The Secrecy Comparison of RF and FSO Eavesdropping Attacks in Mixed RF-FSO Relay Networks

Eylem Erdogan, *Senior Member, IEEE*, Ibrahim Altunbas, *Senior Member, IEEE*, Gunes Karabulut Kurt, *Senior Member, IEEE*, and Halim Yanikomeroglu, *Fellow, IEEE*

***Abstract*—In this paper, we study the secrecy performance of mixed radio-frequency (RF) - free space optical (FSO) systems by considering both RF and FSO eavesdropper attacks. More precisely, we shed light into the design of secure mixed RF-FSO relay networks by questioning two critical design problems: 1) What are the main parameters in the design of secure RF-FSO relay networks? 2) How can we improve the confidentiality of the optical information? To do so, we derive the secrecy outage probability and the probability of positive secrecy capacity performance for mixed RF-FSO relaying schemes under RF and FSO eavesdropper attacks, respectively. To justify the problem, we consider two general fading models, Nakagami-*m* at the RF side and exponentiated Weibull distribution at the FSO side. The results, which are validated with the Monte-Carlo simulations, show that both the location and the size of the photo-aperture is very important in the design of RF-FSO relay networks to enhance the secrecy performance of the overall system.**

***Index Terms*—Physical layer security, mixed RF-FSO relaying, RF and FSO eavesdropping.**

I. Introduction

DUE to the explosive growth of wireless systems and devices, spectrum scarcity has become an important problem in wireless communications. To meet the demand for reliable and ubiquitous communications, new technologies have been emerged most recently. Among them, free-space optical (FSO) communication has attracted much interest from the academia and industry as it can solve the last mile problem in wireless networks, while enabling fast, reliable and secure communication between two stationary points by using the unlicensed optical spectrum [1]. On account of this potential, FSO systems are planning to be used in video surveillance, security, broadcasting, and campus connectivity in the next generation wireless communication systems [2].

Even though FSO systems can bring numerous advantages, the turbulence-induced fading due to bad weather conditions, including rain, snow, fog, and wind can cause destructive effects on FSO communication. To overcome these adverse effects and to improve the coverage and reliability, mixed radio frequency (RF)-FSO systems were proposed [3]. In mixed RF-FSO communication, RF and FSO systems are used in a dual-hop configuration with the aid of decode-and-forward (DF) and amplify-and-forward (AF) relaying techniques [4]. Based on these observations, mixed RF-FSO transmission can be a powerful alternative for the spectrum scarcity problem in wireless systems as it can reap all the advantages of FSO communication while coping with the turbulence-induced fading. Hence, mixed RF-FSO systems have been considerably investigated in the literature, e.g., in [5]–[12] and the references therein.

Another critical problem in wireless communications is the confidentiality of the information as wireless systems are prone to security threats due to their inherent nature [13]. So far, wireless communication security has been provided with the aid of various encryption/decryption methods, which are performed at the upper layers of the protocol stack [14]. A recent complementary or even an alternative technology, physical layer security, addresses the security problem in the physical layer by using the randomness and time-varying nature of the wireless systems. Physical layer security, which was pioneered by Wyner in [15], can be accomplished as long as the main channel is superior to the wire-tap channel. In physical layer security, the eavesdropper can be a legitimate member of the network that can overhear the communication, or an illegitimate malicious user that has the intention of listening to the communication. Two important secrecy performance metrics, the secrecy outage probability (SOP), and the probability of positive secrecy capacity (PPSC) have been proposed based on the Wyner's model [16], [17].

In the literature, physical layer security has been introduced into mixed RF-FSO systems most recently. Specifically, [18]–[23] considered a mixed RF-FSO relaying scheme in the presence of an RF eavesdropper, which tackles the information from the source node, whereas [24] focuses on the RF eavesdropping

Manuscript received September 17, 2021; revised October 27, 2021; accepted November 9, 2021. Date of publication November 11, 2021; date of current version November 25, 2021. *(Corresponding author: Eylem Erdogan.)*

Eylem Erdogan is with the Department of Electrical and Electronics Engineering, Istanbul Medeniyet University, Goztepe, Istanbul 34720, Turkey (e-mail: erdoganeyl@gmail.com).

Ibrahim Altunbas is with the Electronics and Communications Engineering, Istanbul Technical University, Maslak, Istanbul 34467, Turkey (e-mail: ibraltunbas@itu.edu.tr).

Gunes Karabulut Kurt is with the Department of Electrical Engineering, Polytechnique Montreal, Montreal, QC H3T 1J4, Canada (e-mail: gunes.kurt@polymtl.ca).

Halim Yanikomeroglu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: halim@sce.carleton.ca).

Digital Object Identifier 10.1109/JPHOT.2021.3127397

from the relay node on a dual-hop mixed FSO-RF configuration. Different than RF eavesdropping, in its FSO counterpart, the information can be collected by an unfriendly observer that is positioned close to the receiver photo-aperture [25]. Owing to this, Wyner's model has been implemented into a mixed RF-FSO relaying network[1], where an FSO eavesdropper is intercepting the information from the relay terminal in [26].

As the aforementioned studies show, the current literature is generally focused on the RF eavesdropping from the source node in dual-hop mixed RF-FSO configuration, and almost all the existing works have focused on the Gamma-Gamma distribution at the FSO path, which can be used for some specific aperture sizes. Different from the current literature, in this study, we focus on RF and FSO eavesdropping attacks from the relay terminal [27], which can be considered as untrusted due to its security gaps [28], [29]. To do so, RF and FSO eavesdropper attacks are demonstrated by using mixed FSO-RF and RF-FSO relaying configurations. Furthermore, considering that Nakagami-*m* distribution can be suitable for various RF environments and owing to the fact that Exponentiated Weibull (EW) fading can be used to model different atmospheric turbulence levels along with various aperture sizes [30], [31], we provide a general framework about RF and FSO eavesdropping for mixed RF-FSO relay networks. Specifically, the paper makes the following contributions:

- Unlike previous works, which mainly focus on the RF eavesdropping for mixed RF-FSO relaying, we introduce a general physical layer security framework for dual-hop mixed RF-FSO relay networks by considering both RF and FSO eavesdropper attacks. The introduced framework answers three critical design problems: 1) How can we improve the confidentiality of the optical information? 2) What is the impact of the photo-aperture size on the performance of secure FSO communication? 3) What is the impact of the Nakagami-*m* parameter on the RF eavesdropping?
- To quantify the performance of the RF and FSO eavesdropper attacks, we first obtain the instantaneous signal-to-noise ratio (SNR). Thereafter, the first time in the literature, we derive new SOP and PPSC expressions for Nakagami-*m*/EW fading channels.
- In the last part of this work, we provide insightful remarks to shed light into the design of secure mixed RF-FSO relay networks. These results show that the receiver aperture size, Nakagami-*m* fading parameter, and the weather conditions are of utmost importance in the design of secure mixed RF-FSO and FSO-RF communications. Specifically, keeping the photo aperture size around 200mm and choosing a higher ground for the relay node[2] can provide 10^{-6} SOP performance for the proposed network even in harsh weather conditions.

[1]Note that, RF and FSO eavesdropping attacks through the relay terminal can be implemented by using mixed FSO-RF and mixed RF-FSO relay networks, respectively as can be seen from the aforementioned studies.

[2]Increasing the height of the relay node can decrease the turbulence induced fading, and weak turbulence regimes can be established based on the refractive index structure parameter models [32].

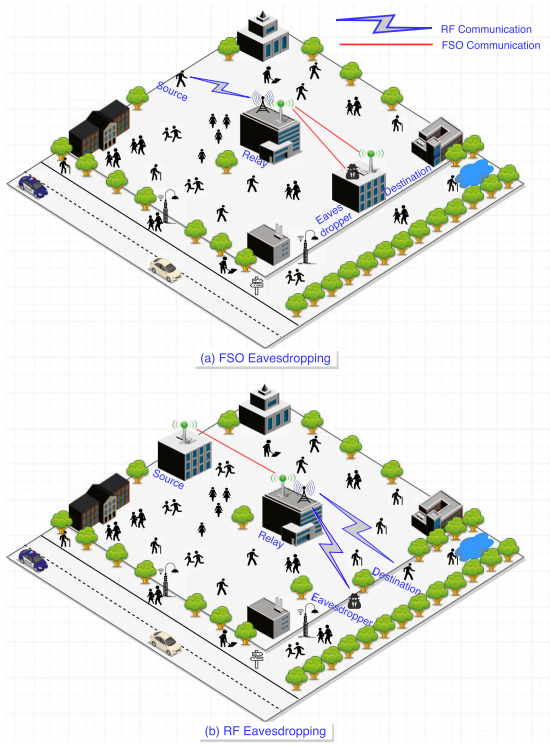

Fig. 1. Illustration of the HAPS-aided laser inter-satellite communication model.

The remainder of the paper is organized as follows: In Section II, the signal and system models are presented for RF and FSO eavesdropping. In Section III, SOP and PPSC analysis are pursued for Nakagami-*m*/EW fading channels. Our numerical results and some crucial remarks are provided in Section IV, and Section V concludes the paper.

II. Signal and System Model

A. System Model

In this section, we consider dual-hop mixed RF-FSO relaying configurations where source node S wishes to send confidential information to the legitimate destination node D over a DF relay terminal R, which is equipped with a single antenna from one side and a single photo-aperture on the other side in the presence of an eavesdropper node E, which is attempting to tackle the classified information from R as it may not be trustable due to its simple structure. In this architecture, we focus on RF and FSO eavesdropper attacks by considering mixed FSO-RF and mixed RF-FSO relaying schemes, respectively as demonstrated in Fig. 1.

1) FSO Eavesdropping: We consider a mixed RF-FSO relaying scheme, where an FSO eavesdropper located very close to D, is trying to intercept the information of R as depicted in Fig. 1(a). In this network, the RF information is transmitted to R through a single transmit antenna in the first phase of communication. In the second phase of the communication, receive antenna at R collects the source information and filters out the DC components. Then, R detects the source signal,

modulates it with binary phase shift keying and forwards to D with proper biasing. In this scenario, E, that is positioned at a close proximity to the receiver aperture, can intercept the information from the laser beam,[3] when the beam is reflected by aerosols and gases [25]. In this structure, the received signals at R and D can be expressed as

$$y_R = \sqrt{P_S} h_{SR} x_S + n_R, \tag{1}$$

and

$$y_D = \sqrt{\zeta_1 P_R} I_{RD} \tilde{x}_S + n_D, \tag{2}$$

where P_S and P_R are the source and relay transmit powers respectively, x_S and $\tilde{x}_S$ are the source information and detected source information respectively. n_R and n_D[4] are the additive white Gaussian noises with N_0 one-sided power spectral density, h_{SR} and I_{RD} denote RF and FSO channel coefficients respectively[5], and ζ_1 denotes the electrical-to-optical conversion coefficient.

2) RF Eavesdropping: In a mixed FSO-RF communication model, which is shown in Fig. 1(b), the electrical signal is converted into an optical signal by adding a DC bias, ensuring that it is positive. Then the optical signal is transmitted to the optical aperture of the R. R first filters out the DC component, converts the optical signal into electrical and forwards to D. In this architecture, E targets to decode and obtain the secret data content from R [33]. After two transmission phases, the received signals at R and D can respectively be expressed as [34]

$$y_R = \sqrt{\zeta_2 P_S} x_S I_{SR} + n_R, \tag{3}$$

and

$$y_D = \sqrt{P_R} \tilde{x}_S h_{RD} + n_D, \tag{4}$$

where I_{SR} is the FSO channel coefficient, h_{RD} shows the RF channel coefficient, and ζ_2 is the optical-to-electrical coefficient. For computational simplicity, electrical-to-optical and optical-to-electrical conversion parameters are set as $\zeta_1 = \zeta_2 = 1$. Following the above-mentioned assumption and with the aid of (1)–(4), the overall SNR for mixed RF-FSO and FSO-RF DF relaying schemes can be expressed as [19]

$$\gamma_o = \begin{cases} \min\left(\gamma_{SR}^{\text{RF}}, \gamma_{RD}^{\text{FSO}}\right), & \text{FSO eavesdropping} \\ \min\left(\gamma_{SR}^{\text{FSO}}, \gamma_{RD}^{\text{RF}}\right), & \text{RF eavesdropping,} \end{cases} \tag{5}$$

where $\gamma_{SR}^{\text{RF}} = \frac{P_S}{N_0}|h_{SR}|^2$, $\gamma_{RD}^{\text{FSO}} = \frac{P_R}{N_0} I_{RD}^2$, $\gamma_{SR}^{\text{FSO}} = \frac{P_S}{N_0} I_{SR}^2$ and $\gamma_{RD}^{\text{RF}} = \frac{P_R}{N_0}|h_{RD}|^2$. In addition, the SNR at E can be expressed as

$$\gamma_E = \begin{cases} \frac{P_R}{N_0} I_{RE}^2, & \text{FSO eavesdropping} \\ \frac{P_R}{N_0}|h_{RE}|^2, & \text{RF eavesdropping,} \end{cases} \tag{6}$$

where I_{RE} and h_{RE} are the FSO and RF eavesdropper channel coefficients respectively.

[3]The interception of the FSO information can arise in harsh weather conditions, including snow, heavy rain and fog, when the beam is heavily refracted, reflected and scattered.

[4]Even though shot noise can be affective in FSO links, we assume that only thermal noise is dominant in the RF and FSO communications.

[5]Throughout the paper, all RF channel coefficients are modeled as complex, and FSO channel coefficients are modeled as real.

B. Channel Models

It is important to mention that Nakagami-*m* distribution is a general fading model that matches empirical data better than Rayleigh fading in many RF communication scenarios. Owing to that fact, in this paper, the RF channel h_z, $z \in \{SR, RD, E\}$ is assumed to follow Nakagami-*m* fading with integer-valued fading severity parameter m_z. Thereby, the cumulative distribution function (CDF) of γ_z^{RF} can be expressed as [35, eqn. (8.352.6)]

$$\begin{aligned} F_{\gamma_z}^{\text{RF}} &= 1 - \frac{\Gamma\left(m_z, \frac{m_z \gamma}{\bar{\gamma}_z^{\text{RF}}}\right)}{\Gamma(m_z)}, \\ &= 1 - \exp\left[-\frac{m_z \gamma}{\bar{\gamma}_z^{\text{RF}}}\right] \sum_{t=0}^{m_z - 1} \left(\frac{m_z \gamma}{\bar{\gamma}_z^{\text{RF}}}\right)^t \frac{1}{t!}, \end{aligned} \tag{7}$$

where $\Gamma(a, x)$ denotes the lower incomplete Gamma function [35, eqn. (8.350.1)], $\Gamma(x)$ is the Gamma function as described in [35, eqn. (8.310.1)], $\bar{\gamma}_z^{\text{RF}} = \frac{P_k}{N_0}\mathbb{E}\{|h_z|^2\}$, $k \in \{S, R\}$ is the average SNR of the RF link and $\mathbb{E}\{\cdot\}$ is the expectation operation.

The FSO fading I_z, on the other hand, experiences EW distribution model whose CDF of SNR is given by [30]

$$F_{\gamma_z^{\text{FSO}}}(\gamma) = \left(1 - \exp\left[-\left(\frac{\gamma}{\eta_z^2 \bar{\gamma}_z^{\text{FSO}}}\right)^{\beta_z/2}\right]\right)^{\alpha_z}, \tag{8}$$

where α_z, β_z are the shape parameters, η_z is the scale parameter and $\bar{\gamma}_z^{\text{FSO}} = \frac{P_k}{N_0}\mathbb{E}\{I_z^2\}$ is the the average SNR of the FSO path. The above expression can be expressed more tractable as [36, eqn. (10)]

$$F_{\gamma_z^{\text{FSO}}}(\gamma) = \sum_{\rho=0}^{\infty} \binom{\alpha_z}{\rho} (-1)^\rho \exp\left[-\rho\left(\frac{\gamma}{\eta_z^2 \bar{\gamma}_z^{\text{FSO}}}\right)^{\frac{\beta_z}{2}}\right]. \tag{9}$$

III. Secrecy Performance Analysis

This section derives new SOP and PPSC expressions by considering RF and FSO eavesdropper attacks.

A. Secrecy Outage Probability Analysis

In physical layer security, E can be considered as an illegitimate malicious user that has the intention of listening to the communication. In such scenarios, S has to transmit the information at a constant achievable secrecy rate R_s satisfying that $C_s > R_s$, where C_s stands for the secrecy capacity, which can be defined as

$$C_s = \begin{cases} \frac{1}{2}\log_2(1 + \gamma_o) - \frac{1}{2}\log_2(1 + \gamma_E), & \gamma_o > \gamma_E \\ 0, & \text{otherwise,} \end{cases} \tag{10}$$

and the SOP can be expressed as [19]

$$\begin{aligned} P_{\text{SO}} &= \Pr[C_s < R_s], \\ &= \int_0^\infty F_{\gamma_o}(\gamma\gamma_{th} + \gamma_{th} - 1) f_{\gamma_E}(\gamma) d\gamma, \\ &\approx \int_0^\infty F_{\gamma_o}(\gamma\gamma_{th}) f_{\gamma_E}(\gamma) d\gamma, \end{aligned} \tag{11}$$

where $\gamma_{th} = 2^{2R_s}$. It is important to note that the third line in (11) can provide a tight lower bound SOP expression.

1) FSO Eavedropping: In this scenario, mixed RF-FSO relaying is taken into consideration in the presence of an FSO eavesdropper. For this network, the CDF of overall SNR can be expressed as

$$\begin{aligned} F_{\gamma_o}(\gamma) &= 1 - \Pr[\gamma_{SR}^{\text{RF}} > \gamma] \Pr[\gamma_{RD}^{\text{FSO}} > \gamma] \\ &= 1 - (1 - F_{\gamma_{SR}^{\text{RF}}}(\gamma))(1 - F_{\gamma_{RD}^{\text{FSO}}}(\gamma)). \end{aligned} \tag{12}$$

$F_{\gamma_o}(\gamma)$ can be obtained by substituting (7) and (9) into (12) as

$$\begin{aligned} F_{\gamma_o}(\gamma) = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{\rho=1}^{\infty} \binom{\alpha_{RD}}{\rho} (-1)^{\rho+1} \left(\frac{1}{k!}\right) \left(\frac{m_{SR}\gamma}{\bar{\gamma}_{SR}}\right)^k \\ \times \exp\left[-\frac{m_{SR}\gamma}{\bar{\gamma}_{SR}}\right] \exp\left[-\rho\left(\frac{\gamma}{\eta_{RD}^2 \bar{\gamma}_{RD}}\right)^{\frac{\beta_{RD}}{2}}\right], \end{aligned} \tag{13}$$

and the probability density function (PDF) of γ_E can be obtained by taking the derivative of (8) with respect to γ as

$$\begin{aligned} f_{\gamma_E}(\gamma) = \frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2}-1}}{2(\eta_E^2 \bar{\gamma}_E)^{\frac{\beta_E}{2}}} \left(1 - \exp\left[-\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]\right)^{\alpha_E - 1} \\ \times \exp\left[-\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]. \end{aligned} \tag{14}$$

By using the Binomial expansion, the above expression can be written in a more tractable form as

$$\begin{aligned} f_{\gamma_E}(\gamma) = \frac{\alpha_E \beta_E \gamma^{\frac{\beta_E}{2}-1}}{2(\eta_E^2 \bar{\gamma}_E)^{\frac{\beta_E}{2}}} \sum_{t=0}^{\infty} \binom{\alpha_E - 1}{t} (-1)^t \\ \times \exp\left[-(t+1)\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right]. \end{aligned} \tag{15}$$

Then, by substituting $f_{\gamma_E}(\gamma)$ and $F_{\gamma_o}(\gamma)$ into (11), SOP can be written as

$$\begin{aligned} P_{\text{SO}} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{\rho=1}^{\infty} \sum_{t=0}^{\infty} \binom{\alpha_{RD}}{\rho} \binom{\alpha_E - 1}{t} (-1)^{t+\rho+1} \left(\frac{1}{k!}\right) \\ \times \left(\frac{m_{SR}}{\bar{\gamma}_{SR}}\right)^k \left(\frac{\alpha_E \beta_E}{2(\eta_E^2 \bar{\gamma}_E)^{\frac{\beta_E}{2}}}\right) \int_0^{\infty} (\gamma\gamma_{th})^k \gamma^{\frac{\beta_E}{2}-1} \\ \times \exp\left[-\frac{m_{SR}\gamma\gamma_{th}}{\bar{\gamma}_{SR}}\right] \exp\left[-(t+1)\left(\frac{\gamma}{\eta_E^2 \bar{\gamma}_E}\right)^{\frac{\beta_E}{2}}\right] \\ \times \exp\left[-\rho\left(\frac{\gamma\gamma_{th}}{\eta_{RD}^2 \bar{\gamma}_{RD}}\right)^{\frac{\beta_{RD}}{2}}\right] d\gamma. \end{aligned} \tag{16}$$

To the best of our knowledge, the above integral can not be calculated in a closed-form. However, in optical eavesdropping, the eavesdropper should be located very close to the receiver photo-aperture to collect the reflected information due to aerosols or gases. In this case, the eavesdropper can experience very similar turbulence conditions with the destination. Hence, the shape parameter β and the scale parameter η, which depends on β in EW fading, can be assumed as $\beta_E = \beta_{RD} = \beta$ and $\eta_E = \eta_{RD} = \eta$. Based on this assumption, the above integral expression can be written as

$$\begin{aligned} P_{\text{SO}} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{\rho=1}^{\infty} \sum_{t=0}^{\infty} \binom{\alpha_{RD}}{\rho} \binom{\alpha_E - 1}{t} (-1)^{t+\rho+1} \left(\frac{1}{k!}\right) \\ \times \left(\frac{m_{SR}\gamma_{th}}{\bar{\gamma}_{SR}}\right)^k \left(\frac{\alpha_E \beta}{2(\eta^2 \bar{\gamma}_E)^{\frac{\beta}{2}}}\right) \int_0^{\infty} \gamma^{k+\frac{\beta}{2}-1} \exp\left[-\frac{m_{SR}\gamma\gamma_{th}}{\bar{\gamma}_{SR}}\right] \\ \times \exp\left[-\gamma^{\frac{\beta}{2}}\left\{(t+1)\left(\frac{1}{\eta^2 \bar{\gamma}_E}\right)^{\frac{\beta}{2}} + \rho\left(\frac{\gamma_{th}}{\eta^2 \bar{\gamma}_{RD}}\right)^{\frac{\beta}{2}}\right\}\right] d\gamma. \end{aligned} \tag{17}$$

By invoking $\exp\left[-\frac{m_{SR}\gamma\gamma_{th}}{\bar{\gamma}_{SR}}\right] = G_{0,1}^{1,0}\left[\frac{m_{SR}\gamma\gamma_{th}}{\bar{\gamma}_{SR}} \middle| \begin{matrix} - \\ 0 \end{matrix}\right]$ into (17), then by changing the variables in the above integration as $x = \gamma^{\frac{\beta}{2}}\left\{(t+1)\underbrace{\left(\frac{1}{\eta^2 \bar{\gamma}_E}\right)^{\frac{\beta}{2}}}_{\varphi} + \rho\underbrace{\left(\frac{\gamma_{th}}{\eta^2 \bar{\gamma}_{RD}}\right)^{\frac{\beta}{2}}}_{\psi}\right\}$, P_{SO} can be expressed as

$$\begin{aligned} P_{\text{SO}} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{\rho=1}^{\infty} \sum_{t=0}^{\infty} \binom{\alpha_{RD}}{\rho} \binom{\alpha_E - 1}{t} (-1)^{t+\rho+1} \left(\frac{1}{k!}\right) \\ \times \left(\frac{m_{SR}\gamma_{th}}{\bar{\gamma}_{SR}}\right)^k \left(\frac{\alpha_E}{(\eta^2 \bar{\gamma}_E)^{\frac{\beta}{2}}}\right) \left(\frac{1}{(t+1)\varphi + \rho\psi}\right)^{\frac{2}{\beta}k+1} \int_0^{\infty} x^{\frac{2}{\beta}k} \\ \times G_{0,1}^{1,0}\left[\left(\frac{m_{SR}\gamma_{th}}{((t+1)\varphi + \rho\psi)^{\frac{2}{\beta}} \bar{\gamma}_{SR}}\right) x^{\frac{2}{\beta}} \middle| \begin{matrix} - \\ 0 \end{matrix}\right] G_{0,1}^{1,0}\left[x \middle| \begin{matrix} - \\ 0 \end{matrix}\right] dx, \end{aligned} \tag{18}$$

where $G_{p,q}^{m,n}\left[\cdot \middle| \begin{matrix} \cdot \\ \cdot \end{matrix}\right]$ denotes the Meijer-G function [37, eqn. (07.34.02.0001.01)]. Then, with the aid of [37, eqn. (07.34.21.0012.01)], the solution of the above expression can be obtained as

$$\begin{aligned} P_{\text{SO}} = 1 - \sum_{k=0}^{m_{SR}-1} \sum_{\rho=1}^{\infty} \sum_{t=0}^{\infty} \binom{\alpha_{RD}}{\rho} \binom{\alpha_E - 1}{t} (-1)^{t+\rho+1} \left(\frac{1}{k!}\right) \\ \times \left(\frac{m_{SR}\gamma_{th}}{\bar{\gamma}_{SR}}\right)^k \left(\frac{\alpha_E}{(\eta^2 \bar{\gamma}_E)^{\frac{\beta}{2}}}\right) \left(\frac{1}{(t+1)\varphi + \rho\psi}\right)^{\frac{2}{\beta}k+1} \\ \times H_{1,1}^{1,1}\left[\left(\frac{m_{SR}\gamma_{th}}{((t+1)\varphi + \rho\psi)^{\frac{2}{\beta}} \bar{\gamma}_{SR}}\right) \middle| \begin{matrix} \left(-\frac{2}{\beta}k, \frac{2}{\beta}\right) \\ (0,1) \end{matrix}\right], \end{aligned} \tag{19}$$

where $H_{p,q}^{m,n}\left[\cdot \middle| \begin{matrix} (\cdot,\cdot) \\ (\cdot,\cdot) \end{matrix}\right]$ denotes the Fox H-function [38].

2) RF Eavesdropping: In this scenario, mixed FSO-RF relaying is considered where the eavesdropper is trying to steal

the information from the relay terminal over the RF path. In this architecture, the CDF of γ_o can be expressed as

$$F_{\gamma_o}(\gamma) = 1 - (1 - F_{\gamma_{SR}^{\text{FSO}}}(\gamma))(1 - F_{\gamma_{RD}^{\text{RF}}}(\gamma)), \quad (20)$$

and $F_{\gamma_o}(\gamma)$ can be obtained with the aid of (7) and (9) as

$$F_{\gamma_o}(\gamma) = 1 - \sum_{\rho=1}^{\infty} \sum_{k=0}^{m_{RD}-1} \binom{\alpha_{SR}}{\rho} (-1)^{\rho+1} \left(\frac{m_{RD}\gamma}{\bar{\gamma}_{RD}}\right)^k \frac{1}{k!} \times \exp\left[-\rho\left(\frac{\gamma}{\eta_{SR}^2 \bar{\gamma}_{SR}}\right)^{\frac{\beta_{SR}}{2}}\right] \exp\left[-\frac{m_{RD}\gamma}{\bar{\gamma}_{RD}}\right]. \quad (21)$$

The PDF of γ_E can be expressed by taking the derivative of (7) as

$$f_{\gamma_E}(\gamma) = \left(\frac{m_E}{\bar{\gamma}_E}\right)^{m_E} \frac{\gamma^{m_E-1}}{\Gamma(m_E)} \exp\left[-\frac{m_E\gamma}{\bar{\gamma}_E}\right]. \quad (22)$$

By substituting (22) and (21) into (11), SOP can expressed as

$$P_{\text{SO}} = 1 - \sum_{\rho=1}^{\infty} \sum_{k=0}^{m_{RD}-1} \binom{\alpha_{SR}}{\rho} (-1)^{\rho+1} \left(\frac{\gamma_{th} m_{RD}}{\bar{\gamma}_{RD}}\right)^k \frac{1}{k!} \left(\frac{m_E}{\bar{\gamma}_E}\right)^{m_E} \times \frac{1}{\Gamma(m_E)} \int_0^{\infty} \gamma^{k+m_E-1} \exp\left[-\rho\left(\frac{\gamma\gamma_{th}}{\eta_{SR}^2 \bar{\gamma}_{SR}}\right)^{\frac{\beta_{SR}}{2}}\right] \times \exp\left[-\gamma \underbrace{\left(\frac{m_{RD}\gamma_{th}}{\bar{\gamma}_{RD}} + \frac{m_E}{\bar{\gamma}_E}\right)}_{\zeta}\right] d\gamma. \quad (23)$$

Thereafter, by applying the identity of $\exp\left[-\zeta\gamma\right] = G_{0,1}^{1,0}\left[\zeta\gamma \left| \begin{matrix} - \\ 0 \end{matrix}\right.\right]$ into (23), and after changing the variables as $x = \rho\left(\frac{\gamma}{\eta_{SR}^2 \bar{\gamma}_{SR}}\right)^{\frac{\beta_{SR}}{2}}$, the above expression can be written as

$$P_{\text{SO}} = 1 - \sum_{\rho=1}^{\infty} \sum_{k=0}^{m_{RD}-1} \binom{\alpha_{SR}}{\rho} (-1)^{\rho+1} \left(\frac{\gamma_{th} m_{RD}}{\bar{\gamma}_{RD}}\right)^k \frac{1}{k!} \left(\frac{m_E}{\bar{\gamma}_E}\right)^{m_E} \times \frac{1}{\Gamma(m_E)} \left(\frac{2}{\beta_{SR}}\right) \left(\frac{\eta_{SR}^2 \bar{\gamma}_{SR}}{\gamma_{th}\rho^{2/\beta_{SR}}}\right)^{k+m_E} \int_0^{\infty} x^{\frac{2}{\beta_{SR}}(k+m_E)-1} \times G_{0,1}^{1,0}\left[\left(\frac{\zeta\eta_{SR}^2 \bar{\gamma}_{SR}}{\gamma_{th}\rho^{2/\beta_{SR}}}\right) x^{\frac{2}{\beta_{SR}}} \left| \begin{matrix} - \\ 0 \end{matrix}\right.\right] G_{0,1}^{1,0}\left[x \left| \begin{matrix} - \\ 0 \end{matrix}\right.\right] dx, \quad (24)$$

and with the aid of [37, eqn. (07.34.21.0012.01)], a SOP expression can be obtained as

$$P_{\text{SO}} = 1 - \sum_{\rho=1}^{\infty} \sum_{k=0}^{m_{RD}-1} \binom{\alpha_{SR}}{\rho} (-1)^{\rho+1} \left(\frac{\gamma_{th} m_{RD}}{\bar{\gamma}_{RD}}\right)^k \frac{1}{k!} \left(\frac{m_E}{\bar{\gamma}_E}\right)^{m_E} \times \frac{1}{\Gamma(m_E)} \left(\frac{2}{\beta_{SR}}\right) \left(\frac{\eta_{SR}^2 \bar{\gamma}_{SR}}{\gamma_{th}\rho^{2/\beta_{SR}}}\right)^{k+m_E} \times H_{1,1}^{1,1}\left[\left(\frac{\zeta\eta_{SR}^2 \bar{\gamma}_{SR}}{\gamma_{th}\rho^{2/\beta_{SR}}}\right) \left| \begin{matrix} \left(1 - \frac{2}{\beta_{SR}}(k+m_E), \frac{2}{\beta_{SR}}\right) \\ (0,1) \end{matrix}\right.\right]. \quad (25)$$

B. Probability of Positive Secrecy Capacity Analysis

To quantify the PPSC performance of the proposed network, we assume that E is a licensed user in the system which has a bad intention of eavesdropping the communication between R and D. In that case, S has the information of E and to provide information theoretic security, it has to satisfy $C_s > 0$. Mathematically speaking, PPSC can be defined as

$$P_{\text{PPSC}} = \Pr[C_s > 0] = \Pr\left[\frac{1}{2}\log_2(1+\gamma_o) > \frac{1}{2}\log_2(1+\gamma_E)\right], \quad (26)$$

After a few manipulations, it can be written as [39]

$$P_{\text{PPSC}} = 1 - \int_0^{\infty} F_{\gamma_o}(\gamma) f_{\gamma_E}(\gamma) d\gamma \quad (27)$$

For FSO and RF eavesdropping schemes, PPSC can be obtained very similar to (19) and (25) respectively, as

$$P_{\text{PPSC}} = \sum_{k=0}^{m-1} \sum_{\rho=1}^{\infty} \sum_{t=0}^{\infty} \binom{\alpha_{RD}}{\rho} \binom{\alpha_E - 1}{t} (-1)^{t+\rho+1} \left(\frac{1}{k!}\right) \times \left(\frac{m_{SR}}{\bar{\gamma}_{SR}}\right)^k \left(\frac{\alpha_E}{(\eta^2\bar{\gamma}_E)^{\frac{\beta}{2}}}\right) \left(\frac{1}{(t+1)\varphi + \rho\psi}\right)^{\frac{2}{\beta}k+1} \times H_{1,1}^{1,1}\left[\left(\frac{m_{SR}}{((t+1)\varphi + \rho\psi)^{\frac{2}{\beta}} \bar{\gamma}_{SR}}\right) \left| \begin{matrix} \left(-\frac{2}{\beta}k, \frac{2}{\beta}\right) \\ (0,1) \end{matrix}\right.\right], \quad (28)$$

and

$$P_{\text{PPSC}} = \sum_{\rho=1}^{\infty} \sum_{k=0}^{m_{RD}-1} \binom{\alpha_{SR}}{\rho} (-1)^{\rho+1} \left(\frac{m_{RD}}{\bar{\gamma}_{RD}}\right)^k \frac{1}{k!} \left(\frac{m_E}{\bar{\gamma}_E}\right)^{m_E} \times \frac{1}{\Gamma(m_E)} \left(\frac{2}{\beta_{SR}}\right) \left(\frac{\eta_{SR}^2 \bar{\gamma}_{RD}}{\rho^{2/\beta_{SR}}}\right)^{k+m_E} \times H_{1,1}^{1,1}\left[\left(\frac{\zeta\eta_{SR}^2 \bar{\gamma}_{SR}}{\rho^{2/\beta_{SR}}}\right) \left| \begin{matrix} \left(1 - \frac{2}{\beta_{SR}}(k+m_E), \frac{2}{\beta_{SR}}\right) \\ (0,1) \end{matrix}\right.\right]. \quad (29)$$

Even though the Fox-H function given in (19), (25), (28) and (29) is not an elementary function, it can be evaluated by using well-known software programs like MATHEMATICA as described in [40, Appen. 1]. Furthermore, the infinite series in the SOP and PPSC expressions converges very fast, so that, SOP and PPSC expressions can be obtained by using 5 to 10 terms with a convergence error on the order of 10^{-7}.

IV. Numerical Results

In this section, the theoretical findings are validated with the aid of Monte-Carlo simulations. Furthermore, RF and FSO

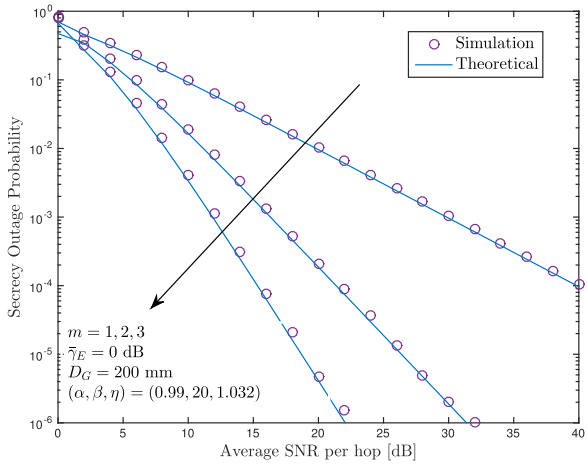

Fig. 2. SOP performance of the mixed RF-FSO relaying scheme for various m parameters when $D_G = 200$ mm.

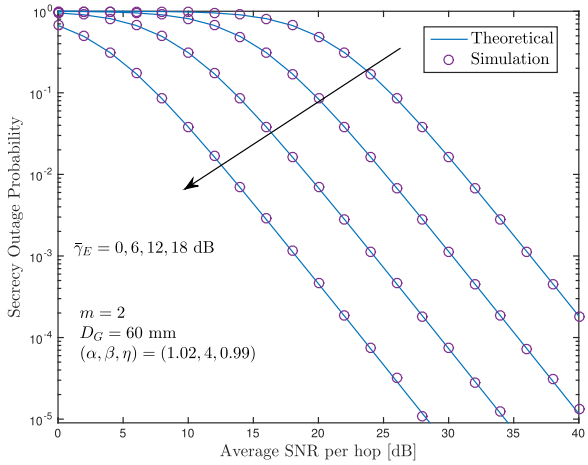

Fig. 3. SOP performance of the mixed FSO-RF relay network for various $\bar{\gamma}_E$ values when $D_G = 60$ mm.

eavesdropper attacks are compared in terms of SOP and PPSC, and important design guidelines are presented. For the sake of a fair comparison, the parameters utilized in the numerical results are set to $\alpha_{SR} = \alpha_{RD} = \alpha_E = \alpha$, $\beta_{SR} = \beta_{RD} = \beta_E = \beta$, $\eta_{SR} = \eta_{RD} = \eta_E = \eta$, $m_{SR} = m_{RD} = m_E = m$, and $R_s = 0.01$ bit/sn/Hz. The optical wavelength is chosen as 780nm and $D_G = 60, 100$ and 200mm receiver aperture sizes are used to demonstrate the performance of the FSO communication [41]. In addition, similar to the related works, the average SNRs at both hops satisfy $\bar{\gamma}_{SR} = \bar{\gamma}_{RD} = \bar{\gamma}$ as given in the x-axis of the figures.

In the first part of this section, the theoretical results are validated with the aid of simulations[6]. The first two figures, Fig. 2 and 3, show the SOP performance of FSO and RF eavesdropper attacks respectively. As observed from both figures, the theoretical results are in good agreement with the marker symbols which are generated through Monte-Carlo simulations.

[6]Herein, we omit verifying the PPSC expressions through Monte-Carlo simulations, as they can be easily validated through SOP expressions. (Please see (27) and (11).

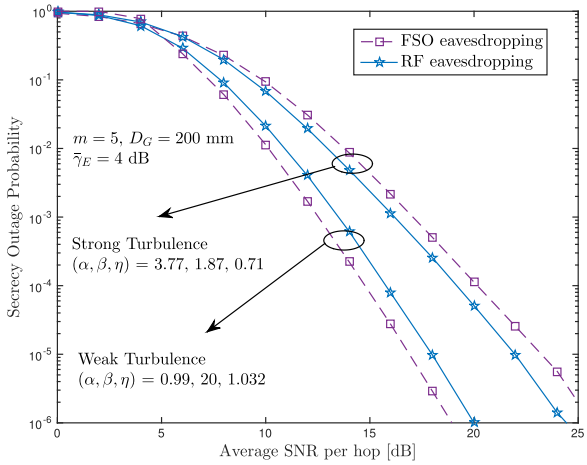

Fig. 4. Comparison of RF and FSO eavesdropper attacks for different turbulence conditions when $\bar{\gamma}_E = 4$ dB and $m = 5$.

In addition, Fig. 2 shows that the SOP performance of the mixed RF-FSO relaying scheme outperforms when the level of RF fading decreases as Nakagami-*m* parameter increases from $m = 1$ to $m = 3$. This means that the SOP performance of the proposed scenario enhances when the amount of fading is low. Fig. 3 on the other hand, illustrates that the SOP performance decreases monotonically as the impact of eavesdropper increases due to higher $\bar{\gamma}_E$.

A. Comparison of RF and FSO Eavesdropper Attacks

Next, we compare the RF and FSO eavesdropper attacks in terms of SOP and PPSC. In Fig. 4, the RF and FSO eavesdropper attacks are compared for different FSO turbulence levels. It is observed from the figure that, at strong turbulence levels, the FSO eavesdropping achieves worse SOP performance than RF eavesdropping as the eavesdropper can collect the optical information easily in strong turbulence conditions. In contrast, and as expected, FSO eavesdropping achieves a better SOP performances in weak turbulence levels due to low reflection and scattering effects.

Fig. 5 illustrates the SOP performance of RF and FSO eavesdropping at different Nakagami-*m* fading parameters. As observed from the figure, increasing the fading parameter of the RF communication does not enhance the overall SOP performance. By contrast, as we assume $m_{SR} = m_{RD} = m_E = m$, the gap between RF and FSO eavesdropping is increasing as m_E increases.

In Fig. 6, RF and FSO eavesdropper attacks are compared for two different receiver aperture sizes at moderate turbulence conditions. As observed from the figure, when the aperture size is $D_G = 100$ mm, mixed RF-FSO relaying scheme achieves worse SOP performance than mixed FSO-RF relaying as lower aperture diameter gives a better chance for eavesdropper to capture the signal. By contrast, at $D_G = 200$ mm, mixed RF-FSO relaying performs average 1dB better SOP performance. It is noteworthy to mention that, increasing the receiver aperture enhances the SOP performance of the mixed RF-FSO relaying.

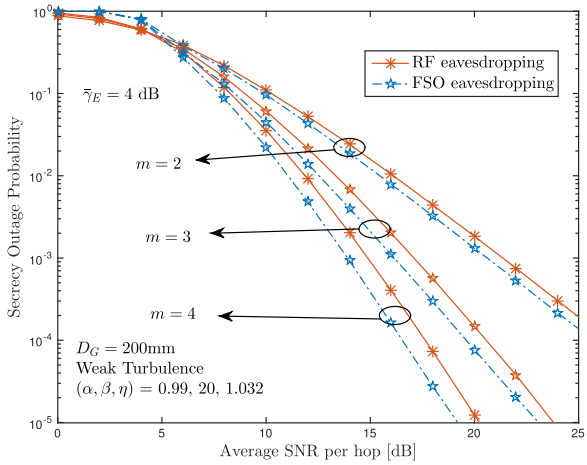

Fig. 5. Comparison of RF and FSO eavesdropper attacks for different fading severity parameters when $\bar{\gamma}_E = 4$ dB and $D_G = 100$ mm.

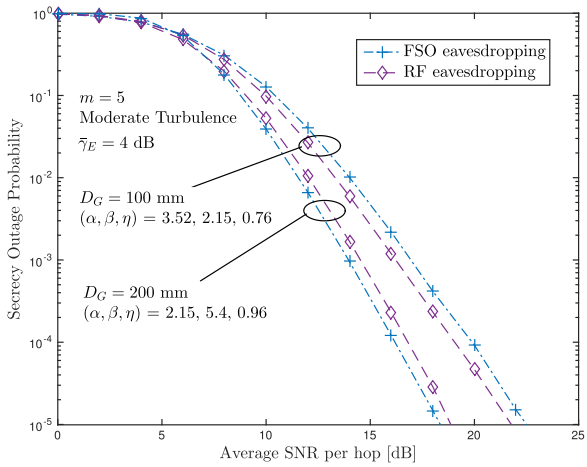

Fig. 6. Comparison of RF and FSO eavesdropper attacks for different receiver photo-aperture sizes under moderate turbulence conditions, when $\bar{\gamma}_E = 4$ dB and $m = 5$.

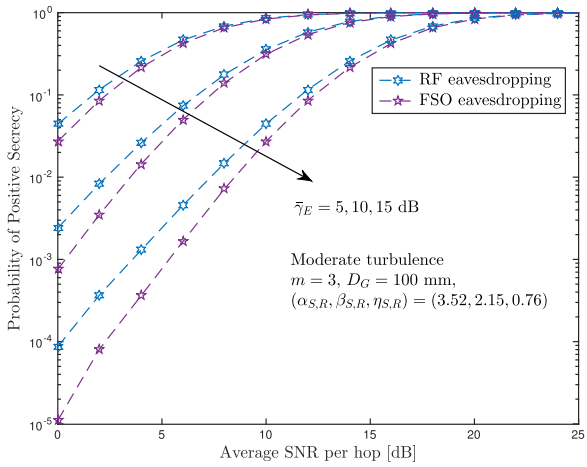

Fig. 7. PPSC performance of RF and FSO eavesdropper attacks for various $\bar{\gamma}_E$ levels under moderate turbulence conditions when $m = 3$ and $D_G = 100$ mm.

Fig. 7 illustrates the PPSC performance of RF and FSO eavesdropper attacks for various $\bar{\gamma}_E$ values. As observed from the figure, the PPSC performance of the RF eavesdropping outperforms its FSO counterpart under moderate turbulence settings as the receiver aperture diameter is selected as 100mm. In addition, the PPSC performance increases monotonically as the impact of eavesdropper decreases due to lower $\bar{\gamma}_E$ values.

B. Remarks

Finally, we provide some important remarks that can be used in the design of secure mixed RF-FSO and FSO-RF relay networks.

- From Fig. 6, it is clear that keeping the receiver photo-aperture around 200mm can enhance the secrecy of mixed RF-FSO relay networks.
- Increasing the Nakagami-*m* severity parameter (m) can enhance the overall SOP performance of both relay networks[7]. However, if m_E is equal to m_{SR} or m_{RD}, using RF transmission at the first hop can be preferable to enhance the physical layer security.
- From Fig. 4, we can understand that the location of the receiver photo-aperture is very important in RF-FSO relay networks to reduce the effects of turbulence-induced fading. Thereby, placing the receiver photo-aperture on a higher ground can provide weak turbulences, and enhances the secrecy performance of the overall system.
- Average eavesdropper SNR can be crucial in the design of secure mixed RF-FSO relay networks. To reduce the effects of the eavesdropper, relay node can be placed closer to the source terminal in mixed RF-FSO relaying and destination node in mixed FSO-RF relaying.
- The receiver photo-aperture size and the height of the relay node can be changeable based on the desired secrecy performance of the overall network. For example, 100mm receiver aperture can be enough to provide 10^{-5} SOP performance, whereas a high ground relay node with 200mm receiver aperture can achieve up to 10^{-6} SOP performance even in harsh weather conditions.

V. Conclusion

In this paper, we provided a general framework about RF and FSO eavesdropping by considering both mixed FSO-RF and RF-FSO relay networks, respectively. To quantify the performance of the proposed schemes, SOP and PPSC expressions were obtained for Nakagami-*m*/EW fading channels. The results which were validated with the aid of simulations, have shown that photo-aperture size, fading parameters, and the average eavesdropper SNR can be crucial to secure the RF-FSO communication. More precisely, almost in all weather conditions, and when the size of the photo-aperture is about 200mm, mixed RF-FSO relaying can be preferable to design a secure RF-FSO relay network.

[7]In Nakagami-*m* fading, the level of fading decreases when *m* increases, and the level of fading increases when *m* decreases.

In future work, we will consider weather dependent attenuation affects, and provide a detailed analysis about the secrecy performance of mixed RF/FSO relay networks.

REFERENCES

[1] F. Demers, H. Yanikomeroglu, and M. St-Hilaire, "A survey of opportunities for free space optics in next generation cellular networks," in *Proc. Commun. Netw. Serv. Res. Conf.*, 2011, pp. 210–216.

[2] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surv. Tut.*, vol. 16, no. 4, pp. 2231–2258, Oct.–Dec. 2014.

[3] 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.

[4] J. N. Laneman, D. N. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[5] O. M. S. Al-Ebraheemy, A. M. Salhab, A. Chaaban, S. A. Zummo, and M.-S. Alouini, "Precise performance analysis of dual-hop mixed RF/unified-FSO DF relaying with heterodyne detection and two IM-DD channel models," *IEEE Photon. J.*, vol. 11, no. 1, Feb. 2019, Art. no. 7900522.

[6] J. Gupta, V. K. Dwivedi, and V. Karwal, "On the performance of RF-FSO system over Rayleigh and κ-μ/inverse Gaussian fading environment," *IEEE Access*, vol. 6, pp. 4186–4198, 2018, doi: 10.1109/ACCESS.2018.2789478.

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

[8] B. Ashrafzadeh, E. Soleimani-Nasab, M. Kamandar, and M. Uysal, "A framework on the performance analysis of dual-hop mixed FSO-RF cooperative systems," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4939–4954, Jul. 2019.

[9] E. Erdogan, N. Kabaoglu, I. Altunbas, and H. Yanikomeroglu, "On the error probability of cognitive RF-FSO relay networks over Rayleigh/EW fading channels with primary-secondary interference," *IEEE Photon. J.*, vol. 12, no. 1, Feb. 2020, Art. no. 7900313.

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

[11] M. I. Petkovic and Z. Trpovski, "Exact outage probability analysis of the mixed RF/FSO system with variable-gain relays," *IEEE Photon. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 6602814.

[12] P. K. Singya, N. Kumar, V. Bhatia, and M.-S. Alouini, "On the performance analysis of higher order QAM schemes over mixed RF/FSO systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7366–7378, Jul. 2020.

[13] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks–Part II: Connectivity," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[14] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the Internet of Things from the physical layer, An overview," *Entropy*, vol. 19, no. 8, pp. 1–16, 2017.

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

[16] 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.

[17] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[18] 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.

[19] 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.

[20] 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, Sep. 2019, Art. no. 7904113.

[21] 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. 12 427–12431, Dec. 2018.

[22] 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. 104127–104138, 2020.

[23] N. H. Juel *et al.*, "Secrecy performance analysis of mixed α- μ and exponentiated Weibull RF-FSO cooperative relaying system," *IEEE Access*, vol. 9, pp. 72342–72356, 2021, doi: 10.1109/ACCESS.2021.3078610.

[24] 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.

[25] 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.

[26] 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. 66 725–66730, 2019, doi: 10.1109/ACCESS.2019.2914227.

[27] C. Kundu, S. Ghose, and R. Bose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4614–4625, Aug. 2015.

[28] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[29] R. Zhao, X. Tan, D.-H. Chen, Y.-C. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11511–11524, Dec. 2018.

[30] R. Barrios and F. Dios, "Exponentiated Weibull distribution family under aperture averaging for Gaussian beam waves," *Opt. Exp.*, vol. 20, no. 12, pp. 13055–13064, 2012.

[31] R. Barrios and F. Dios, "Exponentiated Weibull model for the irradiance probability density function of a laser beam propagating through atmospheric turbulence," *Opt. Laser Technol.*, vol. 45, no. 2, pp. 13–20, 2013.

[32] R. A. Barrios, "Exponentiated Weibull fading channel model in free-space optical communications under atmospheric turbulence," Ph.D. dissertation, Universitat Politécnica de Catalunya (UPC), May 2013.

[33] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1773–1828, Apr.–Jun. 2019.

[34] J. Chen *et al.*, "A novel energy harvesting scheme for mixed FSO-RF relaying systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8259–8263, Aug. 2019.

[35] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. San Diego, CA, USA: Academic, 2007.

[36] E. Erdogan, "Joint user and relay selection for relay-aided RF/FSO systems over exponentiated Weibull fading channels," *Opt. Commun.*, vol. 436, pp. 209–215, 2019.

[37] "From Wolfram research, The mathematical functions site," 2001. [Online]. Available: http://functions.wolfram.com

[38] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. Berlin, Germany: Springer, 2009.

[39] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[40] F. Yilmaz and M.-S. Alouini, "Product of the powers of generalized Nakagami-m variates and performance of cascaded fading channels," in *Proc. IEEE Glob. Telecommun. Conf.*, 2009, pp. 1–8.

[41] P. Wang *et al.*, "Performance analysis for relay-aided multihop BPPM FSO communication system over exponentiated Weibull fading channels with pointing error impairments," *IEEE Photon. J.*, vol. 7, no. 4, Aug. 2015, Art. no. 4600420.