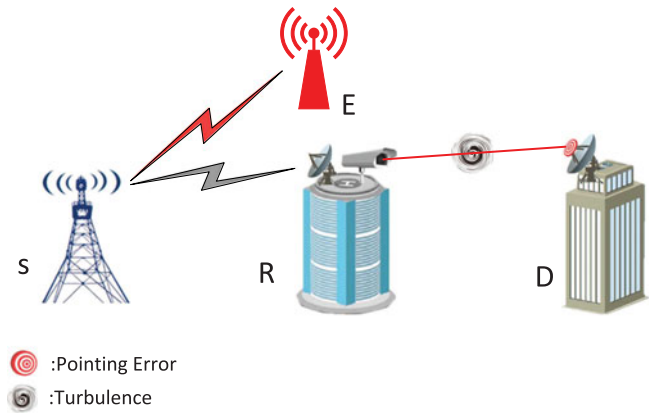
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

On Secrecy Performance of Mixed RF-FSO Systems

Volume 9, Number 4, August 2017

Hongjiang Lei, *Member, IEEE*
Zhijun Dai
Imran Shafique Ansari, *Member, IEEE*
Ki-Hong Park, *Member, IEEE*
Gaofeng Pan, *Member, IEEE*
Mohamed-Slim Alouini, *Fellow, IEEE*



DOI: 10.1109/JPHOT.2017.2723422
1943-0655 © 2017 IEEE

On Secrecy Performance of Mixed RF-FSO Systems

**Hongjiang Lei,[1,2] *Member, IEEE*, Zhijun Dai,[1]
Imran Shafique Ansari,[3] *Member, IEEE*,
Ki-Hong Park,[2] *Member, IEEE*, Gaofeng Pan,[4] *Member, IEEE*,
and Mohamed-Slim Alouini,[2] *Fellow, IEEE***

[1]Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[2]CEMSE Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia
[3]Department of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha 23874, Qatar
[4]School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K.

DOI:10.1109/JPHOT.2017.2723422

Manuscript received May 4, 2017; revised June 22, 2017; accepted June 30, 2017. Date of publication July 5, 2017; date of current version July 13, 2017. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61471076, in part by Chinese Scholarship Council under Grant 201607845004, in part by the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT_16R72, in part by the special fund for Key Lab of Chongqing Municipal Education Commission, in part by the Project of Fundamental and Frontier Research Plan of Chongqing under Grants cstc2015jcyjBX0085 and cstc2017jcyjAX0204, and in part by the Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grants KJ1600413 and KJ1704088. Corresponding author: Hongjiang Lei. (e-mail: leihj@cqupt.edu.cn)

Abstract: In this paper, we study the secrecy performance of a mixed radio frequency-free space optical (RF-FSO) transmission systems. All RF links experience Nakagami-*m* fading and the FSO link experiences the Gamma–Gamma fading. The effect of pointing error and two types of detection techniques (i.e., heterodyne detection and intensity modulation with direct detection) are considered. We derive closed-form expressions for lower bound of the secrecy outage probability (SOP) and exact average secrecy capacity (ASC). Furthermore, by utilizing the expansion of Meijer's G-function, asymptotic results for SOP and ASC are derived when the electrical signal-to-noise ratio of the FSO link tends to infinity. Numerical and Monte Carlo simulation results are provided to verify the accuracy of our proposed results.

Index Terms: Physical layer security, mixed radio frequency-free space optical (RF-FSO) systems, Gamma-Gamma fading, secrecy outage probability, average secrecy capacity.

1. Introduction

1.1 Background and Related Works

Free space optical (FSO) communications have received considerable attention because it can be utilized for fiber backup, back-haul for wireless cellular networks, enterprise/local area network connectivity, metropolitan area network extensions, and disaster recovery, etc. It is a cost-effective and wide bandwidth solution operating at the unlicensed optical spectrum [1]. Relative to radio

frequency (RF) communication systems, FSO communication systems have higher bandwidth and capacity. In addition, FSO is also regarded as a promising solution for the last mile problem in wireless communication. However, the atmospheric turbulence and pointing error significantly affect the performance of FSO systems [2], [3].

The mixed RF-FSO system has been presented as a solution to minimize the effect of atmospheric turbulence and pointing error [4]. In such networks, the information is transmitted via RF link to relay node. Then the relay forwards them to the destination over an FSO link. The system performance of the mixed RF-FSO systems has been analyzed in many prior research works, such as outage probability (OP), average bit error rate (ABER), and ergodic capacity (EC) [4]–[12]. The authors in [4] firstly analyzed the performance of a mixed Rayleigh - Gamma-Gamma systems and derived the closed-form expression for OP where the fixed gain amplify-and-forward (AF) and subcarrier intensity modulation schemes are utilized at relay node. The performance of AF-based mixed RF-FSO systems with pointing error was investigated in [5] and closed-form expressions for OP, ABER, and EC were derived. The closed-form expressions for OP, ABER, and EC of AF-based mixed RF-FSO systems over Nakagami-m - Gamma-Gamma channels were derived in [6] under the effect of the atmospheric turbulence over the FSO link along with the effects of turbulence and pointing error. Similar works for decode-and-forward (DF) based systems were performed in [7]. A unified performance analysis of mixed RF-FSO systems with both fixed and variable gain relay scheme was analyzed in [8] and the closed-form expressions for the exact and asymptotic OP, ABER, and EC were derived where both heterodyne detection (HD) and intensity modulation with direct detection (IM/DD) are considered. The RF link was modeled as $\eta - \mu$ or $\kappa - \mu$ fading in [9] and new analytical expressions for the exact and asymptotic OP and ABER were derived. The authors in [10] derived the closed-form expressions for OP and ABER of mixed dual-hop RF-FSO systems with semi-blind AF relaying under partial selection with outdated channel state estimation. The performance of multiple users over DF-based mixed RF-FSO syatems was analyzed in [11] and analytical expressions for the exact and asymptotic end-to-end OP and average symbol error probability (ASER) of each user were derived. The analysis in [11] was extended in [12] where the channel state information of the RF link was considered to be outdated and the effect of pointing error was also taken into account.

In recent years, physical layer security has been one of the hottest spots in information security as it can realize the perfect secrecy communication by utilizing the randomness and time-varying nature of the wireless channels without any encryption algorithm [13]–[15]. The physical layer security of Wyner's model over FSO channels was investigated in [16] and the closed-form expressions for probability of a non-zero secrecy capacity (PNSC) was derived. The effect of atmospheric turbulence on secrecy performance of orbital angular momentum (OAM) multiplexing FSO channels was analyzed in [17] and the numerical results demonstrated that the secrecy performance of FSO systems can be improved by using OAM multiplexing in weak and medium turbulence regimes. The communication over FSO link is more secure than traditional wireless communications due to the high directionality of laser beam. Since the RF link of mixed RF-FSO systems can be easily attacked by eavesdroppers, physical layer security of mixed RF-FSO systems has gained great attention from researchers. The security reliability trade-off (SRT) of mixed RF-FSO systems with opportunistic user scheduling scheme was analyzed in [18] and the closed-form expressions for the OP, average symbol error probability, channel capacity, and intercept probability (IP) were derived. Furthermore, the impact of RF co-channel interference on the SRT performance of multiuser mixed RF-FSO systems with opportunistic user scheduling was studied in [19] and the closed-form expressions for the IP was derived.

1.2 Motivation and Contributions

To date, based on the open literature and to the best of the authors' knowledge, it is still an open area to analyze the secrecy performance of mixed RF-FSO systems. In this paper, we investigate the secrecy performance of mixed RF-FSO networks over Nakagami-m - Gamma-Gamma fading

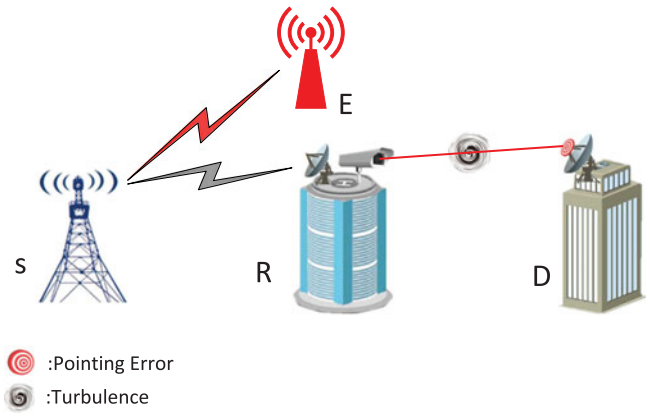


Fig. 1. System model of a mixed RF-FSO systems which consists of a source (S), a relay (R), a desired receiver/destination (D), and an undesired receiver/eavesdropper (E).

channels where the effects of pointing error and two types of detection techniques are considered. The main contributions of our work are listed as follows:

1) We investigate the secrecy performance of the mixed RF-FSO relaying over Nakagami-m - Gamma-Gamma fading channels in presence of fixed and variable gain relaying schemes. Both the effects of pointing error and two types of detection techniques are considered. The closed-form expressions for average secrecy capacity (ASC) and lower bound for secrecy outage probability (SOP) are derived.
2) Moreover, to obtain more insights about the secrecy performance of mixed RF-FSO systems, the closed-form expressions for asymptotic SOP and ASC are derived under both relaying schemes by utilizing the expansion of Meijer's G-function.
3) The accuracy of the derived analysis results are validated by Monte-Carlo simulations. From the numerical and simulation results, we find out that the secrecy performance deteriorates as the atmospheric turbulence conditions and the pointing error gets severe and HD technique can provide better secrecy performance compared with IM/DD.
4) Although the SRT was clearly illustrated by obtaining the relationship between the reliability and the security performance, the IP (security measure) only considered the wiretap channels and is a special case of physical layer security, in which the secrecy capacity is defined as the difference between the capacity of main and eavesdropper channels. Relative to [18] and [19], generalized secrecy performance (ASC and SOP) is analyzed in this work. We also investigate the effects of fading/scintillation parameters, pointing error, and detection techniques on the physical layer security of mixed RF-FSO systems with fixed and variable gain relaying schemes.

2. Channel and System Models

In this work, a mixed RF-FSO system is considered, which is composed of Nakagami-m fading and Gamma-Gamma atmospheric turbulence with pointing error under IM/DD and HD techniques. As shown in Fig. 1, the confidential information is sent by source node S to the destination D through an intermediate relay R, in which AF scheme is utilized, where an eavesdropper node E attempts to obtain the confidential information through decoding the signal received. It is assumed that ideal angle-of-arrival tracking system is employed at the receiver so that the received signal phasefront can be estimated and perfectly compensated. Thus, there is no phase misalignment between the receiver and local fields in the focal plane so that the idealized coherent detection is achieved [20].

Since all the RF links experience the Nakagami-m fading, the probability density function (PDF) and cumulative distribution function (CDF) for the received signal-to-noise ratio (SNR) at R and E

are given by

$$f_{Si}(\gamma) = \frac{{\lambda_i}^{m_i}}{\Gamma(m_i)}\gamma^{m_i-1}e^{-\lambda_i\gamma}, \tag{1}$$

$$F_{Si}(\gamma) = \frac{\Upsilon(m_i, \lambda_i\gamma)}{\Gamma(m_i)} = 1 - e^{-\lambda_i\gamma}\sum_{n=0}^{m_i-1}\frac{{\lambda_i}^n}{n!}\gamma^n, \tag{2}$$

respectively, where $i \in \{R, E\}$, $\lambda_i = \frac{m_i}{\bar{\gamma}_i}$, m_i is the fading parameter that is integer and $\bar{\gamma}_i$ is average SNR, respectively, and $\Gamma(\cdot)$ is the Gamma function as defined by [21, eq. (8.310)].

The CDF of the FSO link is given as [22]

$$F_{RD}(\gamma) = \eta G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|\begin{matrix}1,K_1\\K_2,0\end{matrix}\right.\right], \tag{3}$$

where $\eta = \frac{\xi^2 r^{\alpha+\beta-2}}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)}$, r is the parameter that represents the type of detection being utilized, i.e., $r = 1$ is associated with HD and $r = 2$ is associated with IM/DD, ξ signifies the ratio between the equivalent beam radius and the pointing error displacement standard deviation (jitter) at the destination [23], α and β are the fading parameters related to the atmospheric turbulence conditions [24], $\rho = \frac{(h\alpha\beta)^r}{\mu_r r^{2r}}$, μ_r represents the electrical SNR of the FSO link, $K_1 = \Delta\left(r, \xi^2 + 1\right)$, $K_2 = \Delta\left(r, \xi^2\right)$, $\Delta(r, \alpha)$, $\Delta(r, \beta)$, where $\Delta(k, a) = \frac{a}{k}, \frac{a+1}{k}, \ldots, \frac{a+k-1}{k}$, $h = \frac{\xi^2}{\xi^2+1}$, and $G_{p,q}^{m,n}[\cdot]$ is the Meijer's G-function, as defined by [21, eq. (9.301)].

2.1 Fixed Gain Relaying

When fixed gain relaying scheme is utilized at R, the received SNR at D can be expressed as [8], [25]

$$\gamma_{eq}^{\mathrm{F}} = \frac{\gamma_{SR}\gamma_{RD}}{\gamma_{RD} + C}, \tag{4}$$

where γ_{SR} and γ_{RD} denote the SNR of the RF $S-R$ link and FSO $R-D$ link, respectively, C stands for a fixed relay gain [25]. The CDF of γ_{eq}^{F} is given as [8]

$$\begin{aligned} F_{\gamma_{eq}^{\mathrm{F}}}(\gamma) &= 1 - \underbrace{\eta\sum_{p=0}^{m_R-1}\sum_{q=0}^{p}\frac{{\lambda_R}^{p-q}}{q!\,(p-q)!}}_{\triangleq\sum_{pq}}\gamma^{p-q}e^{-\lambda_R\gamma}G_{r,3r+1}^{3r+1,0}\left[\rho C\lambda_R\gamma\left|\begin{matrix}K_1\\K_3\end{matrix}\right.\right] \\ &= 1 - \sum_{pq}\gamma^{p-q}e^{-\lambda_R\gamma}G_{r,3r+1}^{3r+1,0}\left[\rho C\lambda_R\gamma\left|\begin{matrix}K_1\\K_3\end{matrix}\right.\right], \end{aligned} \tag{5}$$

where $K_3 = [K_2, q]$. When $\mu_r \to \infty$, the asymptotic CDF of γ_{eq}^{F} is given as [8]

$$F_{\gamma_{eq}^{\mathrm{F}},RD}^{\infty}(\gamma) = 1 - \sum_{pq}\sum_{k=1}^{3r+1}B_k\gamma^{p-q+K_{3,k}}e^{-\lambda_R\gamma}, \tag{6}$$

where $B_k = (\rho\lambda_R C)^{K_{3,k}}\frac{\prod_{l=1,l\neq k}^{3r+1}\Gamma(K_{3,l}-K_{3,k})}{\prod_{l=1}^{r}\Gamma(K_{1,l}-K_{3,k})}$.

2.2 Variable Gain Relaying

When the CSI-assisted relaying scheme is utilized at R, the received SNR at D can be expressed as [25]

$$\gamma_{eq}^{V} = \frac{\gamma_{SR}\gamma_{RD}}{\gamma_{SR} + \gamma_{RD} + 1} \cong \min\left(\gamma_{SR}, \gamma_{RD}\right). \tag{7}$$

The CDF of γ_{eq}^{V} is given as [8]

$$F_{\gamma_{eq}^{V},RD}\left(\gamma\right) = 1 + \left(e^{-\lambda_R\gamma}\sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\gamma^p\right)\left(\eta G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|\begin{matrix}1,K_1\\K_2,0\end{matrix}\right.\right] - 1\right). \tag{8}$$

When $\mu_r \to \infty$, the asymptotic CDF of γ_{eq}^{V} is given as [8]

$$F_{\gamma_{eq}^{V},RD}^{\infty}\left(\gamma\right) = 1 + e^{-\lambda_R\gamma}\sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\gamma^p\left(\eta\sum_{q=1}^{3r}\varphi_q\gamma^{K_{2,q}} - 1\right), \tag{9}$$

where $\varphi_q = \rho^{K_{2,q}}\prod_{l=1,l\neq q}^{3r}\Gamma\left(K_{2,l} - K_{2,q}\right)\Big/\left(K_{2,q}\prod_{l=1}^{r}\Gamma\left(K_{1,l} - K_{2,q}\right)\right)$.

3. Secrecy Outage Probability Analysis

A secrecy outage event occurs when the instantaneous secrecy capacity falls below a target secrecy rate R_s. Thus, the SOP of mixed RF-FSO can be expressed as [26], [27]

$$\begin{aligned} P_{out}\left(R_s\right) &= \Pr\left\{C_s\left(\gamma_{eq}, \gamma_{SE}\right) \leq R_s\right\} \\ &= \Pr\left\{\gamma_{eq} \leq \Theta\gamma_{SE} + \Theta - 1\right\} \\ &= \int_0^{\infty} F_{eq}\left(\Theta\gamma_{SE} + \Theta - 1\right) f_{SE}\left(\gamma_{SE}\right) d\gamma_{SE}, \end{aligned} \tag{10}$$

where $\Theta = e^{R_s}$. In the following, we derive the lower bound of the SOP as follows [28]

$$\begin{aligned} P_{out}\left(R_s\right) &= \Pr\left\{\gamma_{eq} \leq \Theta\gamma_{SE} + \Theta - 1\right\} \\ &\geq P_{out}^{L}\left(R_s\right) = \Pr\left\{\gamma_{eq} \leq \Theta\gamma_{SE}\right\}. \end{aligned} \tag{11}$$

3.1 The Lower Bound With Fixed Gain Relaying

Substituting (1) and (5) into (11), making use of [28, eq. (8)] and [29, eq. (21)], and with some simple algebraic manipulations, we obtain

$$\begin{aligned} P_{out}^{F,L}\left(R_s\right) &= \int_0^{\infty} F_{\gamma_{eq}^{F}}\left(\Theta\gamma\right) f_{SE}\left(\gamma\right) d\gamma \\ &= 1 - \frac{{\lambda_E}^{m_E}}{\Gamma\left(m_E\right)}\sum_{pq}\Theta^{p-q}\int_0^{\infty}\gamma^{m_E+p-q-1}e^{-\left(\lambda_E+\lambda_R\Theta\right)\gamma}G_{r,3r+1}^{3r+1,0}\left[\rho C\lambda_R\Theta\gamma\left|\begin{matrix}K_1\\K_3\end{matrix}\right.\right]d\gamma \\ &= 1 - \frac{{\lambda_E}^{m_E}}{\Gamma\left(m_E\right)}\sum_{pq}\Theta^{p-q}\left(\lambda_R\Theta + \lambda_E\right)^{q-m_E-p}G_{r+1,3r+1}^{3r+1,1}\left[\frac{\rho C\lambda_R\Theta}{\lambda_R\Theta + \lambda_E}\left|\begin{matrix}1-p-m_E+q,K_1\\K_3\end{matrix}\right.\right]. \end{aligned} \tag{12}$$

3.2 The Lower Bound With Variable Gain Relaying

Substituting (1) and (8) into (11) and making use of [28, eq. (8)], [29, eq. (21)], and [21, eq. (3.326.2)], we obtain

$$\begin{aligned} P_{out}^{\mathrm{V,L}}(R_s) &= \int_0^{\infty} F_{\gamma_{eq}^{\mathrm{V}}}(\Theta\gamma) f_{SE}(\gamma)\, d\gamma \\ &= 1 + \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p=0}^{m_R-1} \frac{{\lambda_R}^p}{p!} \Theta^p \int_0^{\infty} \gamma^{m_E+p-1} e^{-(\lambda_R\Theta+\lambda_E)\gamma} \left(\eta G_{r+1,3r+1}^{3r,1}\left[\Theta\rho\gamma \left| \begin{matrix} 1,K_1 \\ K_2,0 \end{matrix} \right. \right] - 1 \right) d\gamma \\ &= 1 + \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p=0}^{m_R-1} \frac{(\Theta\lambda_R)^p}{p!} \left(H_1^L - H_2^L \right), \end{aligned} \tag{13}$$

where $H_1^L = \eta(\lambda_R\Theta+\lambda_E)^{-m_E-p} G_{r+2,3r+1}^{3r,2}\left[\frac{\Theta\rho}{\lambda_R\Theta+\lambda_E} \left| \begin{matrix} 1,1-m_E-p,K_1 \\ K_2,0 \end{matrix} \right. \right]$ and $H_2^L = \frac{\Gamma(m_E+p)}{(\lambda_R\Theta+\lambda_E)^{m_E+p}}$.

Another important metric to evaluate the security performance of passive eavesdropping, PNSC, can be easily obtained by utilizing the relationship between SOP and PNSC [28].

In order to get more insights, in the following subsection we will analyze the secrecy outage performance where the destination D is located close to the relay R, which can be mathematically described as $\mu_r \to \infty$.

3.3 Asymptotic Secrecy Outage Probability When $\mu_r \to \infty$ With Fixed Gain Relaying

Substituting (1) and (6) into (11) and making use of [21, eq. (3.326.2)], we have

$$\begin{aligned} P_{out,RD}^{\mathrm{F,L},\infty}(R_s) &= \int_0^{\infty} F_{\gamma_{eq}^{\mathrm{F}},RD}^{\infty}(\Theta\gamma) f_{SE}(\gamma)\, d\gamma \\ &= 1 - \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p}\sum_{q} \sum_{k=1}^{3r+1} B_k \Theta^{p-q+K_{3,k}} \int_0^{\infty} \gamma^{p-q+K_{3,k}+m_E-1} e^{-(\lambda_R\Theta+\lambda_E)\gamma} d\gamma \\ &= 1 - \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p}\sum_{q} \sum_{k=1}^{3r+1} B_k \Theta^{p-q+K_{3,k}} (\lambda_R\Theta+\lambda_E)^{q-p-m_E-K_{3,k}} \Gamma(p-q+m_E+K_{3,k}). \end{aligned} \tag{14}$$

3.4 Asymptotic Secrecy Outage Probability When $\mu_r \to \infty$ With Variable Gain Relaying

Substituting (1) and (9) into (11) and making use of [21, eq. (3.326.2)], we have

$$\begin{aligned} P_{out,RD}^{\mathrm{V,L},\infty}(R_s) &= \int_0^{\infty} F_{\gamma_{eq}^{\mathrm{V}},RD}^{\infty}(\Theta\gamma) f_{SE}(\gamma)\, d\gamma \\ &= 1 + \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p=0}^{m_R-1} \frac{{\lambda_R}^p}{p!} \Theta^p \int_0^{\infty} e^{-(\lambda_R\Theta+\lambda_E)\gamma} \gamma^{m_E+p-1} \left(\eta \sum_{q=1}^{3r} \varphi_q \Theta^{K_{2,q}} \gamma^{K_{2,q}} - 1 \right) d\gamma \\ &= 1 + \frac{{\lambda_E}^{m_E}}{\Gamma(m_E)} \sum_{p=0}^{m_R-1} \frac{(\Theta\lambda_R)^p}{p!} \left(\left(\eta \sum_{q=1}^{3r} \frac{\varphi_q \Theta^{K_{2,q}} \Gamma(K_{2,q}+p+m_E)}{(\lambda_R\Theta+\lambda_E)^{K_{2,q}+p+m_E}} \right) - \frac{\Gamma(m_E+p)}{(\lambda_R\Theta+\lambda_E)^{m_E+p}} \right). \end{aligned} \tag{15}$$

4. Average Secrecy Capacity Analysis

ASC is the most important metric to evaluate the security performance of active eavesdropping [26], [27], [30]. When all the channels experience independent fading, the ASC can be expressed as [30]

$$\bar{C}_s = \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1 - F_{eq}(\gamma)\right) d\gamma. \tag{16}$$

4.1 Exact Average Secrecy Capacity With Fixed Gain Relaying

Substituting (2) and (5) into (16), we have

$$\begin{aligned}\bar{C}_s^F &= \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1 - F_{\gamma_{eq}^F}(\gamma)\right) d\gamma \\ &= \sum\nolimits_{pq} (H_1 - H_2),\end{aligned} \tag{17}$$

where

$$H_1 = \int_0^\infty \frac{1}{1+\gamma}\gamma^{p-q} e^{-\lambda_R \gamma} G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma,$$

$$H_2 = \sum_{n=0}^{m_E-1} \frac{{\lambda_E}^n}{n!} \int_0^\infty \frac{\gamma^{p-q+n}}{1+\gamma} e^{-(\lambda_R+\lambda_E)\gamma} G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma.$$

Making use of [29, eq. (10) and (11)], [21, eq. (9.31.5)], and [31, eq. (20)], we have

$$\begin{aligned} H_1 &= \int_0^\infty \frac{\gamma^{p-q}}{1+\gamma} e^{-\lambda_R\gamma} G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma \\ &= \int_0^\infty G_{0,1}^{1,0}\left[\lambda_R \gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right] G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} p-q \\ p-q \end{matrix}\right] G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma \\ &= \frac{1}{\lambda_R} G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} p-q \\ p-q \end{matrix} \middle| \begin{matrix} K_1 \\ K_3 \end{matrix} \middle| \frac{1}{\lambda_R}, \rho C \right], \end{aligned} \tag{18}$$

$$\begin{aligned} H_2 &= \sum_{n=0}^{m_E-1} \frac{{\lambda_E}^n}{n!} \int_0^\infty \frac{\gamma^{n+p-q}}{1+\gamma} e^{-(\lambda_R+\lambda_E)\gamma} G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma \\ &= \sum_{n=0}^{m_E-1} \frac{{\lambda_E}^n}{n!} \int_0^\infty G_{0,1}^{1,0}\left[(\lambda_R+\lambda_E)\gamma \middle| \begin{matrix} - \\ 0 \end{matrix}\right] G_{1,1}^{1,1}\left[\gamma \middle| \begin{matrix} n+p-q \\ n+p-q \end{matrix}\right] G_{r,3r+1}^{3r+1,0}\left[\rho C \lambda_R \gamma \middle| \begin{matrix} K_1 \\ K_3 \end{matrix}\right] d\gamma \\ &= \frac{1}{\lambda_R+\lambda_E} \sum_{n=0}^{m_E-1} \frac{{\lambda_E}^n}{n!} G_{1,0:1,1:r,3r+1}^{1,0:1,1:3r+1,0}\left[\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} n+p-q \\ n+p-q \end{matrix} \middle| \begin{matrix} K_1 \\ K_3 \end{matrix} \middle| \frac{1}{\lambda_R+\lambda_E}, \frac{\rho C \lambda_R}{\lambda_R+\lambda_E} \right], \end{aligned} \tag{19}$$

where $G_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}[\cdot]$ is the extended generalized bivariate Meijer's G-function (EGBMGF), as defined by [32, eq. (8)] with implementation given in [33, Table 1].

4.2 Exact Average Secrecy Capacity With Variable Gain Relaying

Substituting (2) and (8) into (16), we have

$$\begin{aligned}\bar{C}_s^V &= \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1-F_{\gamma_{eq}^V}(\gamma)\right)d\gamma \\ &= \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\underbrace{\int_0^\infty \frac{1}{1+\gamma}e^{-\lambda_R\gamma}\gamma^p\,d\gamma}_{C_1} - \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\underbrace{\eta\int_0^\infty \frac{1}{1+\gamma}e^{-\lambda_R\gamma}\gamma^p G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma}_{C_2} \\ &\quad - \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\underbrace{\sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\int_0^\infty \frac{1}{1+\gamma}\gamma^{p+n}e^{-(\lambda_R+\lambda_E)\gamma}d\gamma}_{C_3} \\ &\quad + \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\underbrace{\eta\sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\int_0^\infty \frac{1}{1+\gamma}\gamma^{p+n}e^{-(\lambda_R+\lambda_E)\gamma}G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma}_{C_4} \\ &= \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}(C_1-C_2-C_3+C_4). \end{aligned} \tag{20}$$

Making use of [34, eq. (2.3.6.9)], we have

$$C_1 = \Gamma(p+1)\,\psi(p+1,p+1;\lambda_R), \tag{21}$$

$$C_3 = \sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\Gamma(p+n+1)\,\psi(p+n+1,p+n+1;\lambda_E+\lambda_R), \tag{22}$$

where $\psi(a,b;c)$ is confluent hypergeometric function, as defined by [21, eq. (9.211.4)].

By using of [29, eq. (10) and (11)], [21, eq. (9.31.5)], and [31, eq. (20)], we obtain

$$\begin{aligned} C_2 &= \eta\int_0^\infty \frac{1}{1+\gamma}e^{-\lambda_R\gamma}\gamma^p G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma \\ &= \eta\int_0^\infty G_{0,1}^{1,0}\left[\lambda_R\gamma\left|{}^{-}_{0}\right.\right]G_{1,1}^{1,1}\left[\gamma\left|{}^{p}_{p}\right.\right]G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma \\ &= \eta G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1}\left[\left.{}^{1}_{-}\right|{}^{p}_{p}\left|{}^{1,K_1}_{K_2,0}\right|\frac{1}{\lambda_R},\frac{\rho}{\lambda_R}\right], \end{aligned} \tag{23}$$

$$\begin{aligned} C_4 &= \eta\sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\int_0^\infty \frac{1}{1+\gamma}\gamma^{p+n}e^{-(\lambda_R+\lambda_E)\gamma}G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma \\ &= \eta\sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\int_0^\infty G_{0,1}^{1,0}\left[(\lambda_E+\lambda_R)\gamma\left|{}^{-}_{0}\right.\right]G_{1,1}^{1,1}\left[\gamma\left|{}^{p+n}_{p+n}\right.\right]G_{r+1,3r+1}^{3r,1}\left[\rho\gamma\left|{}^{1,K_1}_{K_2,0}\right.\right]d\gamma \\ &= \frac{\eta}{\lambda_E+\lambda_R}\sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1}\left[\left.{}^{1}_{-}\right|{}^{p+n}_{p+n}\left|{}^{1,K_1}_{K_2,0}\right|\frac{1}{\lambda_E+\lambda_R},\frac{\rho}{\lambda_E+\lambda_R}\right]. \end{aligned} \tag{24}$$

4.3 Asymptotic Secrecy Capacity When $\mu_r \to \infty$ With Fixed Gain Relaying

Substituting (1) and (6) into (16) and utilizing [34, eq. (2.3.6.9)], we have

$$\bar{C}_{s,RD}^{F,\infty} = \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1 - F_{\gamma_{eq}^F,RD}^{\infty}(\gamma)\right) d\gamma$$
$$= \sum_{pq}\sum_{k=1}^{3r+1} B_k \left(H_{1,RD}^{\infty} - H_{2,RD}^{\infty}\right), \tag{25}$$

where $H_{1,RD}^{\infty} = \Gamma(\alpha)\,\psi(\alpha,\alpha;\lambda_R)$, $H_{2,RD}^{\infty} = \sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\Gamma(\alpha+n)\,\psi(\alpha+n,\alpha+n;\lambda_R+\lambda_E)$, and $\alpha = p - q + K_{3,k} + 1$.

4.4 Asymptotic Secrecy Capacity When $\mu_r \to \infty$ With Variable Gain Relaying

Substituting (1) and (9) into (16) and utilizing [34, eq. (2.3.6.9)], we obtain

$$\bar{C}_{s,RD}^{V,\infty} = \int_0^\infty \frac{F_{SE}(\gamma)}{1+\gamma}\left(1 - F_{\gamma_{eq}^V,RD}^{\infty}(\gamma)\right) d\gamma$$
$$= \sum_{p=0}^{m_R-1}\frac{{\lambda_R}^p}{p!}\left(C_{1,RD}^{\infty} - C_{2,RD}^{\infty}\right), \tag{26}$$

where

$$C_{1,RD}^{\infty} = \int_0^\infty \frac{\gamma^p}{1+\gamma} e^{-\lambda_R\gamma}\left(1 - \eta\sum_{q=1}^{3r}\varphi_q\gamma^{K_{2,q}}\right) d\gamma, \tag{27}$$

$$C_{2,RD}^{\infty} = \sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\int_0^\infty \frac{\gamma^{p+n}}{1+\gamma} e^{-(\lambda_R+\lambda_E)\gamma}\left(1 - \eta\sum_{q=1}^{3r}\varphi_q\gamma^{K_{2,q}}\right) d\gamma. \tag{28}$$

Making use of [34, eq. (2.3.6.9)], we obtain

$$C_{1,RD}^{\infty} = \Gamma(p+1)\,\psi(p+1,p+1;\lambda_R)$$
$$- \eta\sum_{q=1}^{3r}\varphi_q\Gamma\left(K_{2,q}+p+1\right)\psi\left(K_{2,q}+p+1,K_{2,q}+p+1;\lambda_R\right), \tag{29}$$

$$C_{2,RD}^{\infty} = \sum_{n=0}^{m_E-1}\frac{{\lambda_E}^n}{n!}\left(\Gamma(p+n+1)\,\psi(p+n+1,p+n+1;\lambda_R+\lambda_E)\right.$$
$$\left. - \eta\sum_{q=1}^{3r}\varphi_q\Gamma\left(K_{2,q}+p+n+1\right)\psi\left(K_{2,q}+p+n+1,K_{2,q}+p+n+1;\lambda_R+\lambda_E\right)\right). \tag{30}$$

5. Numerical Results and Discussions

In this section, numerical and Monte-Carlo simulations results are presented to verify our analytical results. Furthermore, the impacts of pointing error and detection techniques on the secrecy performance are demonstrated. The main parameters utilized in simulations and analysis are set as $m_R = m_E = 2$, $C = 1$, and $R_s = 0.01$ nat/s.

The impact of ξ, α, and β on SOP and ASC is investigated in Figs. 2–5 for both fixed and variable gain relaying schemes, respectively. One can observe that the analysis results match very well with simulation curves in all the figures. It can also be observed that increasing $\bar{\gamma}_{SR}$ always affects the secrecy performance of the mixed systems with fixed gain relaying scheme but this is not true for

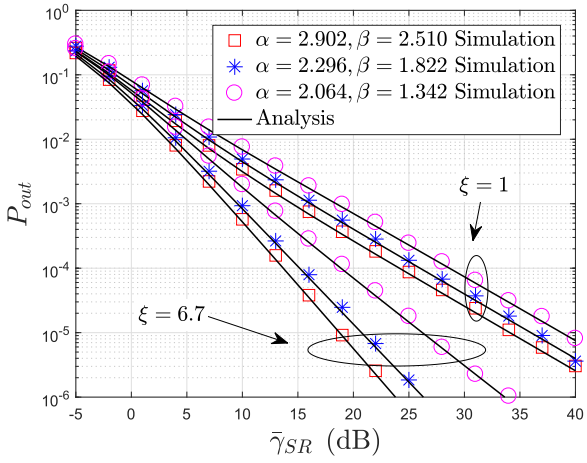


Fig. 2. SOP for fixed gain relaying versus $\bar{\gamma}_{SR}$ with $r = 1$, $\mu_r = 10$ dB, and $\bar{\gamma}_{SE} = -10$ dB.

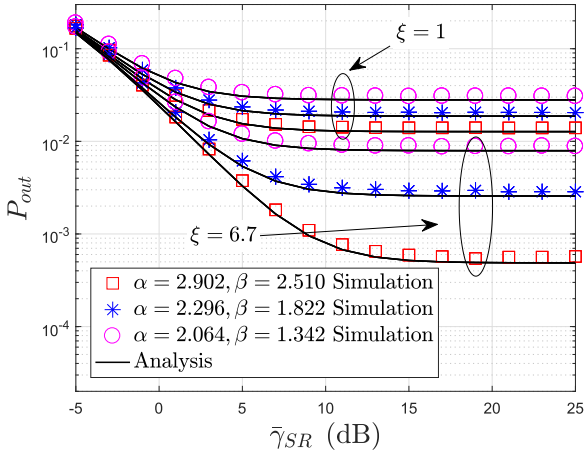


Fig. 3. SOP for variable gain relaying versus $\bar{\gamma}_{SR}$ with $r = 1$, $\mu_r = 10$ dB, and $\bar{\gamma}_{SE} = -10$ dB.

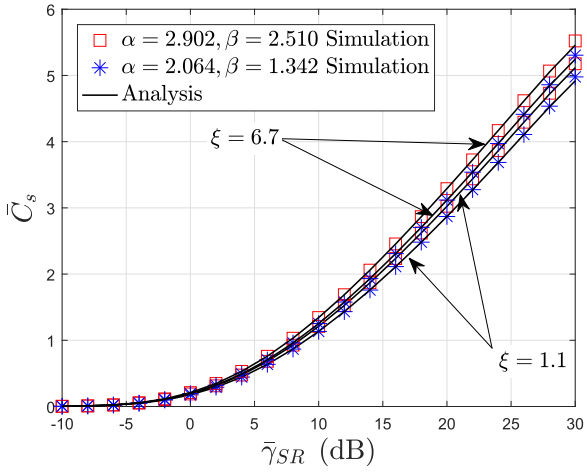


Fig. 4. ASC for fixed gain relaying versus $\bar{\gamma}_{SR}$ with with $r = 2$, $\mu_r = 5$ dB, and $\bar{\gamma}_{SE} = -5$ dB.

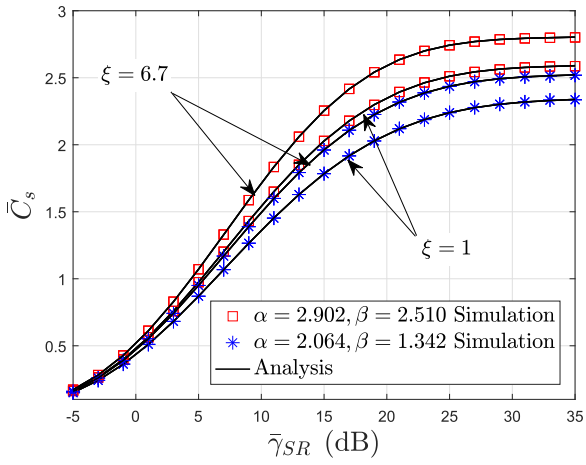


Fig. 5. ASC for variable gain relaying versus $\bar{\gamma}_{SR}$ with $r = 2$, $\mu_r = 15$ dB, and $\bar{\gamma}_{SE} = -10$ dB.

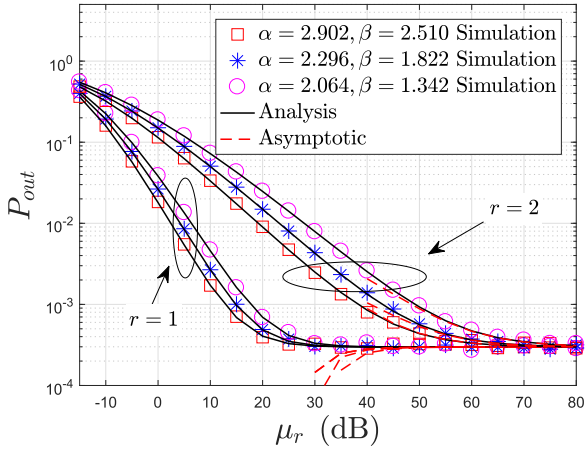


Fig. 6. SOP for fixed gain relaying versus μ_r with $\xi = 6.7$, $\bar{\gamma}_{SR} = 20$ dB, and $\bar{\gamma}_{SE} = 0$ dB.

that with the variable gain relaying scheme. This is because the SNR at D with variable gain relaying will be equal to $\bar{\gamma}_{RD}$ even when $\bar{\gamma}_{SR}$ becomes large. One can also observe from all the figures that the secrecy performance deteriorates as the pointing error gets severe (i.e., the lower the values of ξ, the higher the SOP will be and the lower the ASC will be). Furthermore, we can find from Fig. 2 that the secrecy diversity order of the mixed system with fixed gain relaying depends on the pointing error when pointing error is strong ($\xi = 1$). When the pointing error is negligible ($\xi = 6.7$), the secrecy diversity order dominates by the atmospheric turbulence and the fading of RF link.

The effect of detection techniques and atmospheric turbulence conditions on SOP and ASC is investigated in Figs. 6–9 for both relaying schemes, respectively. It can be observed that HD technique ($r = 1$) provides better secrecy performance compared to the IM/DD technique ($r = 2$), (i.e., the lower SOP or the higher ASC). This is because the SNR at destination with HD technique outperforms the one with IM/DD technique, as testified in [8], [22], and [24]. because physical layer security is utilizing the physical characteristics of wireless channels (such as fading, turbulence, and pointing error, etc.) to enhance the secrecy performance.

Additionally, we can observe that the secrecy performance for a higher (α, β) outperforms the one for a lower (α, β), which are the fading/scintillation parameters, respectively. This is because the atmospheric turbulence only influences the SNR at D. It also can be observed that at high SNR

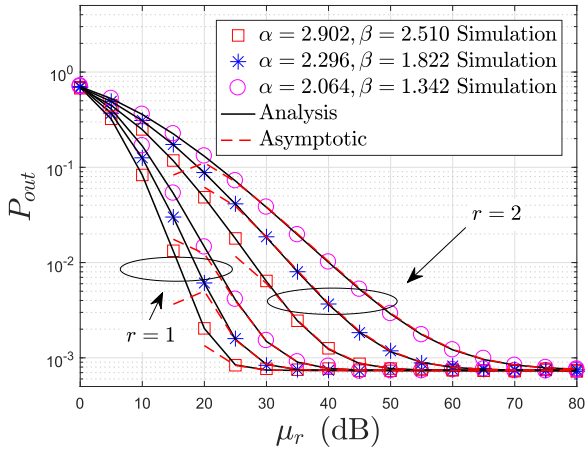


Fig. 7. SOP for variable gain relaying versus μ_r with $\xi = 6.7$, $\bar{\gamma}_{SR} = 20$ dB, and $\bar{\gamma}_{SE} = 2$ dB.

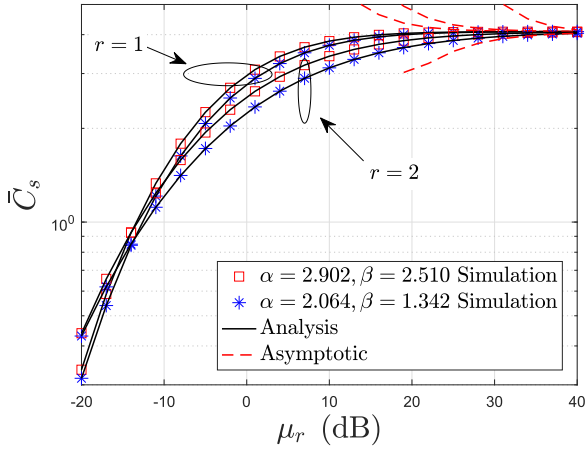


Fig. 8. ASC for fixed gain relaying versus μ_r with $\xi = 1$, $\bar{\gamma}_{SR} = 20$ dB, and $\bar{\gamma}_{SE} = -5$ dB.

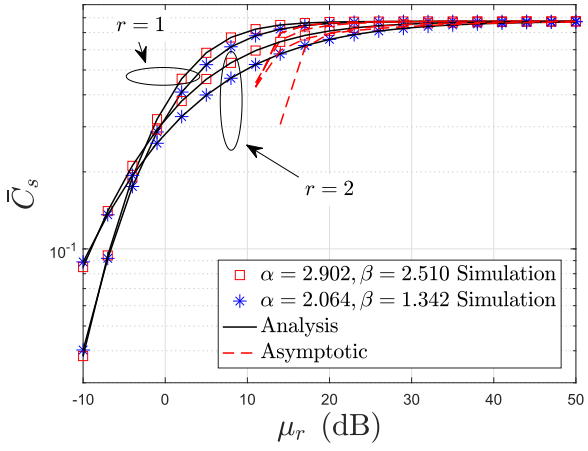


Fig. 9. ASC for variable gain relaying versus μ_r with $\xi = 1.1$, $\bar{\gamma}_{SR} = 2$ dB, and $\bar{\gamma}_{SE} = -10$ dB.

regime, the asymptotic expression utilizing the Meijer's G-function expansion converges quite fast to the exact result proving its tightness.

6. Conclusion

In this work, the secrecy performance of mixed RF-FSO systems was investigated. The exact and asymptotic closed-form expressions for the SOP and ASC were derived and validated through simulations. Numerical results illustrated that the RF link has less influence to the secrecy performance of the mixed systems with variable gain relaying and the pointing error deteriorates the secrecy performance of mixed systems. Besides, the secrecy performance in weak atmospheric turbulence conditions outperforms that of strong conditions since atmospheric turbulence only influences the SNR at destination. Furthermore, we found that HD technique provides better secrecy performance compared to the IM/DD technique.

References

[1] D. Kedar and S. Arnon, "Urban optical wireless communication networks: The main challenges and possible solutions," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. S2–S7, May 2004.

[2] M. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," *Opt. Eng.*, vol. 40, no. 8, pp. 1554–1562, Aug. 2001.

[3] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing error," *J. Lightw. Technol.*, vol. 25, no. 7, pp. 1702–1710, Jul. 2007.

[4] 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.

[5] I. S. Ansari, F. Yilmaz, and M. S. Alouini, "Impact of pointing error on the performance of mixed RF/FSO dual-hop transmission systems," *IEEE Wireless Commun. Lett.*, vol. 2, no. 3, pp. 351–354, Jun. 2013.

[6] S. Anees and M. R. Bhatnagar, "Performance of an amplify-and-forward dual-hop asymmetric RF-FSO communication system," *IEEE J. Opt. Commun. Netw.*, vol. 7, no. 2, pp. 124–135, Feb. 2015.

[7] S. Anees and M. R. Bhatnagar, "Performance evaluation of decode-and-forward dual-hop asymmetric radio frequency-free space optical communication system," *IET Optoelectron.*, vol. 9, no. 5, pp. 232–240, Oct. 2015.

[8] 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.

[9] J. Zhang, L. Dai, Y. Zhang, and Z. Wang, "Unified performance analysis of mixed radio frequency/free-space optical dual-hop transmission systems," *J. Lightw. Technol.*, vol. 33, no. 11, pp. 2286–2293, Jul. 2015.

[10] M. I. Petkovic, A. M. Cvetkovic, G. T. Djordjevic, and G. K. Karagiannidis, "Partial relay selection with outdated channel state estimation in mixed RF/FSO systems," *J. Lightw. Technol.*, vol. 33, no. 13, pp. 2860–2867, Jul. 2015.

[11] N. I. Miridakis, M. Matthaiou, and G. K. Karagiannidis, "Multiuser relaying over mixed RF/FSO links," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1634–1645, May 2014.

[12] A. M. Salhab, F. S. Al-Qahtani, R. M. Radaydeh, S. A. Zummo, and H. Alnuweiri, "Power allocation and performance of multiuser mixed RF/FSO relay networks with opportunistic scheduling and outdated channel information," *J. Lightw. Technol.*, vol. 34, no. 13, pp. 3259–3272, Jul. 2016.

[13] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer-Verlag, 2016.

[14] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. Switzerland: Springer-Verlag, 2016.

[15] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over $\alpha - \mu$ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[16] 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.

[17] 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, Feb. 2016, Art. no. 7901110.

[18] 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.

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

[20] R. M. Gagliardi and S. Karp, *Optical Communications*. New York, NY, USA: Wiley-Interscience, 1976.

[21] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[22] 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.*, Glasgow, May 2015, pp. 1–5.

[23] 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.

[24] 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.

[25] M. O. Hasna and M.-S. Alouini, "A performance study of dual-hop transmissions with fixed gain relays," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1963–1968, Nov. 2004.
[26] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[27] H. Lei *et al.*, "Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 408–411, Feb. 2016.
[28] 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.
[29] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, Tokyo, Japan, 1990, pp. 212–224.
[30] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[31] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. Qaraqe, "On physical layer security over SIMO generalized-K fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.
[32] S. C. Gupta, "Integrals involving products of G-function," *Proc. Nat. Acad. Sci., India*, vol. 39(A), no. II, pp. 193–200, Apr. 1969.
[33] 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.
[34] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series, vol. 1: Elementary Functions*. New York, NY, USA: Gordon and Breach, 1992.