. \tag{15}$$

By substituting (10) and (14) into (15) and considering $\lambda_r = \lambda_e = 2$, ASC is obtained as (20), as shown at the bottom of the next page. In the following, we derive the terms $\hbar_1$, $\hbar_2$, $\hbar_3$, and $\hbar_4$.

1) DERIVATION OF $\hbar_1$

At first, some simplifications have been done utilizing [42, Eqs. (8.4.2.5), (8.2.2.15) and (8.4.3.1)]. Finally, using [38, Eq. (7.811.1)], the expression of $\hbar_1$ can be obtained as

$$\begin{aligned} \hbar_1 &= \int_0^\infty \frac{\Psi_D^{p_1}}{1+\Psi_D} e^{-M_3\Psi_D} d\Psi_D \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\Psi_D \middle| \begin{matrix} p_1 \\ p_1 \end{matrix}\right] G_{0,1}^{1,0}\left[M_3\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] d\Psi_D \\ &= G_{1,2}^{2,1}\left[M_3 \middle| \begin{matrix} -p_1 \\ 0, -p_1 \end{matrix}\right]. \end{aligned} \tag{16}$$

2) DERIVATION OF $\hbar_2$

Following all the simplification procedures of $\hbar_1$ derivation and utilizing [43, Eq. (20)], finally $\hbar_2$ can be expressed as

$$\begin{aligned} \hbar_2 &= \int_0^\infty \frac{\Psi_D^{p_1}}{1+\Psi_D} e^{-M_3\Psi_D} G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right] d\Psi_D \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\Psi_D \middle| \begin{matrix} p_1 \\ p_1 \end{matrix}\right] G_{0,1}^{1,0}\left[M_3\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right] d\Psi_D \\ &= \frac{1}{M_3} G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} p_1 \\ p_1 \end{matrix} \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix} \middle| \frac{1}{M_3}, \frac{\chi}{\mu_r M_3}\right], \end{aligned} \tag{17}$$

where $G_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}[.]$ represents the extended generalized bivariate Meijer's G function (EGBMGF) that is obtained by utilzing [43] and its implementation is done by utilizing [44, Table 2].

3) DERIVATION OF $\hbar_3$

Similar to $\hbar_1$, the expression for $\hbar_3$ can be expressed as

$$\begin{aligned} \hbar_3 &= \int_0^\infty \frac{\Psi_D^{z}}{1+\Psi_D} e^{-Z\Psi_D} d\Psi_D \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\Psi_D \middle| \begin{matrix} z \\ z \end{matrix}\right] G_{0,1}^{1,0}\left[Z\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] d\Psi_D \\ &= G_{1,2}^{2,1}\left[Z \middle| \begin{matrix} -z \\ 0, -z \end{matrix}\right], \end{aligned} \tag{18}$$

where $Z = M_3 + N_3$ and $z = p_1 + q_1$.

4) DERIVATION OF $\hbar_4$

The final form of $\hbar_4$ has been deduced by following the similar procedures of obtaining $\hbar_2$ as

$$\begin{aligned} \hbar_4 &= \int_0^\infty \frac{\Psi_D^{z}}{1+\Psi_D} e^{-Z\Psi_D} G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right] d\Psi_D \\ &= \int_0^\infty G_{1,1}^{1,1}\left[\Psi_D \middle| \begin{matrix} z \\ z \end{matrix}\right] G_{0,1}^{1,0}\left[Z\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{r+1,3r+1}^{3r,1}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right] d\Psi_D \\ &= \frac{1}{Z} G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} z \\ z \end{matrix} \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix} \middle| \frac{1}{Z}, \frac{\chi}{\mu_r Z}\right]. \end{aligned} \tag{19}$$

B. SECRECY OUTAGE PROBABILITY (SOP) ANALYSIS

The SOP is interpreted as the probability that instantaneous secrecy capacity (C_s) falls below a predetermined threshold,

R_s. The SOP of mixed RF-FSO channel in the presence of an eavesdropper can be expressed as [28, Eq. (10)]

$$\begin{aligned} P_{out}(R_s) &= Pr\{C_s(\Psi_D, \Psi_E) \leq R_s\} \\ &= Pr\{\Psi_D \leq \Theta(\Psi_E+1)-1\} \\ &= \int_0^\infty F_D(\Theta(\Psi_E+1)-1) f_E(\Psi_E) d\Psi_E, \end{aligned} \quad (21)$$

where $\Theta = 2^{R_s}$ and $R_s > 0$. The lower bound of the SOP can be derived as [32, Eq. (7)]

$$\begin{aligned} P_{out}(R_s) &= Pr\{\Psi_D \leq \Theta(\Psi_E+1)-1\} \\ \geq P_{out}^L(R_s) &= Pr\{\Psi_D \leq \Theta\Psi_E\} \\ &= \int_0^\infty F_D(\Theta\Psi) f_E(\Psi) d\Psi. \end{aligned} \quad (22)$$

By substituting (10) and (13) into (22), the SOP is expressed as

$$\begin{aligned} P_{out}^L(R_s) &= 1 - N_1 \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1}\Theta^{\tilde{\lambda}_r p_1}}{p_1!} \int_0^\infty e^{\Xi}\Psi^{\Lambda} \\ &\times \left(1 - R\sum_{m=1}^{\beta_o} w_m G_{r+1,3r+1}^{3r,1}\left[\frac{\Theta\chi}{\mu_r}\Psi \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right]\right) d\Psi, \end{aligned} \quad (23)$$

where $\Xi = -N_3\Psi^{\tilde{\lambda}_e} - M_3(\theta\Psi)^{\tilde{\lambda}_r}$ and $\Lambda = \tilde{\lambda}_e c_e + \tilde{\lambda}_r p_1 - 1$. After completing integration by utilizing the properties of [42, Eqs. (8.4.3.1), (2.24.1.1)], and [38, Eq. (3.326.2)], and assuming a special case with $\lambda_r = \lambda_e = 2$, we derive the final expression of SOP as

$$P_{out}^L(R_s) = 1 - N_1 \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1}\Theta^{p_1}}{p_1!}(\Im_1^L - \Im_2^L), \quad (24)$$

where $\Im_1^L = \frac{\Gamma(c_e+p_1)}{(N_3+M_3\Theta)^{c_e+p_1}}$ and $\Im_2^L = R\sum_{m=1}^{\beta_o} w_m (N_3 + M_3\Theta)^{-c_e-p_1} G_{r+2,3r+1}^{3r,2}\left[\frac{\Theta\chi}{\mu_r(N_3+M_3\Theta)} \middle| \begin{matrix} 1, 1-c_e-p_1, s_1 \\ s_2, 0 \end{matrix}\right]$.

C. STRICTLY POSITIVE SECRECY CAPACITY (SPSC) ANALYSIS

In order to ascertain the secrecy of the transmitted information, the secrecy capacity must be a positive quantity. Otherwise the secrecy performance of the system will be endangered. Mathematically, the SPSC can be defined as [45]

$$\begin{aligned} SPSC &= \Pr(C_s > 0) \\ &= \int_0^\infty \int_0^{\Psi_D} f_D(\Psi_D) f_E(\Psi_E) d\Psi_E d\Psi_D \\ &= \int_0^\infty F_E(\Psi_D) f_D(\Psi_D) d\Psi_D. \end{aligned} \quad (25)$$

By substituting (11) and (14) into (25), the SPSC is expressed as (30), as shown at the bottom of this page, where the terms $\Re_1$, $\Re_2$, $\Re_3$, and $\Re_4$ are obtained utilizing [42, Eq. (2.24.2.3)] and considering $\lambda_r = \lambda_e = 2$ as follows.

1) DERIVATION OF $\Re_1$

Utilizing [42, Eqs.(8.4.3.1) & (2.24.1.1)], $\Re_1$ can be expressed as

$$\begin{aligned} \Re_1 &= \int_0^\infty \Psi_D^{c_r-1} e^{-M_3\Psi_D} G_{r+1,3r+1}^{3r+1,0}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} s_1, 1 \\ 0, s_2 \end{matrix}\right] d\Psi_D \\ &= \int_0^\infty \Psi_D^{c_r-1} G_{0,1}^{1,0}\left[M_3\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{r+1,3r+1}^{3r+1,0}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} s_1, 1 \\ 0, s_2 \end{matrix}\right] d\Psi_D \\ &= \frac{1}{M_3^{c_r}} G_{r+2,3r+1}^{3r+1,1}\left[\frac{\chi}{M_3\mu_r} \middle| \begin{matrix} 1-c_r, s_1, 1 \\ 0, s_2 \end{matrix}\right]. \end{aligned} \quad (26)$$

2) DERIVATION OF $\Re_2$

Similar to the derivation of $\Re_1$, $\Re_2$ can be expressed as

$$\begin{aligned} \Re_2 &= \int_0^\infty \Psi_D^{p_1-1} e^{-M_3\Psi_D} G_{1,3}^{3,0}\left[V\left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \epsilon^2+1 \\ \epsilon^2, \alpha_o, m \end{matrix}\right] d\Psi_D \\ &= \int_0^\infty \Psi_D^{p_1-1} G_{0,1}^{1,0}\left[M_3\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \\ &\quad \times G_{1,3}^{3,0}\left[V\left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \epsilon^2+1 \\ \epsilon^2, \alpha_o, m \end{matrix}\right] d\Psi_D \\ &= \frac{r^{\alpha_o+m-1}}{(2\pi)^{r-1}} \times \Re_2', \end{aligned} \quad (27)$$

where $\Re_2' = \frac{1}{M_3^{p_1}} G_{r+1,3r}^{3r,1}\left[\frac{\chi}{M_3\mu_r} \middle| \begin{matrix} 1-p_1, s_1 \\ s_2 \end{matrix}\right]$.

3) DERIVATION OF $\Re_3$

The expressions of $\Re_3$ is deduced as

$$\begin{aligned} \Re_3 &= \int_0^\infty \Psi_D^{c_r+q_1-1} e^{-Z\Psi_D} G_{r+1,3r+1}^{3r+1,0}\left[\frac{\chi}{\mu_r}\Psi_D \middle| \begin{matrix} s_1, 1 \\ 0, s_2 \end{matrix}\right] d\Psi_D \\ &= \int_0^\infty \Psi_D^{c_r+q_1-1} G_{0,1}^{1,0}\left[Z\Psi_D \middle| \begin{matrix} - \\ 0 \end{matrix}\right] \end{aligned}$$

$$ASC = \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1}}{p_1!}\left[\hbar_1 - R\sum_{m=1}^{\beta_o} w_m \hbar_2 - \sum_{q_1=0}^{c_e-1} \frac{N_3^{q_1}}{q_1!}\left(\hbar_3 - R\sum_{m=1}^{\beta_o} w_m \hbar_4\right)\right]. \quad (20)$$

$$SPSC = \sum_{m=1}^{\beta_o} R w_m \left[M_1\left(\Re_1 - \sum_{q_1=0}^{c_e-1} \frac{N_3^{q_1}}{q_1!}\Re_3\right) + \sum_{p_1=0}^{c_r-1} \frac{M_3^{p_1}}{p_1!}\left(\Re_2' - \sum_{q_1=0}^{c_e-1} \frac{N_3^{q_1}}{q_1!}\Re_4'\right)\right]. \quad (30)$$

$$\times G_{r+1,3r+1}^{3r+1,0}\left[\frac{\chi}{\mu_r}\Psi_D\middle|\begin{matrix}s_1,1\\0,s_2\end{matrix}\right]d\Psi_D$$
$$=\frac{1}{Z^{c_r+q_1}}G_{r+2,3r+1}^{3r+1,1}\left[\frac{\chi}{Z\mu_r}\middle|\begin{matrix}1-q_1-c_r,s_1,1\\0,s_2\end{matrix}\right].\quad(28)$$

4) DERIVATION OF $\Re_4$

Following the similar procedures of obtaining $\Re_2$, $\Re_4$ can be expressed as

$$\begin{aligned}\Re_4 &= \int_0^\infty \Psi_D^{z-1}e^{-Z\Psi_D}G_{1,3}^{3,0}\left[V\left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}}\middle|\begin{matrix}\epsilon^2+1\\\epsilon^2,\alpha_o,m\end{matrix}\right]d\Psi_D\\
&= \int_0^\infty \Psi_D^{z-1}G_{0,1}^{1,0}\left[M_3\Psi_D\middle|\begin{matrix}-\\0\end{matrix}\right]\\
&\quad\times G_{1,3}^{3,0}\left[V\left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}}\middle|\begin{matrix}\epsilon^2+1\\\epsilon^2,\alpha_o,m\end{matrix}\right]d\Psi_D\\
&= \frac{r^{\alpha_o+m-1}}{(2\pi)^{r-1}}\times\Re_4',\end{aligned}\quad(29)$$

where $\Re_4'=\frac{1}{Z^z}G_{r+1,3r}^{3r,1}\left[\frac{\chi}{Z\mu_r}\middle|\begin{matrix}1-z,s_1\\s_2\end{matrix}\right]$.

D. SIGNIFICANCE OF OUR ANALYSIS

Our main target in this work is to enhance the level of security of the proposed network by taking advantage of the physical properties of RF-FSO propagation medium. To accomplish this task, we relate all the system parameters with three well-known secrecy measures i.e. ASC, SOP, and SPSC. As per the authors' knowledge based on the open literature, we are the first to derive the expressions in (20), (24), and (30) corresponding to our proposed model, and hence our derived expressions are totally novel. It is noteworthy to point out that for the special case of Rayleigh-ΓΓ scenario, our derived expressions in (24) reduce to the expressions of [35, Eqs. (15)]. Again for the scenario of Nakagami-*m*-ΓΓ fading system as a special case of our model, the expressions presented in (20) and (24) agree with the results of [36, Eqs. (13) & (20)].

IV. NUMERICAL RESULTS

This section illustrates the analytical results corresponding to the closed-form expressions of ASC, SPSC, and SOP. Additionally, the impact of fading, pointing errors, and atmospheric turbulence on the secrecy performance of the proposed framework are also determined. Besides, we also present Monte-Carlo simulations via MATLAB in order to validate the derived analytical expressions. We assume $\lambda_r=\lambda_e=2$ while deriving the expressions in closed-form, but impact of λ_r and λ_e on the system performance are demonstrated below via numerical methods. Other parameters used for both the simulations and analysis are set as $(\alpha_o,\beta_o)=(2.296,2)$ for strong turbulence, $(\alpha_o,\beta_o)=(4.2,3)$ for moderate turbulence, and $(\alpha_o,\beta_o)=(8,4)$ for weak turbulence similar to [33], r = 1 (HD technique) and 2 (IM/DD technique), and $R_s=0.5$ bits/sec/Hz.

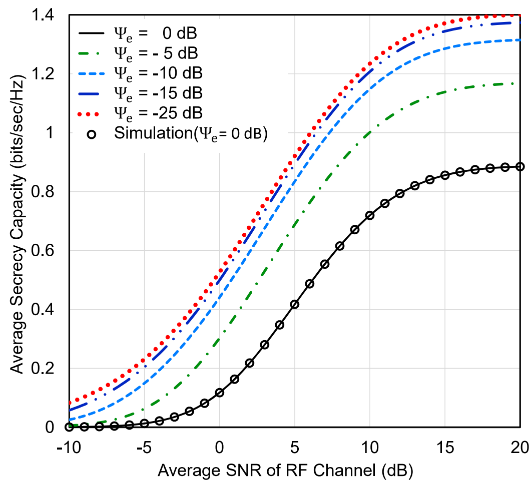


FIGURE 2. The ASC versus Ψ_k for selected values of Ψ_e where $\lambda_r=3$, $\lambda_e=c_r=c_e=2$, $\alpha_o=\beta_o=g_p=2$, $\Omega'=\epsilon=r=1$, and $\bar{\Psi}_{10}=8$dB.

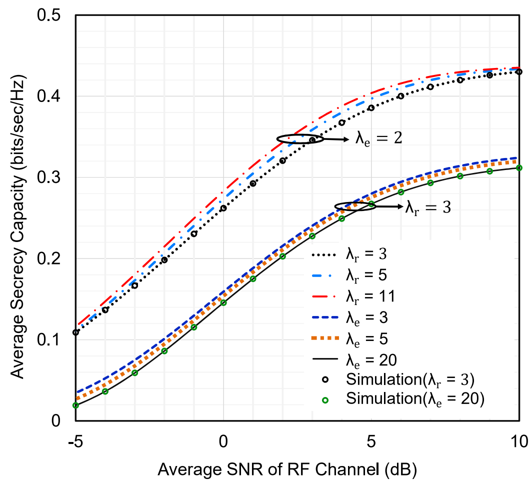


FIGURE 3. The ASC versus Ψ_k for selected values of λ_r and λ_e where $c_r=c_e=2$, $\alpha_o=\beta_o=g_p=2$, $\Omega'=\epsilon=r=1$, $\Psi_e=-10$dB, and $\bar{\Psi}_{10}=0$dB.

In order to investigate the effect of Ψ_e on the secrecy capacity, the ASC is plotted against Ψ_k for selected values of Ψ_e in Fig. 2. An increase in Ψ_e reduces the ASC, as testified in [24]. This is because the lower value of Ψ_e indicates weaker SNR at the eavesdropper terminal. The simulated results demonstrate exact similarities with the analytic results which ensures that our derived expressions are correct.

In Fig. 3, we investigate the impact of fading severity parameters on the ASC for specific values of λ_e and λ_r. We observe that ASC improves for a higher value of λ_r as a higher value of λ_r signifies lower amount of fading in the main channel. On the other hand, ASC decreases for a higher value of λ_e. This is expected because higher value of λ_e denotes weak fading between the source and eavesdropper channel.

A comparison between the two detection techniques is performed in terms of ASC, SPSC, and SOP in Figs. 4, 5,

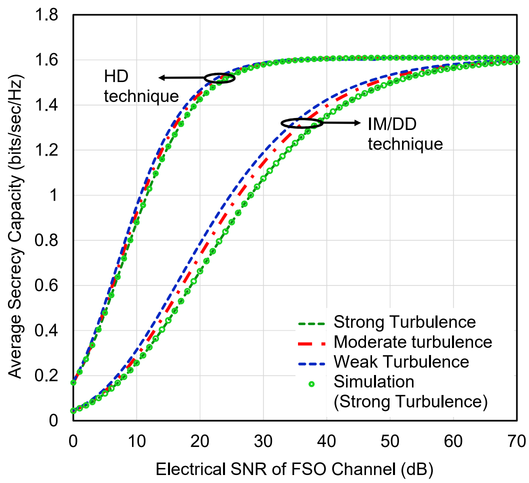


FIGURE 4. **The ASC versus $\bar{\Psi}_{10}$ and $\bar{\Psi}_{20}$ for selected values of α_o and β_o where $\lambda_r = \lambda_e = 3$, $c_r = c_e = 2$, $\Omega' = \epsilon = 1$, $g_p = 2$, $\Psi_k = 10$dB, and $\Psi_e = 0$dB.**

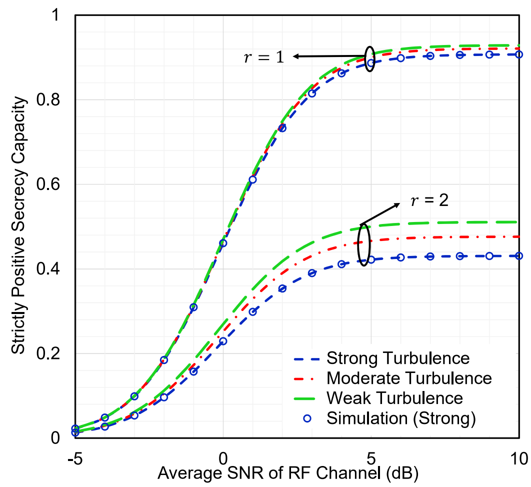


FIGURE 6. **The SPSC versus Ψ_k for selected values of α_o and β_o where $\lambda_r = \lambda_e = 4$, $c_r = c_e = 2$, $\Omega' = 1$, $g_p = 2$, $\epsilon = 1$, $\Psi_e = 0$dB, and $\bar{\Psi}_{10} = \bar{\Psi}_{20} = 15$dB.**

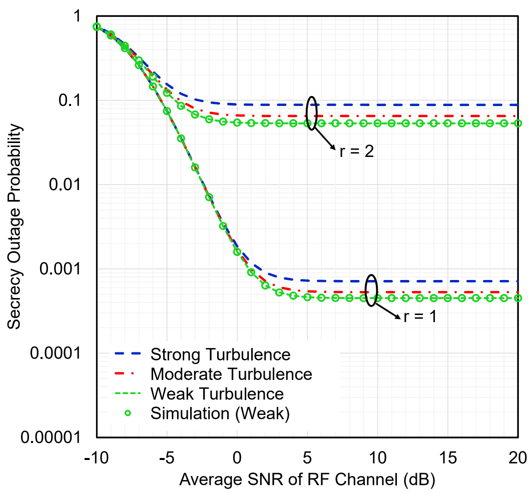


FIGURE 5. **The SOP versus Ψ_k for selected values of α_o and β_o where $\lambda_r = \lambda_e = 4$, $c_r = c_e = 2$, $\Omega' = 1$, $g_p = 2$, $\epsilon = 6.7$, $\Psi_e = -10$dB, and $\bar{\Psi}_{10} = \bar{\Psi}_{20} = 25$dB.**

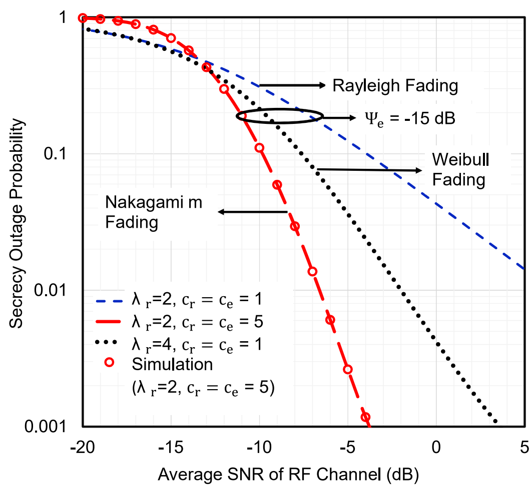


FIGURE 7. **The SOP versus Ψ_k for selected values of λ_r, c_r and c_e of different channels with $\lambda_e = 2$, $\alpha_o = 2.296$, $\beta_0 = g_p = 2$, $\Omega' = r = \epsilon = 1$, $\Psi_e = -15$dB, and $\bar{\Psi}_{10} = 25$dB.**

and 6, respectively, where HD technique ($r = 1$) outperforms the IM/DD technique ($r = 2$). Compared to IM/DD technique, the SNR at destination tends to be higher for HD technique, thus it demonstrates better performance, as testified in [9], [46], and [47]. In addition, we observe that the secrecy performance also varies significantly with various levels of turbulence. It can clearly be seen that better performance is obtained for weaker turbulence compared to stronger turbulence for both HD and IM/DD techniques. This indicates that stronger turbulence affects the SNR at K more significantly than the weaker turbulence. Same conclusions were also made in [9].

Since the main RF link is modelled as generalized Gamma fading channel, the SOP is plotted versus Ψ_k in Fig. 7 to demonstrate the generic nature of this generalized fading channel. It is observed that several multipath fading scenarios can be obtained from this fading model simply by tweaking the fading parameter and normalized variance. It is evident that the SOP is worst for Rayleigh fading model whereas it is considerably better for Nakagami-*m* fading channel.

The impact of pointing error is examined in Figs. 8 and 9. For this purpose ASC and SOP are plotted versus average SNR of RF channel for selected values of λ_r, λ_e, and ϵ. It is observed that both the secrecy capacity and the secure outage performance improve significantly when pointing error is negligible ($\epsilon = 6.7$), whereas the performances deteriorate when the pointing error is strong ($\epsilon = 1$). This improvement in secrecy capacity occurs as higher values of ϵ leads to better pointing accuracy that matches well with the results of [9].

Comparison With Existing Works: We consider two generalized fading scenarios to model the RF and FSO links e.g. the RF link experiences generalized Gamma fading while the

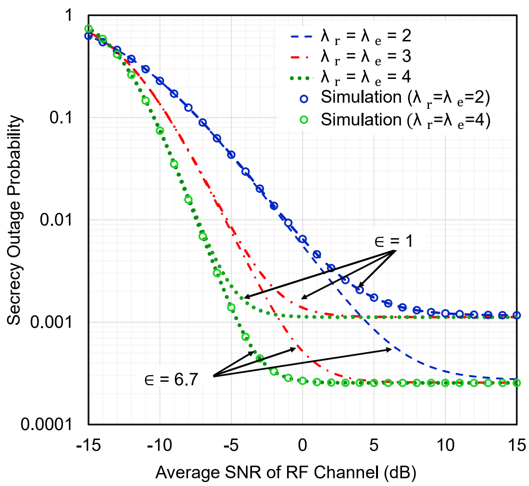


FIGURE 8. The SOP versus Ψ_k for selected values of λ_r and λ_e with $\epsilon = (1, 6.7)$, $\alpha_o = \beta_o = g_p = 2$, $c_r = c_e = 2$, $\Omega' = r = 1$, $\Psi_e = -15$dB, and $\bar{\Psi}_{10} = 25$dB.

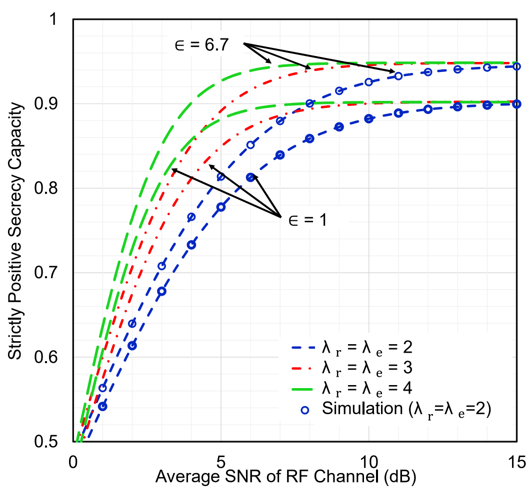


FIGURE 9. The SPSC versus Ψ_k for selected values of λ_r and λ_e where $c_r = c_e = 2$, $\alpha_o = \beta_o = g_p = 2$, $\Omega' = r = 1$, $\Psi_e = 0$dB, and $\bar{\Psi}_{10} = 15$dB.

FSO link experiences Málaga turbulence with pointing errors. Hence, our proposed model unifies the secrecy performance of several classical RF-FSO fading scenarios [34], [37] that are available in the existing literature. For example, Rayleigh-$\Gamma\Gamma$ model [35] is obtained by setting $\lambda_r = 2, c_r = 1$, $\rho = 1$ and $\Omega' = 1$. Again for $\lambda_r = 2$, $\rho = 1$, and $\Omega' = 1$, we obtain Nakagami-m-$\Gamma\Gamma$ scenario [36], where c_r denotes Nakagami-m fading parameter. To generate a Rayleigh-Lognormal mixed fading scenario, the parameters would be $\lambda_r = 2$, $c_r = 1$, $\rho = 0$ and $g_p \to 0$. Besides these special cases, Weibull fading model also exhibits accurate fit to the measurements of experimental fading channels. We can use our proposed model to easily generate a secure Weibull-$\Gamma\Gamma$/Lognormal/Gamma environment with $c_r = 1$ where λ_r represents the Weibull fading parameter. This mixed combination of Weibull distribution with $\Gamma\Gamma$, Lognormal,

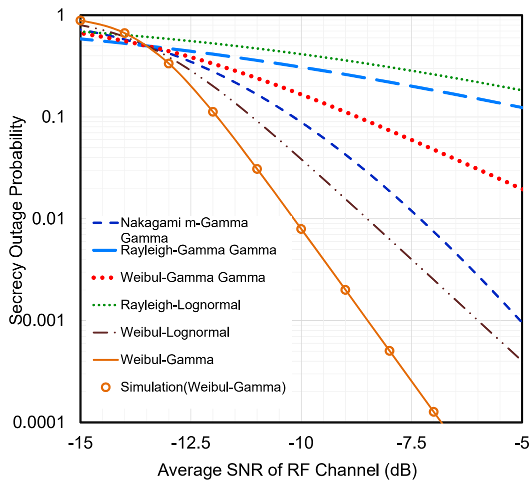


FIGURE 10. The SOP versus Ψ_k for selected values of λ_r, λ_e, c_r, c_e, ρ and Ω' of different channels with $\alpha_o = 2.296$, $\beta_0 = 2$, $r = 1$, $\epsilon = 6.7$, $\bar{\Psi}_{10} = 25$dB.

TABLE 3. Generic nature of proposed model.

Distribution	Parameters
Nakagami-m-$\Gamma\Gamma$	$\lambda_r = 2, \lambda_e = 2, c_r = 6, c_e = 6, \rho = 1, g_p = 0, \Omega' = 1.$
Rayleigh-$\Gamma\Gamma$	$\lambda_r = 2, \lambda_e = 2, c_r = 1, c_e = 1, \rho = 1, g_p = 0, \Omega' = 1.$
Weibull-$\Gamma\Gamma$	$\lambda_r = 4, \lambda_e = 4, c_r = 1, c_e = 1, \rho = 1, g_p = 0, \Omega' = 1.$
Rayleigh-Lognormal	$\lambda_r = 2, \lambda_e = 2, c_r = 1, c_e = 1, \rho = 0, g_p = 0.0001.$
Weibull-Lognormal	$\lambda_r = 8, \lambda_e = 8, c_r = 1, c_e = 1, \rho = 0, g_p = 0.0001.$
Weibull-Gamma	$\lambda_r = 12, \lambda_e = 12, c_r = 1, c_e = 1, \rho = 0, g_p = 0.$

and Gamma distributions to model the RF and FSO links is totally absent in the existing literature.

The above mentioned generic nature of our proposed model has been demonstrated in Fig. 10 by plotting the SOP against Ψ_k. The results demonstrate that our model unifies the performance of various distributions which are summarized in Table 3.

Based on the observations it is trustworthy that our proposed work is novel and most generalized relative to all other existing works.

V. CONCLUSION

This paper deals with the secrecy performance analysis of dual-hop mixed RF-FSO system in the presence of an eavesdropper. The novel closed-form expressions for ASC, SOP, and SPSC are derived and validated through Monte-Carlo simulations. HD and IM/DD techniques were utilized to detect the signals at the receiver. Based on the numerical results, we can confirm that HD technique is a superior approach for obtaining improved secrecy performance because of its enhanced ability to reduce the detrimental impacts of fading, atmospheric turbulence, and pointing error, compared to the IM/DD technique.

REFERENCES

[1] M. Safari and M. Uysal, "Relay-assisted free-space optical communication," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5441–5449, Dec. 2008.

[2] W. Gappmair, "Further results on the capacity of free-space optical channels in turbulent atmosphere," *IET Commun.*, vol. 5, no. 9, pp. 1262–1267, Jun. 2011.

[3] B. Makki, T. Svensson, and M.-S. Alouini, "On the performance of millimeter wave-based RF-FSO links with HARQ feedback," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[4] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, Nov. 2014.

[5] M. T. Dabiri, M. J. Saber, and S. M. S. Sadough, "On the performance of multiplexing FSO MIMO links in log-normal fading with pointing errors," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 974–983, Nov. 2017.

[6] M. A. Amirabadi and V. T. Vakili, "A new optimization problem in FSO communication system," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1442–1445, Jul. 2018.

[7] F. Nadeem, V. Kvicera, M. S. Awan, E. Leitgeb, S. S. Muhammad, and G. Kandus, "Weather effects on hybrid FSO/RF communication link," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1687–1697, Dec. 2009.

[8] E. Lee, J. Park, D. Han, and G. Yoon, "Performance analysis of the asymmetric dual-hop relay transmission with mixed RF/FSO links," *IEEE Photon. Technol. Lett.*, vol. 23, no. 21, pp. 1642–1644, Nov. 1, 2011.

[9] E. Zedini, I. S. Ansari, and M.-S. 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, Art. no. 7900120.

[10] E. Soleimani-Nasab and M. Uysal, "Generalized performance analysis of mixed RF/FSO cooperative systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 714–727, Jan. 2016.

[11] J. Zhao, S.-H. Zhao, W.-H. Zhao, Y. Liu, and X. Li, "Performance of mixed RF/FSO systems in exponentiated Weibull distributed channels," *Opt. Commun.*, vol. 405, pp. 244–252, 2017.

[12] 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.

[13] 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.

[14] R. Li, T. Chen, L. Fan, and A. Dang, "Performance analysis of a multiuser dual-hop amplify-and-forward relay system with FSO/RF links," *J. Opt. Commun. Netw.*, vol. 11, no. 7, pp. 362–370, Jul. 2019.

[15] K. O. Odeyemi and P. A. Owolawi, "Impact of non-zero boresight pointing errors on multiuser mixed RF/FSO system under best user selection scheme," *Int. J. Microw. Opt. Technol.*, vol. 14, no. 3, pp. 210–222, Jun. 2019.

[16] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[17] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[18] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6423–6436, Dec. 2018.

[19] H. Fang, L. Xu, and K. K. R. Choo, "Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks," *Appl. Math. Comput.*, vol. 296, pp. 153–167, Mar. 2017.

[20] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *Comput. Secur.*, vol. 50, pp. 47–59, May 2015.

[21] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–10, Feb. 2016.

[22] 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.

[23] 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.

[24] M. J. Saber and A. Keshavarz, "On secrecy performance of mixed Nakagami-*m* and Málaga RFIFSO variable gain relaying system," in *Proc. Iranian Conf. Electr. Eng. (ICEE)*, May 2018, pp. 354–357.

[25] 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.

[26] 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.

[27] L. Yang, T. Liu, J. Chen, and M.-S. 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, Dec. 2018.

[28] 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.

[29] 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.

[30] 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.

[31] D. R. Pattanayak, V. K. Dwivedi, and V. Karwal, "Physical layer security of a two way relay based mixed FSO/RF network in the presence of multiple eavesdroppers," *Opt. Commun.*, vol. 463, May 2020, Art. no. 125429.

[32] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, early access, Apr. 2, 2020, doi: 10.1109/TCOMM.2020.2985028.

[33] 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.

[34] A. Jurado-Navas, J. M. Garrido-Balsells, J. F. Paris, A. Puerta-Notario, and J. Awrejcewicz, "A unifying statistical model for atmospheric optical scintillation," in *Numerical Simulations of Physical and Engineering Processes*, vol. 181. Rijeka, Croatia: InTech, 2011.

[35] 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.

[36] 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, Jul. 2017.

[37] 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.

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

[39] J.-Y. Wang, J.-B. Wang, M. Chen, and J. Dai, "Average SER performance of distributed antenna systems over shadowed generalized-gamma channels for different modulation schemes," *Wireless Pers. Commun.*, vol. 75, no. 2, pp. 1099–1114, 2014.

[40] H. G. Sandalidis, T. A. Tsiftsis, and G. K. Karagiannidis, "Optical wireless communications with heterodyne detection over turbulence channels with pointing errors," *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4440–4445, Oct. 15, 2009.

[41] S. Anees and M. R. Bhatnagar, "On the capacity of decode-and-forward dual-hop free space optical communication systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 18–23.

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

[43] 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.

[44] 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.

[45] 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.
[46] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Performance analysis of FSO links over unified gamma-gamma turbulence channels," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.
[47] 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.

SHEIKH HABIBUL ISLAM is currently pursuing the B.Sc. degree in Electrical & Electronic Engineering (EEE) with the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh. His research interests include free space optical communication, physical layer security, and NOMA systems.

A. S. M. BADRUDDUZA received the B.Sc. and M.Sc. degrees in Electrical & Electronic Engineering (EEE) from the Rajshahi University of Engineering and 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 and Technology, Rajshahi. He has been working as a Lecturer with the Department of Electronics and Telecommunication Engineering (ETE), RUET, since July 2017. His research interests include information-theoretic security in multicast, cellular and cooperative networks, physical layer security of RF/FSO, and NOMA systems.

S. M. RIAZUL ISLAM (Member, IEEE) has been working as an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, South Korea, since March 2017. He is a Distinguished Professor with the Chongqing College of Electronic Engineering, China. From 2014 to 2017, he worked at the Wireless Communications Research Center, 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. From 2005 to 2014, he was with the University of Dhaka, Bangladesh, as an Assistant Professor and a Lecturer with the Department of Electrical and Electronic Engineering. In 2014, he worked at the Department of Solution Lab, Samsung R&D Institute Bangladesh (SRBD), as a Chief Engineer. His research interests include wireless communications, 5G and the IoT, wireless health, bioinformatics, and machine learning.

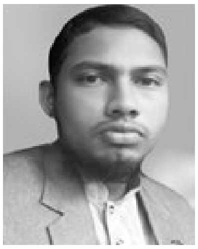
FARDIN IBNE SHAHID is currently pursuing the B.Sc. degree in EEE with the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh. His research interests include physical layer security, cooperative communication, and FSO communication.

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. Since August 2018, he has been a Lecturer (Assistant Professor) with the University of Glasgow, Glasgow, U.K. Prior to this, from November 2017 to July 2018, he was a Lecturer (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. 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 been affiliated with IEEE, since 2007, and has served in various capacities. He has been serving on the IEEE Nominations and Appointments (N&A) Committee, since February 2020, and the IEEE Communication Society Young Professionals (ComSoc YP) Board, since April 2016. He is part of the IEEE 5G Tech Focus Publications Editorial Board, since February 2017. 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 for an Exemplary Reviewer for the IEEE Transaction on Communications, in 2018 and 2016, and the IEEE Wireless Communications Letters, in 2017 and 2014, a recipient of post-doctoral research award (PDRA) (first cycle) with Qatar national research foundation (QNRF), in 2014, and a recipient of IEEE Richard E. Merwin student scholarship award, in July 2013. He has authored/coauthored more than 95 journal and conference publications. He has co-organized the GRASNET'2016, 2017, 2018 workshops in conjunction with IEEE WCNC'2016, 2017 and IEEE Globecom 2018.

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

SUBARTO KUMAR GHOSH received the B.Sc. degree in Electrical & Electronic Engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in 2012. After graduation in January 2013, he joined as a Lecturer at the Department of EEE, Daffodil International University (DIU), Dhaka, Bangladesh. In September 2015, he joined as a Lecturer at the Department of EEE, RUET, where he is currently an Assistant Professor. His research interests include communication systems and control theory application in distribution generation systems.



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 & Electronic Engineering (EEE). In 2016, he was appointed as a Lecturer at 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 was working 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 with the Department of Electrical and Electronic Engineering 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. He had been awarded University Technical Scholarship at RUET for his outstanding academic results, from 2012 to 2015. He has been got Deanship of the Scientific Research (DSR) fund from King Abdulaziz University (KAU), Jeddah, Saudi Arabia, from 2019 to 2020. His research interests are 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.

A. S. M. SANWAR HOSEN received the M.S. and Ph.D. degrees in CSE from JBNU, in 2013 and 2017, respectively. He worked as a Postdoctoral Researcher with the School of Computer, Information and Communication Engineering, Kunsan National University, Gunsan, South Korea, and with the division at JBNU. He is currently an Assistant Professor (Research) with the Division of Computer Science and Engineering (CSE), Jeonbuk National University (JBNU), Jeonju, South Korea. He has published several papers in journals and international conferences, and serves as a reviewer of several reputed journals. His research interests are in wireless sensor networks, the Internet of Things, network security, data distribution services, fog-cloud computing, artificial intelligence, blockchain, and green IT.

GI HWAN CHO received the B.S. degree in computer science from Chonnam University, Gwangju, South Korea, in 1985, the M.S. degree in computer science from Seoul National University, Seoul, South Korea, in 1987, and the Ph.D. degree in computing science from The University of Newcastle, Newcastle Upon Tyne, U.K., in 1996. He worked at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea, as a Senior Member of Technical Staff, from September 1987 to August 1997, for the Department of Computer Science at Mokpo National University, Mokpo, South Korea, as a full time Lecturer, from September 1997 to February 1999. Since March 1999, he has been with the Division of Computer Science and Engineering, Jeonbuk National University, Jeonju, South Korea, and he is currently serving as a Professor. His current research interests include mobile computing, computer communication, security on wireless networks, wireless sensor networks, and distributed computing systems.