Open Access

Impact of Correlation and Pointing Error on Secure Outage Performance Over Arbitrary Correlated Nakagami-m and $\mathcal{M}$-Turbulent Fading Mixed RF-FSO Channel

Sheikh Habibul Islam
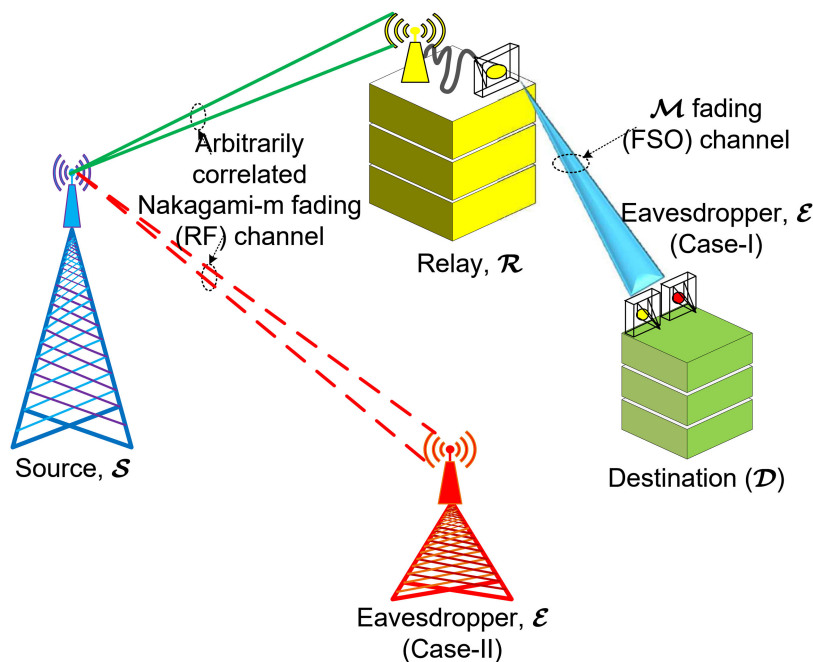**A. S. M. Badrudduza,** *Member, IEEE*
S. M. Riazul Islam, *Member, IEEE*
Fardin Ibne Shahid
Imran Shafique Ansari, *Member, IEEE*
Milton Kumar Kundu, *Member, IEEE*
Heejung Yu , *Senior Member, IEEE*

Impact of Correlation and Pointing Error on Secure Outage Performance Over Arbitrary Correlated Nakagami-*m* and $\mathcal{M}$-Turbulent Fading Mixed RF-FSO Channel

Sheikh Habibul Islam ⓘ,[1] **A. S. M. Badrudduza** ⓘ,[2] *Member, IEEE*,
S. M. Riazul Islam ⓘ,[3] *Member, IEEE*, **Fardin Ibne Shahid** ⓘ,[1]
Imran Shafique Ansari ⓘ,[4] *Member, IEEE*,
Milton Kumar Kundu ⓘ,[5] *Member, IEEE*,
and Heejung Yu ⓘ,[6] *Senior Member, IEEE*

[1]Department of Electrical & Electronic Engineering, Rajshahi University of Engineering & Technology (RUET), Rajshahi 6204, Bangladesh
[2]Department of Electronics & Telecommunication Engineering, Rajshahi University of Engineering & 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 & Computer Engineering, Rajshahi University of Engineering & Technology (RUET), Rajshahi 6204, Bangladesh
[6]Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea

Abstract: In Radio Frequency (RF)-Free Space Optical (FSO) mixed links, secrecy capacity (SC) can be improved by exploiting spatial diversity (i.e., antenna diversity) in the RF path. In addition to atmospheric turbulence and point error of the FSO link, antenna correlation in the RF link can significantly deteriorate the secrecy performance. In this paper, a secrecy rate of wiretap channels with a single source, relay, destination, and eavesdropper is analyzed under practical environments with the aforementioned impairments. The RF hop (source-to-relay) and the FSO hop (relay-to-destination) are modeled utilizing arbitrarily correlated Nakagami-*m* and Málaga ($\mathcal{M}$) distributions, respectively. The correlated signal branches of the RF hop are combined at the relay exploiting equal gain combining reception technique. We assume that the eavesdropper is capable of wiretapping via RF and FSO links separately. We derive novel closed-form expressions for secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC) considering heterodyne detection (HD) and intensity modulation with direct detection (IM/DD) techniques in order to examine the impact of atmospheric scintillation, pointing error, fading, and correlation on the system's secrecy performance. It is shown that the HD technique exhibits a better performance

than an IM/DD technique. In addition, similar to the pointing error and turbulent fading, the correlation imposes a detrimental impact on SC. Finally, Monte-Carlo simulation results are provided for validation of the derived expressions.

Index Terms: $\mathcal{M}$ fading, correlation, eavesdropper, FSO communication, physical layer security.

1. Introduction

1.1 Background Study

In the last few years, data traffic in the radio frequency (RF) range has increased at an unprecedented rate. The resulting shortage of licensed radio spectrum for wireless data transfer has driven researchers into evaluating the plausibility of free-space optical (FSO) network as a replacement [1]–[4]. FSO has comparatively higher speed and larger bandwidth. FSO technology has numerous applications including storage area network (SAN), last-mile access, enterprise connectivity, Fiber backup, metropolitan area network (MAN) extension, backhaul network, local area network (LAN) to LAN connectivity, military communication, and quantum key distribution, among many others [5]–[8]. However, in FSO technology, line of sight (LOS) between the source ($\mathcal{S}$) and destination ($\mathcal{D}$) is required for satisfactory operation, and the presence of fog, dust, and rain restrict the practical range of the system; these being the main reasons as to why FSO is yet to be implemented on a mass scale [9]. Pointing error, which results from the misalignment between the transmitter and the receiver, also severely degrades the overall performance of the system [10]. A mixed RF-FSO system has been suggested as a possible solution to overcome the limitations of both technologies. In this network, complete communication is divided into two phases. The larger portion of the network, i.e. the path between the source and relay ($\mathcal{R}$), is covered utilizing RF technology. In the second phase, the relatively smaller distance, i.e. the relay to destination link, is covered utilizing FSO technology. The shorter range and comparatively higher speed, i.e., wider bandwidth, also warrant FSO as an interesting prospect for finally solving the problem with the last mile access [11].

1.2 Related Works

Over the years, the efficacy of an FSO system has been verified in terms of bit error rate (BER), ergodic capacity (EC), and outage probability (OP) [12]–[14]. Later, the alike approach was supervised by researchers for mixed RF-FSO systems as well. In [15], the authors quantified the performance of the mixed RF-FSO system by deriving the closed-form expression for EC. They also concluded that the performance of a mixed RF-FSO system tends to be slightly worse than that of an RF-RF system. The consequence of atmospheric disturbance and pointing error on the overall performance of the system was analyzed in [16], and the authors utilized Rayleigh and $\Gamma\Gamma$ distributions to model the RF and FSO links, respectively. In [17], the authors took two IM-DD channel models into account alongside HD detection, and then analyzed the performance of the mixed system in terms of OP, average BER, and ergodic channel capacity. The authors in [18] used the Málaga ($\mathcal{M}$) distribution for modeling the FSO link, and this, in turn, enabled them to unify several other existing works because $\mathcal{M}$ distribution engulfs several distributions as its special cases. The performance of a mixed system for both fixed gain and variable gain relaying technique was studied in [19], and therein, the authors derived closed-form expressions for OP, BER, and EC. The effectiveness of a mixed RF-FSO network for fifth-generation (5G) mobile communication was also analyzed in [20]. However, in all these works a single antenna source was communicating with a relay that was also equipped with a single antenna and a single aperture. The lack of antennas in the RF hop made the whole system susceptible to fading since the larger part of the mixed network was dependent on RF technology. Diversity combining technique has been suggested as a means of overcoming this problem i.e. the idea behind it being that signals from all the branches will not go through the same amount of fading at any instant of time. The authors in [21] considered

a single-input multiple-output (SIMO) RF hop where all the branches were combined at the relay using the maximal ratio combining (MRC) technique. A similar SIMO RF hop was considered in [22], but here the output at the relay could be obtained by using either MRC or receive antenna selection (RAS) techniques.

Shannon's work on perfect secrecy assumed that both the main and eavesdropper ($\mathcal{E}$) channels were noiseless, and he suggested the use of a secret key between the transmitter and the intended receiver as the way of ensuring perfectly secure communication [23]. However, wireless channels are never truly noiseless i.e. they are inherently random and time-variant, and the existence of a relay and simpler end-users in the mixed RF-FSO network make upper-layer security measures, such as an encrypted key, much harder to implement in practice [24]. Hence, instead of relying on a secret key, Wyner's key-less approach, which focuses on utilizing the physical properties of the medium, seems like a more credible option in order to ensure secure communication in our mixed network [25]–[29]. The secrecy capability of a mixed RF-FSO network was analyzed in terms of average secrecy capacity (ASC), secrecy outage probability (SOP), and strictly positive secrecy capacity (SPSC). In [30], the authors considered a SIMO mixed RF-FSO system, where the signals were combined at the relay by using MRC and RAS techniques. They also proposed a cooperative model where the worst user was selected by the relay in order to jam a multiple antenna eavesdropper. Considering the presence of an eavesdropper to be in the RF hop, closed-form expressions for ASC and SOP were obtained in [31]. The effects of co-channel interference were studied in [32], and the authors also observed how each hop impacts the performance of the system in different turbulent conditions. In [33], the authors analyzed a simultaneous wireless information and power transfer (SWIPT) system and concluded that secrecy diversity order is mostly affected by the fading parameter of the R-D link and the number of antennas at the receiver. The impact of imperfect channel state information (CSI) for a multiple antenna relay and eavesdropper was studied in [34]. The expressions for average secrecy rate (ASR) and SOP were derived in [35] for both fixed gain and variable gain relaying scheme in a mixed system. Herein, like all previously discussed works, an eavesdropper was considered to be in the RF hop since the optical beam directivity makes the FSO hop less prone to wiretapping. The RF link and the FSO link were modeled using Nakagami-m and $\mathcal{M}$ distributions respectively in [36], and the generalized nature of these distribution models meant that several other existing works could be replicated with this system model. For the first time, the eavesdropper was assumed to be in FSO hop in [37] since it is still possible to wiretap the FSO link if the eavesdropper is placed really close to the actual receiver. A SWIPT system was considered in [38], where the signal branches were combined using the MRC scheme.

1.3 Motivation

Based on the aforecited literature, it is obvious that MRC is the most widely utilized diversity reception technique. However, in a mixed RF-FSO network, equal gain combining (EGC) scheme is so much easier to implement since all the signal branches are attributed the same weight. In practical multi-antenna scenarios, a correlation exists between two consecutive antennas that reduces the data rate as well as the information security. Hence, investigation of secrecy performance of a mixed RF-FSO network with antenna correlation is also drawing attention of the researchers. Although many authors considered multi-antenna relay [34] or eavesdropper [30] in their analysis, the impact of correlation on the secrecy analysis of a RF-FSO system has not been considered yet in any existing researches based on the open literature. Hence, in this work, we focus on a RF-FSO network wherein a relay with correlated multiple antennas is utilizing the EGC scheme to receive signal from the source over Nakagami-m fading channel. To establish a secure source (RF)-relay-destination (FSO) link against passive eavesdropping, we consider the location of the eavesdropper at both RF and FSO hops which are modeled utilizing Nakagami-m and $\mathcal{M}$ distributions, respectively. The main contributions of this paper are summarized as follows:

- We first deduce the probability density function (PDF) of signal-to-noise ratio (SNR) for dual-hop correlated Nakagami-m-$\mathcal{M}$ RF-FSO channel and then the corresponding cumulative
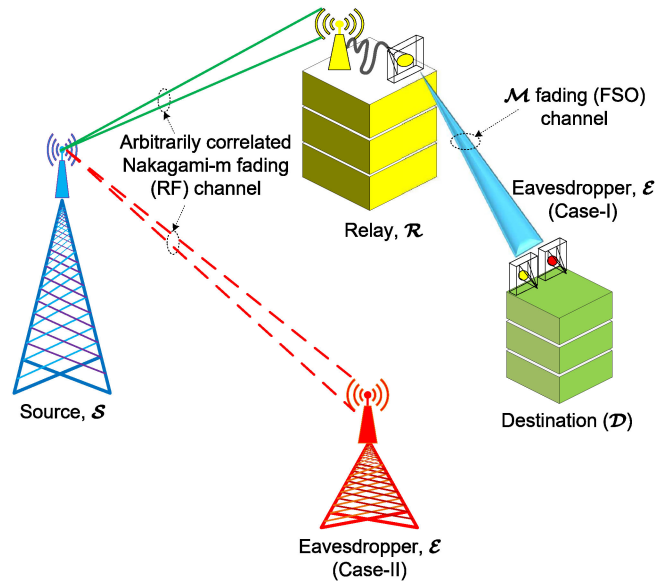
Fig. 1. System model comprises of source ($\mathcal{S}$), relay ($\mathcal{R}$), destination ($\mathcal{D}$), and eavesdropper ($\mathcal{E}$).

distribution function (CDF). We also derive the PDFs of SNR for eavesdropper link depending on the positions of eavesdropper. Our derived PDFs for dual-hop mixed channel is completely novel compared to the existing literature.

- We capitalize on the derived PDFs and CDFs to deduce closed-form expressions of secrecy parameters such as SOP and SPSC assuming two scenarios based on the position of the eavesdropper in either FSO links (scenario I) or RF link (scenario II). As a mixed RF-FSO network with correlated RF link is a new approach, the derived expressions are novel.
- Since $\mathcal{M}$ is a generalized distribution, a wide range of classical FSO models can be obtained as its special cases [39, Table 1]. Besides, unification of system performance over Rician, one-sided Gaussian, Rayleigh etc. fading models can also be performed utilizing Nakagami-m fading channel [40]. Hence, our proposed model exhibits enormous versatility in secrecy performance evaluation of well proportioned RF-FSO mixed system models amid severe correlation, atmospheric turbulence, and pointing error.
- Finally, the justification of the derived mathematical expressions is made making use of Monte-Carlo simulations via MATLAB.

1.4 Paper Orientation

The rest of the paper is arranged in the following manner. The proposed system structure is presented in Section II, and the mathematical models are described in Section III. Closed-form expressions for SOP and SPSC are obtained in Section IV. Simulation results and their analysis are presented in Section V, and finally, the conclusion of the complete work is drawn in Section VI.

2. Proposed Structure of RF-FSO System

We consider a relay aided RF-FSO dual-hop scheme in Fig. 1 to transmit confidential information via a single antenna source ($\mathcal{S}$) to the destination ($\mathcal{D}$) via a relay ($\mathcal{R}$) in presence of a single eavesdropper ($\mathcal{E}$). Here, $\mathcal{R}$ is equipped with multiple receive antennas and a single transmission aperture, and $\mathcal{D}$ has a single receive aperture. The multi-antenna relay is used to meet the high data rate requirements without deploying multiple antennas at the receiver or the transmitter. At the same time, the need for an increased transmit power or additional bandwidth can also be

omitted [41]. Due to insufficient distance between the receive antennas of $\mathcal{R}$, the sub-channels of $\mathcal{S} - \mathcal{R}$ link are arbitrarily correlated and experience Nakagami-m fading where m signifies the Nakagami fading parameter. The $\mathcal{S}$, at first, utilizes this link to transmit information to $\mathcal{R}$ in the first hop. The received RF signal at $\mathcal{R}$ is converted into optical signal by $\mathcal{R}$ that is further transmitted to $\mathcal{D}$ via a FSO link in the second hop. We consider the FSO link experiences $\mathcal{M}$ turbulence with pointing error impairments. Based on the location of the eavesdropper we consider two scenarios.

Scenario I: $\mathcal{E}$ at the FSO Link

In this scenario, we consider the location of $\mathcal{E}$ is close to $\mathcal{D}$ and $\mathcal{E}$ wiretaps information via the FSO link only. Hence, similar to $\mathcal{R} - \mathcal{D}$ link, $\mathcal{R} - \mathcal{E}$ link also experiences $\mathcal{M}$ turbulence. Let us denote the instantaneous SNRs of $\mathcal{S} - \mathcal{R}$, $\mathcal{R} - \mathcal{D}$, and $\mathcal{R} - \mathcal{E}$ links as Ψ_R, Ψ_o, and Ψ_e, respectively. Hence, the secrecy capacity (SC) for $\mathcal{S} - \mathcal{R} - \mathcal{D}$ link is minimum value of the two hops [37], and it is expressed as

$$C_{s_1} = \min(C_{SR_1}, C_{RD_1}), \qquad (1)$$

where $C_{SR_1} = \frac{1}{2}\log_2(1 + \Psi_R)$, $C_{RD_1} = \{\frac{1}{2}(\log_2(1 + \Psi_o) - \log_2(1 + \Psi_e))\}^+$, and $\{x\}^+ = \max\{x, 0\}$.

Scenario II: $\mathcal{E}$ at the RF Link

In this scenario, we assume the FSO link is highly secure. Hence, $\mathcal{E}$ with multiple antennas wiretaps the RF link only. Similar to $\mathcal{S} - \mathcal{R}$ link, the $\mathcal{S} - \mathcal{E}$ link also experiences arbitrary correlated Nakagami-m fading channel. The end-to-end SNR of $\mathcal{S} - \mathcal{R} - \mathcal{D}$ link is shown as [42, Eq. (7)]

$$\Psi_d = \frac{\Psi_o \Psi_R}{\Psi_o + \Psi_R + 1}$$

$$\approx \min\{\Psi_R, \Psi_o\}, \qquad (2)$$

and the SNR of $\mathcal{S} - \mathcal{E}$ link is symbolized by Ψ_E. Hence, the SC is expressed as $C_{s_2} = \{\frac{1}{2}(\log_2(1 + \Psi_d) - \log_2(1 + \Psi_E))\}^+$.

3. Construction of Mathematical Model

3.1 PDF and CDF of SNR for RF Main Channel

We consider multiple antennas with equal gain combiner at the relay. Equal gain combining (EGC) diversity is a popular approach for mitigation of fading as it does not require the knowledge of instantaneous SNR of each diversity branch. In this technique, the signals at each branch are co-phased and then combined utilizing equal weighting. The output SNR of a L-branch EGC combiner is expressed as [43, eq. 7.24]

$$\Psi_R = \frac{1}{P_o L}\left(\sum_{i=1}^{L} r_i\right)^2, \qquad (3)$$

where P_o is the equal noise power spectral density in each branch and r_i symbolizes the amplitude of the fading envelope.

Recently, due to the requirements of high data rate with limited power and bandwidth resources, multi-antenna communication system is gaining much popularity. But in practical scenarios, a correlation between the antennas exists that is responsible for the degradation of diversity gain as-well-as the received SNR. Several correlation models are available in the literature e.g. exponential, arbitrary, circular, linearly arbitrary, constant, Jakes etc. [44]–[49]. The most general one is the arbitrary correlation model since this model includes other models as special cases. For arbitrarily correlated Nakagami-m fading channels with two branch EGC diversity, the PDF of the combiner's output SNR is given as [50, Eq. (36)]

$$f_R(\Psi_R) = \frac{(1 - \rho_R)^{m_R}}{\Gamma(m_R)} \sum_{k_R=0}^{\infty} \frac{B(2\mathcal{A}_R, \frac{1}{2})c_R^{2\mathcal{A}_R}\rho_R^{k_R}}{k_R!\Gamma(\mathcal{A}_R)2^{2(\mathcal{A}_R-1)}} \Psi_R^{2\mathcal{A}_R-1}e^{-2c_R\Psi_R}{}_1F_1\left(2\mathcal{A}_R; 2\mathcal{A}_R + \frac{1}{2}; c_R\Psi_R\right), \qquad (4)$$

where $c_R = \frac{m_R}{\bar{\Psi}_R(1-\rho_R)}$, $\mathcal{A}_R = m_R + k_R$, ρ_R denotes the correlation coefficient, m_R refers to the fading parameter, $\bar{\Psi}_R$ is the average SNR of L-EGC Nakagami-m fading branches, $B(\alpha, \beta) = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$ denotes the beta function, and $_1F_1(\alpha; \beta; x) = \frac{\Gamma(\beta)}{\Gamma(\alpha)} \sum_{n=0}^{\infty} \frac{\Gamma(\alpha+n)x^n}{\Gamma(\beta+n)n!}$ denotes the confluent hyper geometric function as defined in [51, Eq. (15.1.1)]. After algebraic manipulations, the PDF is expressed as

$$f_R(\Psi_R) = \mathcal{H}_R \Psi_R^{v_R-1} e^{-2c_R\Psi_R}, \tag{5}$$

where $\mathcal{H}_R = \frac{(1-\rho_R)^{m_R}}{\Gamma(m_R)} \sum_{k_R=0}^{\infty} \sum_{n_R=0}^{\infty} \frac{\mathcal{B}_R c_R^{v_R} \rho_R^{k_R}}{k_R! n_R! \Gamma(\mathcal{A}_R) 2^{2(\mathcal{A}_R-1)}}$, $\mathcal{B}_R = \frac{\Gamma(v_R)\Gamma(\frac{1}{2})}{\Gamma(v_R+\frac{1}{2})}$, and $v_R = 2\mathcal{A}_R + n_R$. Utilizing [52, Eqs. (3.381.8) and (8.352.6)], the CDF of Ψ_R is expressed as

$$F_R(\Psi_R) = 1 - \mathcal{G}_R e^{-2c_R\Psi_R} \sum_{i=0}^{v_R-1} \frac{(2c_R\Psi_R)^i}{i!}, \tag{6}$$

where $\mathcal{G}_R = \frac{(1-\rho_R)^{m_R}}{\Gamma(m_R)} \sum_{k_R=0}^{\infty} \sum_{n_R=0}^{\infty} \frac{\mathcal{B}_R \rho_R^{k_R}(v_R-1)!}{k_R! n_R! \Gamma(\mathcal{A}_R) 2^{4\mathcal{A}_R+n_R-2}}$.

3.2 PDF and CDF of SNR for FSO Main Channel

The $\mathcal{M}$ turbulence model is basically a physical system that involves a line-of-sight (LOS) contribution, U_L, a component scattered by the eddies on the propagation axis and coupled to the LOS, U_S^C, and an independent component scattered by off-axis eddies, U_S^G. It is also well-known as a generalized model that incorporates some classical turbulence models as its special cases [39, Table 1]. We consider the FSO link undergoes $\mathcal{M}$ turbulence with pointing error impairments. Hence, the PDF of Ψ_o is expressed as [53]

$$f_o(\Psi_o) = \frac{\epsilon_o^2 A_o}{2^r \Psi_o} \sum_{o=1}^{\beta_o} b_o G_{1,3}^{3,0}\left[B_o \left(\frac{\Psi_o}{\mu_r}\right)^{\frac{1}{r}} \Bigg| \begin{matrix} \epsilon_o^2 + 1 \\ \epsilon_o^2, \alpha_o, o \end{matrix} \right], \tag{7}$$

where $A_o = \frac{2\alpha_o^{\frac{\alpha_o}{2}}}{g^{1+\frac{\alpha_o}{2}}\Gamma(\alpha_o)}\left(\frac{g\beta_o}{g\beta_o+\Omega}\right)^{\beta_o+\frac{\alpha_o}{2}}$, $B_o = \frac{\epsilon_o^2 \alpha_o \beta_o(g+\Omega)}{(\epsilon_o^2+1)(g\beta_o+\Omega)}$, $a_o = \binom{\beta_o-1}{o-1}\frac{(g\beta_o+\Omega)^{1-\frac{o}{2}}}{(o-1)!}\left(\frac{\Omega}{g}\right)^{o-1}\left(\frac{\alpha_o}{\beta_o}\right)^{\frac{o}{2}}$, and $b_o = a_o\left(\frac{\alpha_o\beta_o}{g\beta_o+\Omega}\right)^{-\frac{\alpha_o+o}{2}}$. Here, α_o refers to the number of large-scale cells that are scattered during the whole process and β_o represents the fading parameter. The ratio between the equivalent beam radius and the pointing error displacement jitter at the destination is denoted by ϵ_o. μ_r refers to the electrical SNR and the value of r indicates the detection technique being utilized i.e. $r = 1$ implies heterodyne detection where $\mu_1 = \mathbb{E}(\Psi_o) = \bar{\Psi}_o$ and $r = 2$ implies intensity modulation/direct detection (IM/DD) technique is being utilized where $\mu_2 = \frac{\alpha_o \epsilon_o^2 (\epsilon_o^2+1)^{-2}(\epsilon_o^2+2)(g+\Omega)}{(\alpha_o+1)[2g(g+2\Omega)+\Omega^2(1+1/\beta_o)]}\bar{\Psi}_o$. Here, $\bar{\Psi}_o$ represents the average SNR of the FSO link. In order to make the calculations simpler, it is assumed that $g = 2b_o(1 - \rho_o)$. The average power of coherent contributions is represented as $\Omega' = \Omega + 2b_o\rho_o + 2\sqrt{2b_o\rho_o\Omega}cos(\phi_A - \phi_B)$, where ϕ_A and ϕ_B are the deterministic phases of the LOS, ρ_o represents the amount of coupled scattering power to the LOS component ($0 \leq \rho_o \leq 1$), and G[.] refers to the the Meijer's G-function as defined in [52]. The CDF of Ψ_o is expressed as [53, Eq. (11)]

$$F_o(\Psi_o) = D_o \sum_{o=1}^{\beta_o} c_m G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_o}{\mu_r}\Psi_o \Bigg| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix} \right], \tag{8}$$

where $D_o = \frac{\epsilon_o^2 A_o}{2^r(2\pi)^{r-1}}$, $c_m = b_o r^{\alpha_o+o-1}$, $\chi_o = \frac{B_o^r}{r^{2r}}$, $s_1 = \triangle(r, \epsilon_o^2 + 1)$ that incorporates r number of terms, $s_2 = \triangle(r, \epsilon_o^2), \triangle(r, \alpha_o), \triangle(r, o)$ that incorporates $3r$ number of terms, and $\triangle(x, a) = \frac{a}{x}, \frac{a+1}{x}, ..., \frac{a+x-1}{x}$.

3.3 PDF and CDF of SNR for the Eavesdropper Channel

3.3.1 Scenario I: The PDF of Ψ_e is defined similar to (7) as

$$f_e(\Psi_e) = \frac{\epsilon_e^2 A_e}{2^r \Psi_e} \sum_{k=1}^{\beta_e} b_k G_{1,3}^{3,0}\left[B_e \left(\frac{\Psi_e}{\mu_{r_e}}\right)^{\frac{1}{r}} \Bigg| \begin{array}{c} \epsilon_e^2 + 1 \\ \epsilon_e^2, \alpha_e, k \end{array} \right],$$ (9)

where $A_e = \frac{2\alpha_e^{\frac{\alpha_e}{2}}}{g^{1+\frac{\alpha_e}{2}}\Gamma(\alpha_e)}(\frac{g\beta_e}{g\beta_e + \Omega})^{\beta_e + \frac{\alpha_e}{2}}$, $B_e = \frac{\epsilon_e^2 \alpha_e \beta_e(g+\Omega)}{(\epsilon_e^2+1)(g\beta_e+\Omega)}$, $a_k = \binom{\beta_e-1}{k-1}\frac{(g\beta_e+\Omega)^{1-\frac{k}{2}}}{(k-1)!}(\frac{\Omega}{g})^{k-1}(\frac{\alpha_e}{\beta_e})^{\frac{k}{2}}$, and $b_k = a_k(\frac{\alpha_e\beta_e}{g\beta_e+\Omega})^{-\frac{\alpha_e+k}{2}}$. Here, α_e refers to the number of large-scale cells that are scattered during the whole process and β_e represents the fading parameter. The ratio between the equivalent beam radius and the pointing error displacement jitter at the destination is denoted by ϵ_e. μ_{r_e} refers to the electrical SNR where $\mu_{1_e} = \mathbb{E}(\Psi_e) = \bar{\Psi}_e$ and $\mu_{2_e} = \frac{\alpha_e\epsilon_e^2(\epsilon_e^2+1)^{-2}(\epsilon_e^2+2)(g+\Omega)}{(\alpha_e+1)[2g(g+2\Omega)+\Omega^2(1+1/\beta_e)]}\bar{\Psi}_e$. Here, $\bar{\Psi}_e$ represents the average SNR of the FSO link. The CDF of Ψ_e is expressed similar to (8) as

$$F_e(\Psi_e) = D_e \sum_{k=1}^{\beta_e} c_k G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_e}{\mu_{r_e}}\Psi_e \Bigg| \begin{array}{c} 1, s_3 \\ s_4, 0 \end{array} \right],$$ (10)

where $D_e = \frac{\epsilon_e^2 A_e}{2^r(2\pi)^{r-1}}$, $c_k = b_k r^{\alpha_e+k-1}$, $\chi_e = \frac{B_e^r}{r^{2r}}$, $s_3 = \triangle(r, \epsilon_e^2 + 1)$ that incorporates r number of terms, and $s_4 = \triangle(r, \epsilon_e^2), \triangle(r, \alpha_e), \triangle(r, k)$ that incorporates $3r$ number of terms.

3.3.2 Scenario II: Considering eavesdropper at the RF link, the PDF of Ψ_E can be expressed as (5)

$$f_E(\Psi_E) = \mathcal{H}_E \Psi_E^{v_E-1} e^{-2c_E\Psi_E},$$ (11)

where $c_E = \frac{m_E}{\bar{\Psi}_E(1-\rho_E)}$, $\mathcal{H}_E = \frac{(1-\rho_E)^{m_E}}{\Gamma(m_E)}\sum_{k_E=0}^{\infty}\sum_{n_E=0}^{\infty}\frac{\mathcal{B}_E c_E^{v_E}\rho_E^{k_E}}{k_E! n_E! \Gamma(\mathcal{A}_E)2^{2(\mathcal{A}_E-1)}}$, $\mathcal{A}_E = m_E + k_E$, $\mathcal{B}_E = \frac{\Gamma(v_E)\Gamma(\frac{1}{2})}{\Gamma(v_E+\frac{1}{2})}$, and $v_E = 2\mathcal{A}_E + n_E$. ρ_E is the correlation coefficient, m_E refers to the fading parameter, and $\bar{\Psi}_E$ denotes the average SNR of the eavesdropper channel. The CDF of the eavesdropper channel can be expressed similar to (6) as

$$F_E(\Psi_E) = 1 - \mathcal{G}_E e^{-2c_E\Psi_E}\sum_{j=0}^{v_E-1}\frac{(2c_E\Psi_E)^j}{j!},$$ (12)

where $\mathcal{G}_E = \frac{(1-\rho_E)^{m_E}}{\Gamma(m_E)}\sum_{k_E=0}^{\infty}\sum_{n_E=0}^{\infty}\frac{\mathcal{B}_E \rho_E^{k_E}(v_E-1)!}{k_E! n_E! \Gamma(\mathcal{A}_E)2^{4\mathcal{A}_E+n_E-2}}$.

3.4 PDF and CDF of SNR for Dual-Hop

The CDF of dual-hop SNR, Ψ_d is expressed as [54, Eq. (15)]

$$F_d(\Psi_d) = P_r\{\min\{\Psi_R, \Psi_o\} < \Psi_d\}$$
$$= F_R(\Psi_d) + F_o(\Psi_d) - F_R(\Psi_d)F_o(\Psi_d).$$ (13)

Substituting (6) and (8) into (13), we obtain

$$F_d(\Psi_d) = 1 - \mathcal{G}_R e^{-2c_R\Psi_d}\sum_{i=0}^{v_R-1}\frac{(2c_R\Psi_d)^i}{i!}\left(1 - D_o\sum_{o=1}^{\beta_o}c_m G_{r+1,3r+1}^{3r,1}\left[\frac{\chi_o}{\mu_r}\Psi_d \Bigg| \begin{array}{c} 1, s_1 \\ s_2, 0 \end{array}\right]\right).$$ (14)

The PDF of Ψ_d can be expressed as [55, Eq. (12)]

$$f_d(\Psi_d) = \frac{d}{d\Psi_d}[F_d(\Psi_d)]$$
$$= f_R(\Psi_d) + f_o(\Psi_d) - f_R(\Psi_d)F_o(\Psi_d) - f_o(\Psi_d)F_R(\Psi_d).$$ (15)

By substituting (5), (6), (7), and (8) into (15), utilizing [56, Eq. (2.24.2.3)], and performing some algebraic manipulations, the PDF of Ψ_d is expressed as

$$f_d(\Psi_d) = \mathcal{H}_R \Psi_R^{\upsilon_R - 1} e^{-2c_R \Psi_R} D_o \sum_{o=1}^{\beta_o} c_m G_{r+1,3r+1}^{3r+1,0} \left[\frac{\chi_o}{\mu_r} \Psi_d \, \middle| \, \begin{matrix} s_1, 1 \\ 0, s_2 \end{matrix} \right]$$

$$+ \, \mathcal{G}_R e^{-2c_R \Psi_R} \sum_{i=0}^{\upsilon_R - 1} \frac{(2c_R \Psi_R)^i}{i!} \frac{\epsilon_o^2 A_o}{2^r \Psi_o} \sum_{o=1}^{\beta_o} b_o G_{1,3}^{3,0} \left[B_o \left(\frac{\Psi_o}{\mu_r} \right)^{\frac{1}{r}} \middle| \begin{matrix} \epsilon_o^2 + 1 \\ \epsilon_o^2, \alpha_o, 0 \end{matrix} \right]. \tag{16}$$

4. Performance Analysis

4.1 Scenario I

4.1.1 Lower-Bound SOP Analysis: The SOP is illustrated as the probability that instantaneous secrecy capacity (SC), C_{s_1}, falls below a target capacity, $\mathcal{R}_{sc}$, which is defined for scenario I as [57, Eq. (24)]

$$P_{SOP_1} = Pr\{C_{s_1} < \mathcal{R}_{sc}\}$$

$$= 1 - \left(1 - \int_0^\infty F_o(\Theta \Psi_e + \Theta - 1) f_e(\Psi_e) d\Psi_e \right) (1 - F_R(\Theta - 1))$$

$$= (1 - F_R(\Theta - 1)) \int_0^\infty F_o(\Theta \Psi_e + \Theta - 1) f_e(\Psi_e) d\Psi_e + F_R(\Theta - 1), \tag{17}$$

where $\Theta = 2^{\mathcal{R}_{sc}}$. The closed-form expression for exact SOP is mathematically difficult to calculate. Hence, we calculate the lower bound of SOP that can be expressed as

$$P_{SOP_1} \geq P_{SOP_{L_1}} = (1 - F_R(\Theta - 1)) \int_0^\infty F_o(\Theta \Psi_e) f_e(\Psi_e) d\Psi_e + F_R(\Theta - 1). \tag{18}$$

Substituting (6), (8), and (9) into (18) and performing integration via utilizing [56, Eq. (2.24.1.1)], the lower bound of the SOP is expressed as

$$P_{SOP_{L_1}} = 1 - \mathcal{G}_R e^{-2c_R(\Theta - 1)} \sum_{i=0}^{\upsilon_R - 1} \frac{(2c_R(\Theta - 1))^i}{i!}$$

$$\times \left(1 - D_o D_e \sum_{o=1}^{\beta_o} \sum_{k=1}^{\beta_e} c_m c_k G_{4r+1,4r+1}^{3r+1,3r} \left[\frac{\mu_o}{\Theta \mu_e} \middle| \begin{matrix} 1 - s_2, 1, s_3 \\ s_4, 0, 1 - s_1 \end{matrix} \right] \right). \tag{19}$$

4.1.2 Asymptotic SOP Analysis: Expanding Meijer's G function in (19) via utilizing [53, Eq. (41)], the final asymptotic expression of SOP is obtained as

$$P_{SOP_{La1}} = 1 - \mathcal{G}_R e^{-2c_R(\Theta - 1)} \sum_{i=0}^{\upsilon_R - 1} \frac{(2c_R(\Theta - 1))^i}{i!} \left[1 - D_o D_e \sum_{o=1}^{\beta_o} \sum_{k=1}^{\beta_e} c_m c_k \right.$$

$$\left. \times \sum_{p=1}^{3r} \frac{\prod_{l=1,l \neq p}^{3r} \Gamma(S_{1,p} - S_{1,l})}{\prod_{l=3r+1}^{4r+1} \Gamma(1 + S_{1,l} - S_{1,p})} \frac{\prod_{l=1}^{3r+1} \Gamma(1 + S_{2,l} - S_{1,p})}{\prod_{l=3r+2}^{4r+1} \Gamma(S_{1,p} - S_{2,l})} \left(\frac{\mu_o}{\Theta \mu_e} \right)^{S_{1,p}-1} \right], \tag{20}$$

where $S_1 = (1 - s_2, 1, s_3)$ and $S_2 = (s_4, 0, 1 - s_1)$.

4.2 Scenario II

4.2.1 Lower-Bound SOP Analysis: The SOP of mixed RF-FSO channel assuming eavesdropper at $\mathcal{S} - \mathcal{R}$ link can be expressed as [42, Eq. (10)]

$$P_{SOP_2}(\mathcal{R}_{sc}) = Pr\{C_s(\Psi_d, \Psi_E) \leq \mathcal{R}_{sc}\}$$

$$= Pr\{\Psi_d \leq \varphi(\Psi_E + 1) - 1\}$$

$$= \int_0^\infty F_d(\varphi\Psi_E + \varphi - 1)f_E(\Psi_E)d\Psi_E, \tag{21}$$

where $\varphi = 2^{\mathcal{R}_{sc}}$ and $\mathcal{R}_{sc} > 0$. The lower bound of the SOP can be derived as [58, Eq. (7)]

$$P_{SOP_2}(\mathcal{R}_{sc}) = Pr\{\Psi_d \leq \varphi\Psi_E + \varphi - 1\}$$

$$\geq P_{SOP_{L_2}}(\mathcal{R}_{sc}) = Pr\{\Psi_d \leq \varphi\Psi_E\} = \int_0^\infty F_d(\varphi\Psi)f_E(\Psi)d\Psi. \tag{22}$$

Substituting (11) and (14) into (22), the lower bound of SOP can be denoted as

$$P_{SOP_{L_2}}(\mathcal{R}_{sc}) = 1 - \mathcal{G}_R\mathcal{H}_E \sum_{i=0}^{v_R-1} \frac{(2c_R\varphi)^i}{i!} \int_0^\infty \Psi^{\varkappa_1} e^{-\varkappa_2\Psi_E}$$

$$\times \left(1 - D_o \sum_{o=1}^{\beta_o} c_m G_{r+1,3r+1}^{3r,1}\left[\frac{\varphi\chi_o}{\mu_r}\Psi \middle| \begin{matrix} 1, s_1 \\ s_2, 0 \end{matrix}\right]\right) d\Psi, \tag{23}$$

where $\varkappa_1 = v_E + i - 1$ and $\varkappa_2 = 2(c_R\varphi + c_E)$. Utilizing [56, Eqs. (8.4.3.1) & (2.24.1.1)], finally, the lower bound of SOP is expressed as

$$P_{SOP_{L_2}}(\mathcal{R}_{sc}) = 1 - \mathcal{G}_R\mathcal{H}_E \sum_{i=0}^{v_R-1} \frac{(2c_R\varphi)^i}{i!}\left(\Im_1 - D_o \sum_{o=1}^{\beta_o} c_m\Im_2\right), \tag{24}$$

where $\Im_1 = \frac{\varkappa_1!}{\varkappa_2^{\varkappa_1}}$ and $\Im_2 = \varkappa_2^{-\varkappa_1} G_{r+2,3r+1}^{3r,2}[\frac{\varphi\chi}{\varkappa_2\mu_r}| \begin{matrix} 1, 1 - v_E - i, s_1 \\ s_2, 0 \end{matrix}]$.

4.2.2 Asymptotic SOP Analysis: At higher SNR, asymptotic analysis can be expressed by inverting the Meijer's G function in (24) via utilizing [59, Eq. (6.2.2)]. Utilizing [53, Eq. (41)], the lower bound of the SOP (asymptotic) is expressed in a simpler form as

$$P_{SOP_{L_{a2}}}(\mathcal{R}_{sc}) = 1 - \mathcal{G}_R\mathcal{H}_E \sum_{i=0}^{v_R-1} \frac{(2c_R\varphi)^i}{i!}\left(\Im_1 - D_o \sum_{o=1}^{\beta_o} c_m\varkappa_2^{-\varkappa_1}\right.$$

$$\left.\times \sum_{p=1}^{3r} \frac{\Gamma(s_{2,p})\prod_{l=1,l\neq p}^{3r}\Gamma(s_{2,l} - s_{2,p})}{\prod_{l=3}^{r+2}\Gamma(s_{1,l} - s_{2,p})}\left(\frac{\varkappa_2\mu_r}{\varphi\chi}\right)^{-s_{2,p}}\right). \tag{25}$$

Note that correlated Nakagami-*m* distribution comprises of few classical channels that can be achieved by altering the value of the fading parameter. Setting $m = 0.5$, Nakagami-*m* channel converges to a one-sided Gaussian distribution. For $m = 1$, the channel takes the form of Rayleigh distribution. A non-fading additive white Gaussian noise (AWGN) channel can be found by setting $m \to \infty$ [40]. $\mathcal{M}$ channel also shows generality. Setting $\rho = 1$, $g_p = 0$, and $\Omega' = 1$, $\mathcal{M}$ channel converges to $\Gamma\Gamma$ channel. It shows lognormal characteristics by setting $\rho = 0$ and $g_p \to 0$. Also, a Rice-Nakagami channel can be obtained by setting $\rho = 0$ [24]. Our derived expression in (19) can be reduced to the expression of [37, Eqs. (19)], which signifies a Rayleigh-$\Gamma\Gamma$ scenario as a special case of our work. Also, the expression presented in (24) can be converted to the expressions of [31, Eqs. (13)] which is a Nakagami-*m*-$\Gamma\Gamma$ scenario. In addition, the SOP expressions in (19), (20), (24), and (25) are novel too as those are not reported in any existing work in the open literature.

4.3 SPSC Analysis

4.3.1 Scenario I: In order to ascertain the secrecy of the transmitted information, the secrecy capacity must be a positive quantity. Otherwise a secrecy performance of the system will be endangered. Mathematically, SPSC can be defined as [60]

$$P_{SPSC_1} = Pr\{\min(C_{SR_1}, C_{RD_1}) > 0\}$$

$$= \Pr\{C_{SR_1} > 0\} \Pr\{C_{RD_1} > 0\}$$

$$= \Pr\{\Psi_R > 0\} \Pr\{\Psi_o > \Psi_e\}$$

$$= 1 - \int_0^\infty F_o(\Psi_e) f_e(\Psi_e) d\Psi_e \quad [\text{As } \Pr\{\Psi_R > 0\} = 1]. \tag{26}$$

Now, substituting (8) and (9) into (26), the probability of SPSC can be expressed as

$$P_{SPSC_1} = 1 - D_o D_e \sum_{o=1}^{\beta_o} \sum_{k=1}^{\beta_e} c_m c_k G_{4r+1,4r+1}^{3r+1,3r} \left[\frac{\mu_o}{\mu_e} \left| \begin{array}{l} 1 - s_2, 1, s_3 \\ s_4, 0, 1 - s_1 \end{array} \right. \right]. \tag{27}$$

4.3.2 Scenario II: Assuming eavesdropper at the RF link, the SPSC can be expressed as [61]

$$SPSC = \int_0^\infty \int_0^{\Psi_d} f_d(\Psi_d) f_E(\Psi_E) d\Psi_E d\Psi_d$$

$$= \int_0^\infty F_E(\Psi_d) f_d(\Psi_d) d\Psi_d. \tag{28}$$

By substituting (12) and (16) into (28) and utilizing [56, Eqs. (2.24.1.1), (2.24.2.3), & (8.4.3.1)], the SPSC can expressed as

$$SPSC = D_o \sum_{o=1}^{\beta_o} c_m \left[\mathcal{H}_R \left(\Re_1 - \mathcal{G}_E \sum_{j=0}^{v_E - 1} \frac{2^j \Re_3}{j! c_E^{-j}} \right) + \mathcal{G}_R \sum_{i=0}^{v_R - 1} \frac{c_R^i}{2^{-i} i!} \left(\Re_2 - \mathcal{G}_E \sum_{j=0}^{v_E - 1} \frac{2^j \Re_4}{j! c_E^{-j}} \right) \right], \tag{29}$$

where $\Re_1 = \frac{1}{(2c_R)^{v_R}} G_{r+2,3r+1}^{3r+1,1} \left[\frac{\chi_o}{2c_R \mu_r} \left| \begin{array}{l} 1 - v_R, s_1, 1 \\ 0, s_2 \end{array} \right. \right]$, $\Re_2 = \frac{1}{(2c_R)^i} G_{r+1,3r}^{3r,1} \left[\frac{\chi_o}{2c_R \mu_r} \left| \begin{array}{l} 1 - i, s_1 \\ s_2 \end{array} \right. \right]$, $\Re_3 = $

$\frac{1}{\varkappa_3^{v_R + j}} G_{r+2,3r+1}^{3r+1,1} \left[\frac{\chi_o}{\varkappa_3 \mu_r} \left| \begin{array}{l} 1 - v_R - j, s_1, 1 \\ 0, s_2 \end{array} \right. \right]$, $\Re_4 = \frac{1}{\varkappa_3^z} G_{r+1,3r}^{3r,1} \left[\frac{\chi_o}{\varkappa_3 \mu_r} \left| \begin{array}{l} 1 - z, s_1 \\ s_2 \end{array} \right. \right]$, $\varkappa_3 = 2(c_R + c_E)$, and $z = i + j$.

Similar to the SOP expressions, the derived results in (27) and (29) represent SPSC expressions for a Rayleigh-$\Gamma\Gamma$ [37, Eqs. (23)] by setting $m = 1$, $\rho = 1$, $g_p = 0$, and $\Omega' = 1$, and Generalized Gamma-$\mathcal{M}$ [24, Eqs. (30)] scenarios as special cases by setting $m = 1$ or ∞. This indicates that our expressions are generalized enough to provide sufficient novelty compared to the existing works.

5. Numerical Results

In this section, we present the analytical results along with figures and their explanations regarding derived expressions for SOP and SPSC. The impact of antenna correlation along with fading, atmospheric turbulence, and pointing errors on the secrecy performance have been taken into consideration. We also present Monte-Carlo simulations via MATLAB in order to validate our derived analytical expressions. For simplification of our analytical work, we assume $\epsilon_o = \epsilon_e = \epsilon_o$, $\alpha_o = \alpha_e = \alpha$, and $\beta_o = \beta_e = \beta$. We also assume several values of the RF and FSO parameters to obtain the graphs, which are illustrated in Table I.

Figs. 2(a) and 2(b) represent SOP versus $\bar{\Psi}_o$ for two scenarios of the proposed model. Basically, the impact due to the variation in detection techniques ($r = 1$ and $r = 2$) is presented over different turbulent conditions (i.e. strong ($\alpha = 2.296$ and $\beta = 2$), moderate ($\alpha = 4.2$ and $\beta = 3$), and weak ($\alpha = 8.1$ and $\beta = 4$) etc. turbulence conditions). It is clearly demonstrated from Figs. 2(a) and 2(b) that relative to IM/DD technique ($r = 2$), the secrecy performance tends to be better for HD technique ($r = 1$). This is expected since the lower cost and reduced complexity of IM/DD technique permits a limited number of modulation schemes, and this, in turn, restricts its performance. Again, an improved SNR at the destination is obtained with HD technique rather than IM/DD technique and such similar results are also exhibited in [34]. It is also noted that, at higher SNR values, the asymptotic SOP in Fig. 2(a) perfectly matches with lower bound SOP that ensures its tightness.

TABLE I

An Illustration of the Considered Values for All RF and FSO Parameters

Parameters	Values
$\alpha_o = \alpha_e = \alpha$	$2.296, 4.2, 8.1$
$\beta_o = \beta_e = \beta$	$2, 3, 4$
r	$1, 2$
$\epsilon_o = \epsilon_e$	$1.1, 6.7$
$\rho_R = \rho_E$	$0.001, 0.1, 0.2, 0.4$
m_R	$1, 2, 3, 4$
ρ_o	0.596
b_o	0.1074
Ω	1

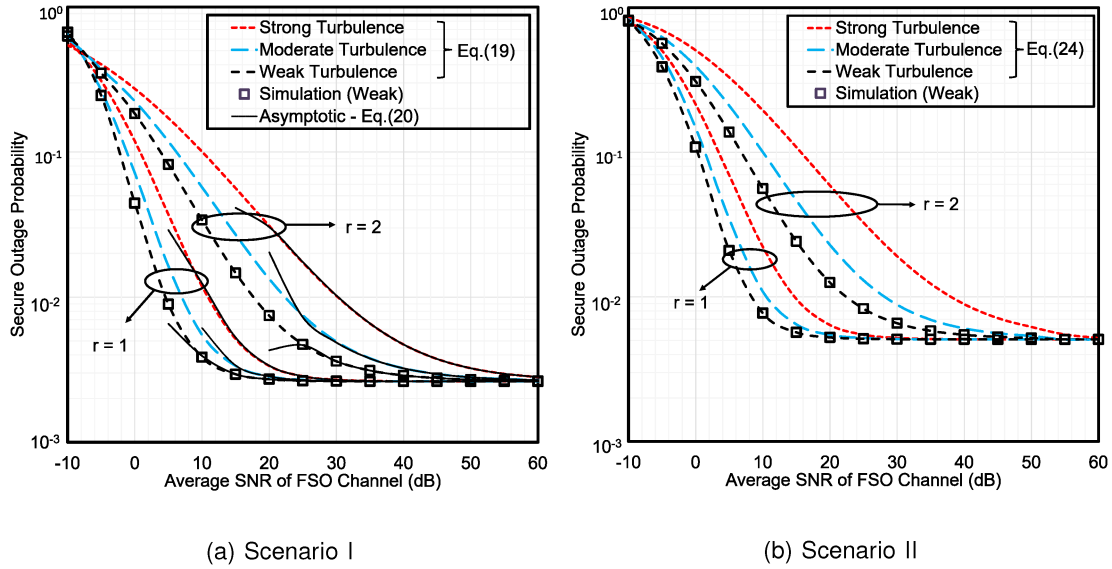
(a) Scenario I
(b) Scenario II

Fig. 2. SOP versus $\bar{\Psi}_o$ with $\epsilon = 6.7$, $\rho_R = \rho_E = 0.001$, $m_R = m_E = 1$, $\mathcal{R}_{sc} = 0.25$ bits/s/Hz, and $\bar{\Psi}_R = 15$ dB. For (a), $\bar{\Psi}_e = -10$ dB and for (b), $\bar{\Psi}_E = -10$ dB.

Similarly, for a set of curves in each figure, analytical and simulation results are compared and one can clearly observe that these strictly agree with each other which validates the derived expressions in (19), (20), (24), and (25).

Figures 3(a), 3(b), 4(a), and 4(b) illustrate how the pointing error variation ($\epsilon = 1.1$ and $\epsilon = 6.7$) exerts influence on the SOP performance. To accomplish this task, SOP is demonstrated against $\bar{\Psi}_o$ in Figs. 3(a) and 3(b), and against $\bar{\Psi}_R$ in Figs. 4(a) and 4(b). In all the figures, it is clearly observed that for a selected turbulent conditions, better secrecy performance (i.e. lower SOP) is obtained when the pointing error is negligible ($\epsilon = 6.7$). Similarly, for a strong pointing error $\epsilon = 1.1$, the secrecy diversity order is greatly affected relative to the negligible pointing error as testified in [31]. Besides pointing error, dominance of several level of turbulences is also presented in the same figure. Since the SNR at the destination is highly deteriorated with increased level of turbulence, the SOP is lowest for weak turbulence relative to moderate and strong turbulences that also agrees well with [24], [30].

Figures 5(a) and 5(b) represent SOP versus $\bar{\Psi}_R$ to analyze the effects of fading parameter of $\mathcal{S} - \mathcal{R}$ link and average SNR of $\mathcal{S} - \mathcal{E}$ link. It can be observed that for selected values of $\bar{\Psi}_e$ and $\bar{\Psi}_E$, the SOP decreases with m_R notably. This result is obtained as increase in m_R reduces the fading of $\mathcal{S} - \mathcal{R}$ link. It is also noted that impact of m_R is more significant in scenario I rather than scenario II. For selected values of m_R, the SOP increases with $\bar{\Psi}_e$ and $\bar{\Psi}_E$. Since an increase in $\bar{\Psi}_e$ and $\bar{\Psi}_E$
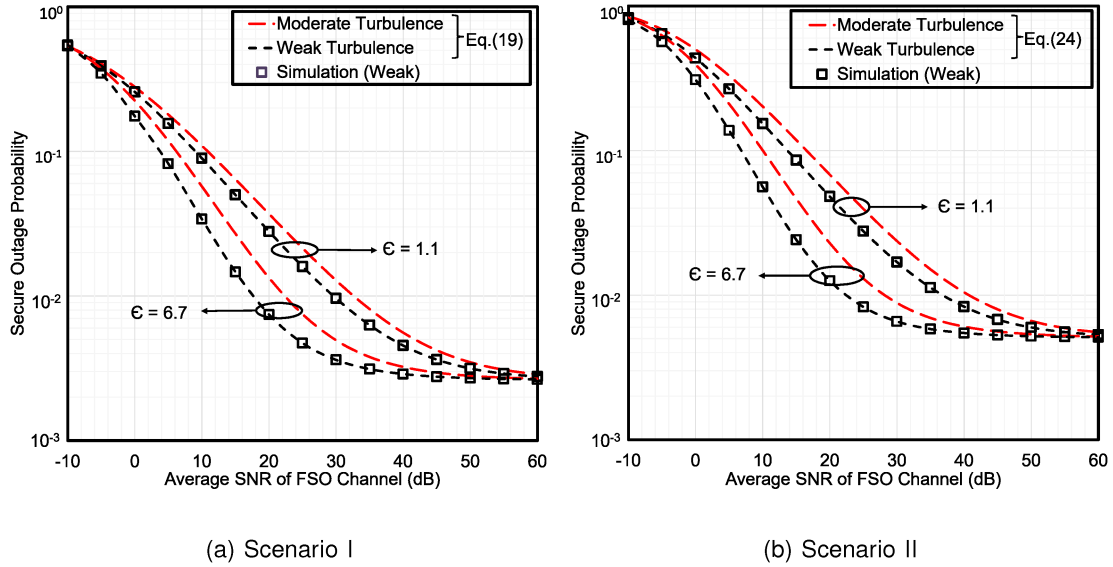
(a) Scenario I   (b) Scenario II

Fig. 3. SOP versus $\bar{\Psi}_o$ with $r = 2$, $\rho_R = \rho_E = 0.001$, $m_R = m_E = 1$, $\mathcal{R}_{sc} = 0.25$ bits/s/Hz, and $\bar{\Psi}_R = 15$ dB. For (a), $\bar{\Psi}_e = -10$ dB and for (b), $\bar{\Psi}_E = -10$ dB.

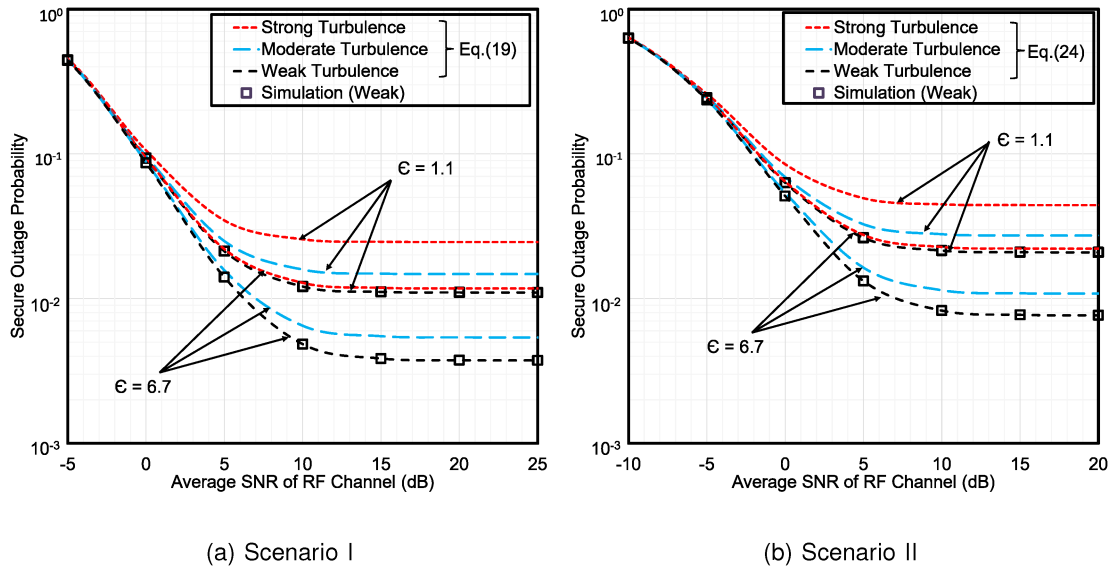(a) Scenario I   (b) Scenario II

Fig. 4. SOP versus $\bar{\Psi}_R$ with $r = 1$, $\rho_R = \rho_E = 0.001$, $m_R = m_E = 1$, $\mathcal{R}_{sc} = 0.25$ bits/s/Hz, and $\bar{\Psi}_o = 10$ dB. For (a), $\bar{\Psi}_e = -10$ dB and for (b), $\bar{\Psi}_E = -10$ dB.

enhances the quality of eavesdropper channel, the SOP performance deteriorates. In addition, for similar settings of system parameters, another significant information can be deduced from all the aforementioned figures i.e. SOP is lesser effected when the eavesdropping occurs via the FSO link (Scenario 1) instead of the RF link (Scenario II). This is because the FSO link is highly secure and the RF link is relatively more prone to external attacks.

Figures 6(a) and 6(b) illustrate how the antenna correlation affects the secrecy outage performance of the mixed RF-FSO system. It can be indisputably observed that the correlation at the $\mathcal{S} - \mathcal{R}$ (Scenarios I & II) link deteriorates the secrecy performance remarkably. This occurs as

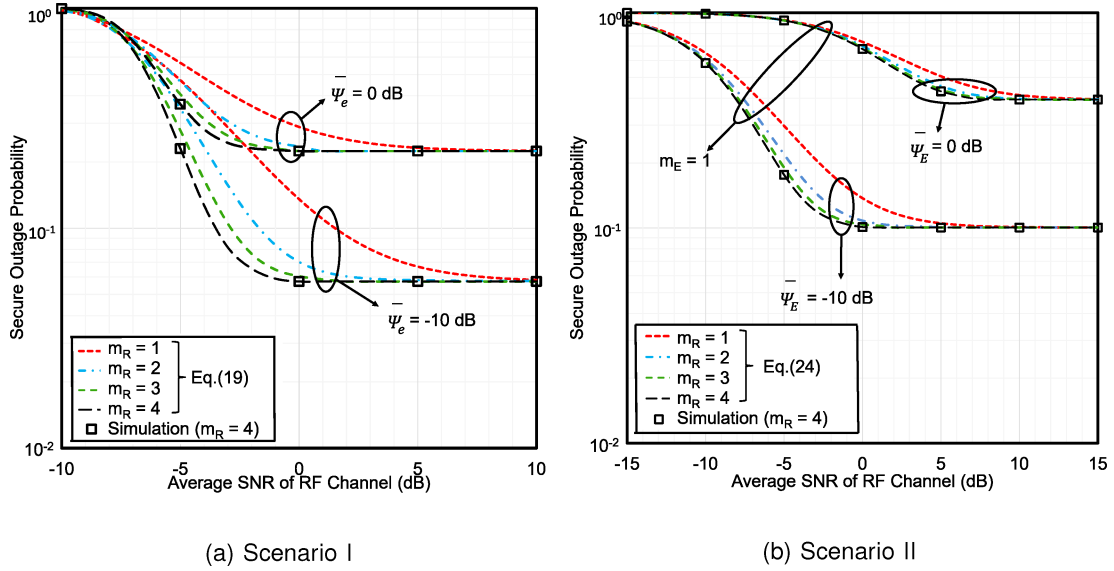(a) Scenario I   (b) Scenario II

Fig. 5. SOP versus $\bar{\Psi}_R$ with $r = 2$, $\rho_R = \rho_E = 0.001$, $\alpha = 4.2$, $\beta = 3$, $\epsilon = 6.7$, and $\bar{\Psi}_o = 10$ dB. For (a), $\bar{\Psi}_e = -10$ and 0 dB and for (b), $\bar{\Psi}_E = -10$ and 0 dB.

(a) Scenario I   (b) Scenario II
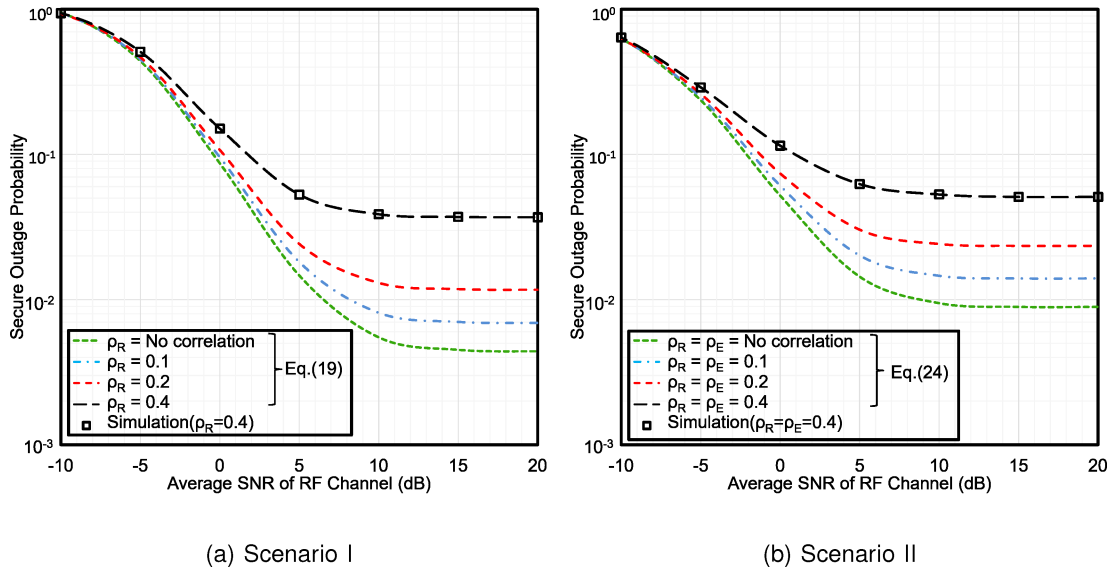
Fig. 6. SOP versus $\bar{\Psi}_R$ with $r = 1$, $m_R = m_E = 1$, $\alpha = 4.2$, $\beta = 3$, $\epsilon = 6.7$, and $\bar{\Psi}_o = 10$ dB. For (a), $\bar{\Psi}_e = -10$ dB and for (b), $\bar{\Psi}_E = -10$ dB.

correlation reduces the SNR at the relay. Similar to the $\mathcal{S} - \mathcal{R}$ link, the correlation must degrade the $\mathcal{S} - \mathcal{E}$ link (Scenario II) and hence an improved secrecy performance must be achieved. But Fig. 6(b) illustrates that impact of correlation at the $\mathcal{S} - \mathcal{R}$ link is more significant than the correlation at the $\mathcal{S} - \mathcal{E}$ link. Similar to Figs. 1−5, a better performance is obtained for Scenario I rather than Scenario II due to the weaker proneness of the FSO links against passive eavesdropping relative to the RF link.
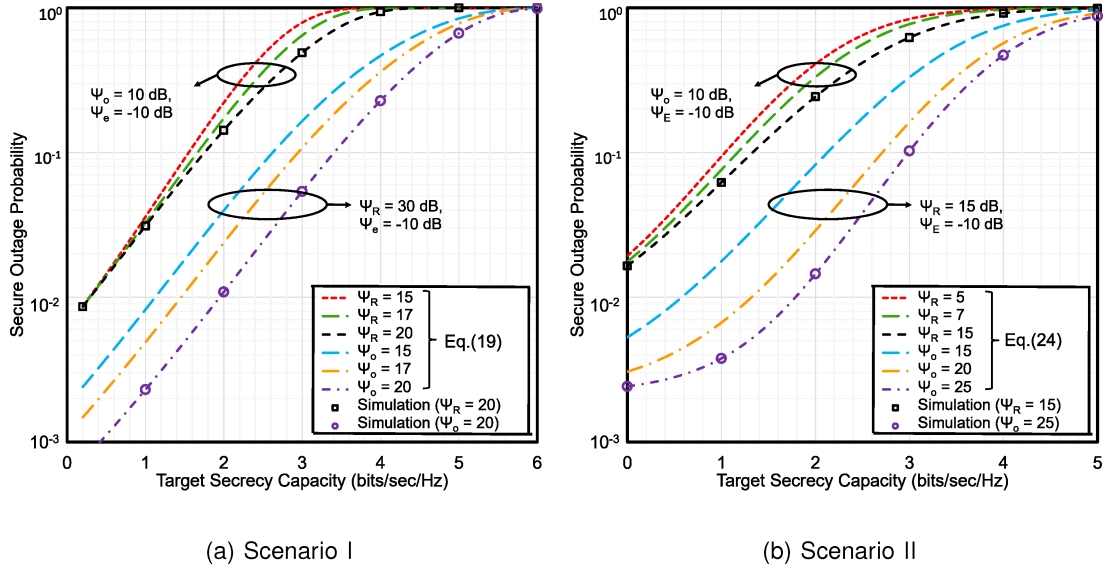
(a) Scenario I   (b) Scenario II

Fig. 7. SOP versus $\mathcal{R}_{sc}$ with $r = 1$, $\alpha = 2.296$, $\beta = 2$, $\epsilon = 6.7$, $m_R = m_E = 1$, and $\rho_R = \rho_E = 0.001$

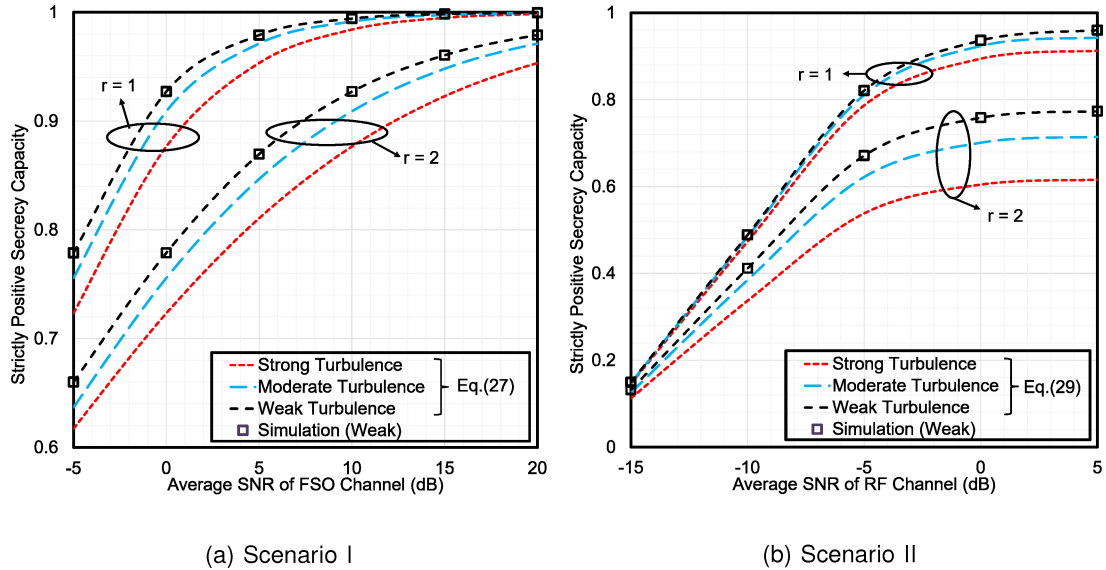(a) Scenario I   (b) Scenario II

Fig. 8. (a) SPSC versus $\bar{\Psi}_o$ with $\epsilon = 1.1$, $\bar{\Psi}_e = -10$ dB, (b) SPSC versus $\bar{\Psi}_R$ with $\epsilon = 1.1$, $\rho_R = \rho_E = 0.001$, $m_R = m_E = 1$, $\bar{\Psi}_o = 5$ dB, and $\bar{\Psi}_E = -10$ dB.

Figures 7(a) and 7(b) depict the impact of Ψ_R, Ψ_E, and Ψ_e on the SOP that are obtained by plotting SOP against target secrecy rate. It is observed that SOP increases successively with $\mathcal{R}_{sc}$. With increase in $\mathcal{R}_{sc}$, the probability of C_s being less than the $\mathcal{R}_{sc}$ is increased and hence the SOP performance degrades. On the other hand, an increase in Ψ_R, Ψ_E, and Ψ_e makes the $\mathcal{S} - \mathcal{R}$, $\mathcal{S} - \mathcal{E}$, and $\mathcal{R} - \mathcal{D}$ links better, respectively, the SOP increases with Ψ_E (Scenario II) and Ψ_e (Scenario I), and decreases with Ψ_R (Scenario I & II).

In Figs. 8(a) and 8(b), the impact of detection techniques is demonstrated on SPSC by demonstrating SPSC vs $\bar{\Psi}_o$ (Scenario I) and vs $\bar{\Psi}_R$ (Scenario II). A matching result with SOP is obtained i.e. in both scenarios the HD technique demonstrates an enhanced secrecy capacity relative to the IM/DD technique. Additionally, utilizing this important performance metric we demonstrate similar results as SOP i.e. the security of the mixed system deteriorates with growing turbulence level. Our obtained results are also supported by [24], [37], [62].

6. Conclusion

In this work, the secrecy performance of a mixed RF-FSO relaying system is analyzed, wherein we considered the eavesdropper can utilize either RF or FSO links for wiretapping. For the ease of determining the impact of each system parameter on the secrecy performance, we derived closed-form expressions for the lower bound of SOP and the SPSC. The RF link is assumed to be arbitrarily correlated and observations indicate that correlation degrades the secrecy capacity, significantly. Asymptotic SOP results also match perfectly with lower bound SOP results at high SNR regime and a perfect agreement of analytical and simulation results is noticed that clearly validates the derived mathematical expressions. In addition, impacts of turbulent fading and pointing error for two detection techniques were also examined and it is seen that the HD technique performs better than the IM/DD technique. Based on the location of the eavesdropper, it is noticed that enhanced performance is achieved when the eavesdropper utilizes the FSO link for wiretapping which is a clear indication of a higher level of security of the FSO link relative to the RF link. As the authors considered correlated multipath fading channel at the RF link, this work can be further extended by introducing correlated Generalized fading channels.

References

[1] 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.
[2] M. A. Esmail, H. Fathallah, and M. Alouini, "Outdoor FSO communications under fog: Attenuation modeling and performance evaluation," *IEEE Photon. J.*, vol. 8, no. 4, Aug. 2016, Art. no. 7905622.
[3] I. S. Ansari, M. M. Abdallah, M. Alouini, and K. A. Qaraqe, "A performance study of two hop transmission in mixed underlay RF and FSO fading channels," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2014, pp. 388–393.
[4] I. S. Ansari, F. Yilmaz, and M. Alouini, "On the sum of squared η-μ random variates with application to the performance of wireless communication systems," in *Proc. IEEE 77th Veh. Technol. Conf.*, 2013, pp. 1–6.
[5] A. Malik and P. Singh, "Free space optics: Current applications and future challenges," *Int. J. Opt.*, vol. 2015, p. 7, Art. no. 945483, 2015, doi: 10.1155/2015/945483
[6] H. A. Willebrand and B. S. Ghuman, "Fiber optics without fiber," *IEEE Spectrum*, vol. 38, no. 8, pp. 40–45, Aug. 2001.
[7] V. Sharma and G. Kaur, "High speed, long reach OFDM-FSO transmission link incorporating OSSB and OTSB schemes," *Optik*, vol. 124, no. 23, pp. 6111–6114, 2013.
[8] R. K. Z. Sahbudin, M. Kamarulzaman, S. Hitam, M. Mokhtar, and S. B. A. Anas, "Performance of SAC OCDMA-FSO communication systems," *Optik-Int. J. Light Electron. Opt.*, vol. 124, no. 17, pp. 2868–2870, 2013.
[9] 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.
[10] D. Kedar and S. Arnon, "Optical wireless communication through fog in the presence of pointing errors," *Appl. Opt.*, vol. 42, no. 24, pp. 4946–4954, 2003.
[11] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 57–96, Jan.–Mar. 2017.
[12] G. Karagiannidis, T. Tsiftsis, and H. Sandalidis, "Outage probability of relayed free space optical communication systems," *Electron. Lett.*, vol. 42, no. 17, pp. 994–996, 2006.
[13] H. G. Sandalidis, T. A. Tsiftsis, G. K. Karagiannidis, and M. Uysal, "BER performance of FSO links over strong atmospheric turbulence channels with pointing errors," *IEEE Commun. Lett.*, vol. 12, no. 1, pp. 44–46, Jan. 2008.
[14] 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.
[15] 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. 2011.
[16] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Impact of pointing errors on the performance of mixed RF/FSO dual-hop transmission systems," *IEEE Wireless Commun. Lett.*, vol. 2, no. 3, pp. 351–354, Jun. 2013.
[17] O. M. S. Al-Ebraheemy, A. M. Salhab, A. Chaaban, S. A. Zummo, and M. 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, Feb. 2019, Art. no. 7900522.

[18] H. Samimi and M. Uysal, "End-to-end performance of mixed RF/FSO transmission systems," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 11, pp. 1139–1144, Nov. 2013.

[19] 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, Feb. 2015, Art. no. 7900120.

[20] P. V. Trinh, T. C. Thang, and A. T. Pham, "Mixed mmWave RF/FSO relaying systems over generalized fading channels with pointing errors," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 5500414.

[21] 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, 2017.

[22] L. Chen and W. Wang, "Multi-diversity combining and selection for relay-assisted mixed RF/FSO system," *Opt. Commun.*, vol. 405, pp. 1–7, 2017.

[23] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IRE*, vol. 76, no. 5, pp. 533–549, May 1988.

[24] S. H. Islam *et al.*, "On secrecy performance of mixed generalized gamma and málaga RF-FSO variable gain relaying channel," *IEEE Access*, vol. 8, pp. 104 127–104138, 2020.

[25] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[26] 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, Apr. 2015, Art. no. 7901014.

[27] H. Yu and T. Kim, "Training and data structures for AN-aided secure communication," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2869–2872, Sep. 2019.

[28] H. Yu and I.-G. Lee, "Physical layer security based on NOMA and AJ for misose channels with an untrusted relay," *Future Gener. Comput. Syst.*, vol. 102, pp. 611–618, 2020.

[29] A. P. Shrestha, S. R. Islam, R. Dhakal, and K. S. Kwak, "Physical layer security for cooperative multihop routing in wireless networks," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf.*, 2019, pp. 0910–0915.

[30] 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.

[31] 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, Aug. 2017, Art. no. 7904814.

[32] 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 2017.

[33] 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.

[34] 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, Jun. 2018, Art. no. 7904113.

[35] 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.

[36] 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, 2018.

[37] 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.

[38] 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.

[39] A. Jurado-Navas, J. M. Garrido-Balsells, J. F. Paris, A. Puerta-Notario, and J. Awrejcewicz, "A unifying statistical model for atmospheric optical scintillation," *Numer. Simul. Phys. Eng. Processes*, vol. 181, no. 8, pp. 181–205, 2011.

[40] K. Cho, J. Lee, and C. G. Kang, "Stochastic geometry-based coverage and rate analysis under Nakagami & log-normal composite fading channel for downlink cellular networks," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1437–1440, Jun. 2017.

[41] I. Baştürk and B. Özbek, "Channel and queue aware joint relay selection and resource allocation for MISO-OFDMA based user-relay assisted cellular networks," *Telecommun. Syst.*, vol. 67, no. 4, pp. 619–633, 2018.

[42] 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, Aug. 2017, Art. no. 7904814.

[43] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[44] A. S. M. Badrudduza, M. Z. I. Sarkar, and M. K. Kundu, "Enhancing security in multicasting through correlated Nakagami-m fading channels with opportunistic relaying," *Phys. Commun.*, vol. 43, 2020, Art. no. 101177.

[45] H. Shin, "Capacity and error exponents for multiple-input multipleoutput wireless channels," Ph.D. dissertation, Seoul National Univ., Seoul, Korea, 2004.

[46] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*. Hoboken, NJ, USA: Wiley, 2005, vol. 95.

[47] V. A. Aalo, "Performance of maximal-ratio diversity systems in a correlated Nakagami-fading environment," *IEEE Trans. Commun.*, vol. 43, no. 8, pp. 2360–2369, Aug. 1995.

[48] M.-S. Alouini, A. Abdi, and M. Kaveh, "Sum of gamma variates and performance of wireless communication systems over Nakagami-fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, pp. 1471–1480, Nov. 2001.

[49] Q. T. Zhang, "Maximal-ratio combining over Nakagami fading channels with an arbitrary branch covariance matrix," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1141–1150, Jul. 1999.

[50] S. Al-Juboori and X. N. Fernando, "Multiantenna spectrum sensing over correlated Nakagami-*m* channels with MRC and EGC diversity receptions," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2155–2164, Mar. 2018.

[51] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. *US Government Printing Office*, 1948, vol. 55.

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

[53] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, "Performance analysis of free-space optical links over málaga *(M)* turbulence channels with pointing errors," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 91–102, Jan. 2016.

[54] 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," vol. 14, no. 3, pp. 210–222, 2019.

[55] 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.*, 2014, pp. 18–23.

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

[57] 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, 2020, Art. no. 125429.

[58] H. Lei *et al.*, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.

[59] M. D. Springer, "The algebra of random variables," Tech. Rep. 519.2 S67, 1979.

[60] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2013, pp. 659–664.

[61] 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.

[62] N. A. Sarker *et al.*, "Secrecy performance analysis of mixed hyper Gamma and Gamma-Gamma cooperative relaying system," *IEEE Access*, vol. 8, pp. 131273–131285, 2020.