Effects of Eavesdropper on the Performance of Mixed $\eta-\mu$ and DGG Cooperative Relaying System

Noor Ahmad Sarker, A. S. M. Badrudduza, Member, IEEE, Milton Kumar Kundu, Graduate Student Member, IEEE, Imran Shafique Ansari, Senior Member, IEEE, and Imtiaz Ahmed, Member, IEEE

Abstract—Free-space optical (FSO) channels offer line-of-sight wireless communication with high data rates utilizing unlicensed optical spectrum. The hybrid radio frequency (RF)–FSO system is currently receiving a great deal of research interest because atmospheric turbulence prevents enhanced secrecy performance. Except for the double generalized gamma (DGG) model, traditional FSO models typically are unable to show secrecy performance across all turbulence severity ranges. Due to this, we propose a dual-hop $\eta-\mu$ and unified DGG mixed RF–FSO network while taking into account the following three different eavesdropping scenarios: 1) the eavesdropper is at the RF link; 2) the eavesdropper is at the FSO link; and 3) both eavesdroppers remain active simultaneously. These proposed scenarios’ security is examined in terms of the probability, of strictly positive secrecy capacity, secure outage probability and effective secrecy throughput, and further investigation is done into the implications of various system settings on the secrecy performance. The analysis shows that, when compared to the other two scenarios, the third scenario exhibits the worst secrecy condition. Intensity modulation/direct detection (IM/DD) and heterodyne detection (HD) approaches are compared, with HD outperforming IM/DD in terms of secrecy performance. Finally, Monte Carlo simulations are used to confirm all analytical findings.

Index Terms—Double generalized gamma (DGG), physical layer security, radio frequency free-space optical (RF–FSO) network, secure outage probability.

I. INTRODUCTION

A. Background and Related Works

In recent years, free-space optical (FSO) communication has gained momentous attention in the field of wireless communication. FSO has many advantages over conventional wireless channels [1] due to its high speed, interference immunity, secured configuration, larger bandwidth, etc. It has also been proven to be a cost-effective wireless system by providing a sufficient amount of license-free spectrum to its users [2]. Meanwhile, having a great potentiality of solving spectrum scarcity complications places FSO as a valuable candidate for wireless technologies in the upcoming era.

Several research studies have been performed over FSO systems [3],[4],[5],[6],[7],[8],[9],[10],[11] to prove its capability for high speed communication. Zhu and Kahn [3] investigated the impact of turbulence-induced fading of an FSO network exploiting spatial diversity techniques with multiple receivers. The expression of capacity-versus-outage-probability was derived in [4] at low and high noise regions for a moderate number of apertures. Utilizing slow fading conditions, the FSO channel was investigated in [5] based on the natural turbulence and pointing error effects. Similar analysis was again demonstrated in [6] using maximal ratio combining (MRC) and selective combining diversity patterns. Investigation of multiple-input–multiple-output FSO channel was performed in [7]. Performance analysis of an FSO system using Málaga($\rho$) turbulence fading was conducted in [8]. As FSO is a short-range communication medium, relaying schemes were applied in many research works [9],[10],[11] to increase its communication range. Safari and Uysal [9] proposed serial and parallel relaying configuration for both amplify-and-forward (AF) and decode-and-forward (DF) based schemes. A direct source-to-destination link incorporated with DF relaying system was modeled in [10] where ergodic capacity (EC) was analyzed. Yang et al. [11] proposed a two-way relaying (TWR) scheme undergoing double generalized gamma (DGG) fading. Apparently, the FSO medium is highly unfriendly in conveying information signals over a long distance and in nonlinear-of-sight conditions. As it happens, the idea of combined radio frequency-free space optical (RF–FSO) communication is brought forward by many researchers [12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25] in such a way that the RF medium covers up the long-distanced path while the FSO medium fills the remaining short portions of that network. For the RF link, Rayleigh fading is a popular model used in several RF–FSO research works [12],[13],[14],[15],[16],[17],[18]. Gupta et al. [12] proposed a DF-based RF–FSO system and analyzed outage probability (OP), EC, bit error rate (BER), and symbol error rate. A TWR scheme was used in [13] with a multiuser theme.
A partial relay selection scheme for mixed RF–FSO channel was employed in [14] to investigate the outage performance of the system. To minimize fading and turbulence effects in mixed a RF–FSO system, a variable-gain relaying scheme is proposed in [15]. Balti et al. [16] introduced a dual-hop RF–FSO model assembled with hardware impairments that created negligible impact in low signal-to-noise ratio (SNR) regime. A channel state information (CSI)-based RF–FSO system with AF relaying was investigated in [17]. Salhab et al. [18] investigated mixed Rayleigh-[gamma–gamma (IT)] channel with a multirelaying scheme considering a multiuser perspective. A lot of interest from the researchers is noticed around considering Nakagami-$m$ fading channel at the RF link of the mixed RF–FSO channel [19], [20], [21], [22], [23]. Al-Ebraheemuy et al. [19] proposed a mixed Nakagami-$m$-Málaga fading channel and investigated OP, average BER (ABER), and EC at high SNRs based on heterodyne detection (HD) and intensity modulation with direct detection (IM/DD) detection techniques at the receiver. A dual-hop AF-based (Nakagami-$m$)-IT fading model was proposed in [20] to investigate OP, EC, and ABER. A combined (Nakagami-$m$)-DGG system was proposed in [21] where novel expressions for probability density function (PDF) and cumulative distribution function (CDF) along with some performance metrics, e.g., OP and ABER. Exact and asymptotic expressions of OP and EC were analyzed in [22]. Arazumand et al. [23] introduced a cognitive cooperative RF–FSO model to analyze the outage performance of the system. To gain a better understanding of the mixed RF–FSO link, some researchers introduced generalized fading in the RF link [24], [25]. Sharma et al. [24] proposed a mixed ($\eta - \mu$)-IT fading link and analyzed OP, EC, and ABER based on the effects of turbulence and detection types. Identical performance metrics were analyzed in [25] while considering ($\eta - \mu$)-Málaga combined channel. Supposedly, some authors investigated the dual-hop system considering imperfect CSI [26], [27]. Zhang et al. [26] studied an asymmetric dual-hop RF/FSO system assuming both AF and DF relaying methods whereas Zhuang and Zhang [27] analyzed nonorthogonal multiple access based FSO-RF channel adopting MRC schemes. Moreover, a secured hybrid RF-visible light communication (VLC) system was proposed in [28] considering a VLC eavesdropper.

Due to the broadcast nature and time-varying uncertainty, unauthorized users can easily intercept the transmitted data from wireless medium. Physical layer security (PLS) is a promising solution to this unwanted problem [29]. Numerous research has been performed on the secrecy of FSO and mixed RF–FSO networks, as such, [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40]. The effect of correlation along with the pointing error was analyzed in [30] considering the presence of eavesdropper at the FSO (scenario I) and RF link (scenario II). Lopez-Martinez et al. [31] investigated PLS over an FSO link experiencing atmospheric turbulence and analyzed the probability of strictly positive secrecy capacity (SPSC). A mixed RF–FSO system was proposed in [32] considering both variable and fixed-gain AF-based relaying where the authors derived the expression of average secrecy capacity (ASC) and secure outage probability (SOP). PLS for mixed ($\eta - \mu$)-Málaga channel was studied in [33] where authors analyzed average secrecy rate and SOP. A multiuser-based RF–FSO PLS relaying network was studied in [34] where authors analyzed intercept probability (IP) and SOP in both exact and asymptotic forms.

The Lei et al. [35] proposed a secure channel model while considering channel imperfection and analyzed the effective secrecy throughput (EST). The SOP was again analyzed in [36] for a mixed RF–FSO simultaneous wireless information and power transfer downlink system. A PLS model with multiple eavesdroppers was proposed in [37] for a DF-based cooperative channel where authors analyzed ASC, SOP, and probability of SPSC. The Sarker et al. [38] proposed an AF-based variable gain relaying model considering cooperative Hyper Gamma -IT link. Again, Sarker et al. [39] analyzed SOP, SPSC, and IP for generalized $\alpha - \kappa - \mu$ shadowed-Málaga fading channel while considering FSO eavesdropper. A DF-based secure Rayleigh-IT mixed system was investigated in [40] for similar scenario, where authors analyzed SPSC and lower bound of SOP.

B. Motivation and Contributions

Researchers have put out various optical channel models for FSO communication during the past few years. The log-normal model first gained a lot of popularity among researchers due to its simplicity. Yet it had the following two major drawbacks: 1) first of all, this model was mathematically intractable and 2) secondly, it was only suitable for low turbulence situations [41]. If atmospheric turbulence is strong, the conclusions from this model become erroneous, making this model impractical. The researchers proposed another model named IT that produced a perfect result at lower turbulence conditions. But an extensive comparison analysis between IT and double Weibull channel model proved the superiority of the latter at medium and high turbulence state [42]. The DGG model, which eliminates all the drawbacks of the earlier FSO communication models, was ultimately offered by researchers as the only model that could mathematically depict every possible atmospheric turbulence scenario accurately. In spite of having all these advantages as a generalized fading model, very few research has been done on this model, especially considering the security of a mixed RF–FSO communication model with another generalized RF link. The majority of studies have only contemplated the possibility of an eavesdropper at RF links [2], [32], [33], [34], [35], [36], [37], [38] or FSO link [39], [40]. Only a few works like [30] consider eavesdroppers at both RF and FSO hops but they did not consider the possibility of simultaneous eavesdropping. Hence, in our proposed model, we introduce a mixed RF–FSO model considering $\eta - \mu$ fading at the RF link and the DGG fading model at the FSO link. Moreover, we have analyzed the following three eavesdropping scenarios.

1) Scenario-1: The eavesdropper solely attempts to take data from the RF link.
2) Scenario-2: The eavesdropper attempts to overhear data only from FSO link.
3) Scenario-3: The eavesdropper tries to eavesdrop data from RF and FSO links, simultaneously.

Our key contributions in this work are as follows.
1) We begin by utilizing the CDF and PDF of the SNR of each individual hop to derive the CDF and PDF of the investigated dual-hop RF–FSO system. To the best of the authors’ knowledge, both of our suggested fading channels (RF and FSO) convey generic fading properties [43], [44], making these expressions unique compared to other current systems [24], [32].

2) With respect to three different eavesdropping scenarios, we derive expressions for two secrecy performance metrics, namely SOP and the probability of strictly positive secrecy capacity (PSPSC), in order to examine the secrecy performance of the system under consideration. We looked deeper into EST for the system when both eavesdroppers are still active and conducting wiretaps simultaneously. Via Monte Carlo (MC) simulations, the analytical results are further confirmed. Additionally, in order to make more insightful observations about the secure outage performance, we also derive the asymptotic SOP expression. Despite the fact that literature, such as [2], [32], [33], [34], [35], [36], [37], [38], [39], [40], proposed similar secure systems, we obtain superiority in our analysis over these research studies because the proposed models in this work can analyze the secrecy performance for all possible turbulent conditions. Furthermore, we demonstrate how special cases of our work can be used to directly obtain the results presented in [32], [34], and [40].

3) The secrecy performance of the proposed system is also demonstrated to show the impact of the RF channel, atmospheric turbulence, pointing errors, etc., utilizing the SOP, PSPSC, and EST expressions. The numerical results unequivocally demonstrate that the system’s secrecy will be more at risk if the data transmission situation is reversed (transmitting data via relay from the FSO source to the RF receiver). Besides, we also investigate HD and IM/DD techniques to demonstrate the supremacy of the HD technique over the IM/DD technique.

C. Article Organization

The rest of this article is organized as follows. Section II presents the system model and formulation of its PDF and CDF expressions. Novel expressions for the SOP, PSPSC, and EST are derived in Section III. Section IV demonstrates the numerical results of our deduced secrecy metrics. Finally, Section V concludes this article.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a cooperative RF–FSO system presented in Fig. 1, where information is transmitted from source S to destination D through a passable medium relay R that converts the radio waves into optical waves. We consider a DF-based relaying scheme for our proposed system wherein S consists of one transmitting antenna, R houses one receive antenna and one transmit aperture, and D has an aperture to receive optical wave. The S–R link (RF) experiences $\eta$–$\mu$ fading while the R–D link (FSO) undergoes DGG fading channel. For being a high-speed, more reliable, and secure system, such a mixed RF–FSO system is applicable to several real-life scenarios, e.g., solving the last-mile access problems, wireless sensor networks, multiuser systems, and military communication [24], [26], [35]. Based on the eavesdropper’s position, this model has the following three different communication scenarios.

1) Scenario-1: Eavesdropper $E_1$ with one receive antenna tries to intercept confidential data transferred through S–R link via another $\eta$–$\mu$ fading link (S–$E_1$). The R–D link is safe from this wiretapping since $E_1$ is located outside the divergence region of the FSO laser beam.

2) Scenario-2: The first hop (S–R link) is totally secure while eavesdropper $E_2$ having one receiver aperture tries to eavesdrop confidential information from R–D link via another DGG fading FSO (R–$E_2$) link. A similar scenario was proposed in [40] assuming $E_2$ within the laser beam’s divergence area.

3) Scenario-3: Both S–R and R–D links experience simultaneous eavesdropping effect as $E_1$ and $E_2$ both remain active at the same time trying to steal information using their respective channels.

A. SNR of Each Link

For the main RF–FSO channel, we represent $\gamma_{r_0} = \phi_{s,r}^2 / \alpha_{s,r}^2$ and $\gamma_{d_0} = \phi_{r,d}^2 / \alpha_{r,d}^2$ as the instantaneous SNRs of S–R and R–D hops, respectively. For eavesdropper channels, $\gamma_{r_e} = \phi_{s,e}^2 / \alpha_{s,e}^2$ and $\gamma_{d_e} = \phi_{r,e}^2 / \alpha_{r,e}^2$ are denoted as the instantaneous SNRs of S–$E_1$ link and R–$E_2$ link, respectively. Here $\phi_{s,r}$, $\phi_{s,e}$, $\phi_{r,d}$, and $\phi_{r,e}$ denote the average SNRs while $\alpha_{s,r}$, $\alpha_{s,e}$, $\alpha_{r,d}$, and $\alpha_{r,e}$ denote the corresponding channel gains of the S–R, S–$E_1$, R–D, and R–$E_2$ links, respectively. For the combined S–R–D link, R is utilized for relaying purpose with the help of CSI. Hence, SNRs of S–R–D and S–R–$E_2$ links are defined as [45, eq. (5)]

$$\gamma_d = \min \{ \gamma_{r_0}, \gamma_{d_0} \} \quad (1a)$$

$$\gamma_e = \min \{ \gamma_{r_0}, \gamma_{d_e} \} \quad (1b)$$
### B. Secrecy Capacity

To ensure secure data transmission between \( S \) and \( D \), the secrecy rate needs to be maintained at which the eavesdropper is unable to wiretap the confidential transmitted data. Following this, secrecy capacity (SC) expressions for all three scenarios in Fig. 1 regarding DF-based relaying scheme are detailed below.

1) **Instantaneous SC for Scenario-1**: Considering the first scenario where only \( E_1 \) remains active, the instantaneous SC for the dual-hop channel is defined as [46, eq. (3)]

\[
T_{D_1} = \begin{cases} \log_2(1 + \gamma_d) - \log_2(1 + \gamma_{r_0}), & \text{if } \gamma_d > \gamma_{r_0} \\ 0, & \text{if } \gamma_d \leq \gamma_{r_0}. \end{cases} \tag{2}
\]

2) **Instantaneous SC for Scenario-2**: In the second scenario of Fig. 1 where only \( E_2 \) remains active, two SCs are found for \( S-R \) and \( R-D \) links. As \( S-R \) link is not affected by \( E_2 \), instantaneous SC for this link is defined as

\[
T_S = \frac{1}{2} \log_2(1 + \gamma_{r_0}). \tag{3}
\]

For \( R-D \) link where data transmission is affected by \( R-E_2 \) eavesdropper link, instantaneous SC is defined as

\[
T_R = \left[ \frac{1}{2} \log_2(1 + \gamma_{d_0}) - \log_2(1 + \gamma_{d_L}) \right]^+ \tag{4}
\]

where \([f]^+ = \max\{f, 0\}\). So the instantaneous SC for the Scenario-2 of this system can be defined as [47, eq. (13)]

\[
T_{D_2} = \min(T_S, T_R). \tag{5}
\]

3) **Instantaneous SC for Scenario-3**: For simultaneous eavesdropping scenario in Fig. 1, the SCs for each hop are addressed as [48]

\[
T_{SR} = \max(3_{SR}, 0) \tag{6}
\]

\[
T_{RD} = \max(3_{RD}, 0) \tag{7}
\]

where \( T_{SR} \) and \( T_{RD} \) define the SC for first hop (\( S-R \) link) and second hop (\( R-D \) link), respectively. Likewise, \( 3_{SR} \) and \( 3_{RD} \) are the channel capacities of first and second hops, respectively, which are defined as

\[
3_{SR} = \frac{1}{2} \left\{ \log_2(1 + \gamma_{r_0}) \right\} - \frac{1}{2} \left\{ \log_2(1 + \gamma_{r_0}) \right\}
\]

\[
3_{RD} = \frac{1}{2} \left\{ \log_2(1 + \gamma_{d_0}) \right\} - \frac{1}{2} \left\{ \log_2(1 + \gamma_{d_L}) \right\}.
\]

Finally, the instantaneous SC for the system in Fig. 1 (applicable to Scenario-3) is denoted as

\[
T_{D_3} = \min(T_{SR}, T_{RD}). \tag{8}
\]

### C. PDF and CDF of SNR for RF Main Channel

Considering \( \eta-\mu \) fading distribution effecting the main RF channel (i.e., \( S-R \) link), the PDF of \( \gamma_{r_0} \) can be given by [33, eq. (2)]

\[
f_{\gamma_{r_0}}(\gamma) = A \sum_{N_0=1}^{2} \sum_{v=0}^{\mu_0-1} X_{N_0, v} \gamma^{\mu_0-1} e^{-\gamma v} \text{cdf}_{N_0, \gamma} \tag{9}
\]

where

\[
\begin{align*}
A &= \frac{k_0^{\mu_0}}{K_0^{\mu_0}} \Gamma(1 + v) \\
X_{1, v} &= \frac{\Gamma(\mu_0 + v)(\mu_0)^{\mu_0-1} (-1)^v}{v! \Gamma(\mu_0 - v)^4 \mu_0^v} \\
X_{2, v} &= \frac{\Gamma(\mu_0 + v)(\mu_0)^{\mu_0-1} (-1)^v}{v! \Gamma(\mu_0 - v)^4 \mu_0^v} \\
\text{cdf}_{N_0, \gamma} &= 2 \mu_0 (K_0 - K_0) \\
\end{align*}
\]

and \( \text{cdf}_{N_0, \gamma} \) represents gamma operator [49, eq. (8.310)]. \( \eta-\mu \) fading distribution has unique generic characteristics that allows it to represent several multipath fading channels as listed in Table I.

The CDF of \( \gamma_{r_0} \) can be expressed as [33, eq. (3)]

\[
F_{\gamma_{r_0}}(\gamma) = 1 - A \sum_{N_0=1}^{2} \sum_{v=0}^{\mu_0-1} \sum_{x=0}^{1} \frac{X_{r, N_0} Y_{N_0, v}}{x! e^{r} \gamma^{x} v^{x}} \tag{10}
\]

where

\[
Y_{1, v} = \frac{\Gamma(\mu_0 + v)(-1)^v K_0^{-v}}{v! 2^{\mu_0+v}(k_0 - K_0)^{\mu_0-v}} \\
Y_{2, v} = \frac{\Gamma(\mu_0 + v)(-1)^v K_0^{-v}}{v! 2^{\mu_0+v}(k_0 + K_0)^{\mu_0-v}}.
\]

### Table I

**SPECIAL CASES OF \( \eta-\mu \) FADING DISTRIBUTION CHANNEL [43]**

| Channels                  | \( \eta - \mu \) Distribution parameters |
|---------------------------|--------------------------------------------|
| Hoyt / Nakagami-\( q \)  | \( \eta \rightarrow q^\ast, \mu = 0.5 \)   |
| One-sided Gaussian        | \( \eta \rightarrow 0 \text{ (or } \eta \rightarrow \infty), \mu = 0.5 \) |
| Rayleigh                  | \( \eta \rightarrow 0 \text{ (or } \eta \rightarrow \infty), \mu = 1 \) |
| Nakagami-\( m \)          | \( \eta \rightarrow 0 \text{ (or } \eta \rightarrow \infty), \mu = m \) |
DGG is a generic fading model for FSO communications thereby housing several classical fading models within itself as listed in [52, Table (II)]. Hence, this is one of the most popular fading models that has attracted many wireless communication (OWC) researchers. The CDF of $\gamma_{d0}$ is defined as [41, eq. (14)]

$$F_{\gamma_{d0}}(\gamma) = B_3G_{s_0 + 1, \delta_0 + 1} \left[ B_4 \left( \frac{\gamma}{U_d} \right)^{7} \right] 1, j_3 \mid j_4, 0 \right] \tag{12}$$

where

$$B_3 = \left( \frac{\beta_5^{\varepsilon_5} \gamma_{\text{eg}}}{s_0^{\delta_0 + 1}} \right), \text{ and } \delta_0 = s_0(\lambda_1 + \lambda_2 + 1).$$

The series terms $j_3 = [\Delta(s_0 : j_2)]$ and $j_4 = \Delta(s_0 : j_1)$ are denoted comprising $s_0$ and $\delta_0$ terms, respectively, where the series expression $[\Delta(\sigma : \Lambda)]$ with $\Lambda$ terms is written as

$$[\Delta(\sigma : \Lambda)] = \Delta(\sigma : 1), \Delta(\sigma : 2), ..., \Delta(\sigma : \Lambda). \tag{13}$$

E. PDF and CDF of SNR for the Eavesdropper Channels

1) Eavesdropper at the RF Link: Similar to (9), the PDF of SNR for $S$–$E_1$ link can be defined as

$$f_{\gamma_{se}}(\gamma) = C \sum_{N=1}^{\infty} \sum_{w=0}^{\infty} X_{N,w} \gamma^{\mu+\nu-w} - 1 e^{-l_0 \gamma_{se} \gamma} \tag{14}$$

where

$$C = \frac{k^{\gamma_{se}}}{K_{\gamma_{se}} \Gamma(\mu \nu)}, \quad X_{1,0} = \frac{\Gamma(\mu \nu) \Gamma(\mu_0 - w)}{\Gamma(\mu \nu - w) K_{\gamma_{se}} K_{\gamma_{se}}} \left( -1 \right)^w,$$

$$X_{2,0} = \frac{\Gamma(\mu \nu) \Gamma(\mu_0 - w)}{\Gamma(\mu \nu - w) K_{\gamma_{se}} K_{\gamma_{se}}} \left( -1 \right)^w, \quad l_0 = \frac{2 \mu_0(\lambda - K_{\gamma_{se}})}{\phi_{\gamma_{se}}}. \tag{15}$$

For the specific condition $\mu_0 > 0$ and $0 < \eta < 4$, the parameters $k_{\gamma_{se}}$ and $K_{\gamma_{se}}$ are denoted as $k_{\gamma_{se}} = 2 + \nu + \nu_{se}$ and $K_{\gamma_{se}} = \frac{\eta_{se}}{4}$. Like (10), CDF of $\gamma_{se}$ is expressed as

$$F_{\gamma_{se}}(\gamma) = 1 - C \sum_{N=1}^{\infty} \sum_{w=0}^{\infty} \sum_{y=0}^{\infty} Y_{N,w,y} \gamma^{\mu+\nu-w} - 1 e^{-l_0 \gamma_{se} \gamma} \tag{15}$$

where

$$Y_{1,0} = \frac{\Gamma(\mu \nu) \Gamma(\mu_0 - w)}{\Gamma(\mu \nu - w) K_{\gamma_{se}} K_{\gamma_{se}}} \left( -1 \right)^w,$$

$$Y_{2,0} = \frac{\Gamma(\mu \nu) \Gamma(\mu_0 - w)}{\Gamma(\mu \nu - w) K_{\gamma_{se}} K_{\gamma_{se}}} \left( -1 \right)^w.$$}

2) Eavesdropper at the FSO Link: The $R$–$E_2$ link experiences DGG fading similar to main FSO link. Accordingly, the PDF of $\gamma_{de}$ is defined just like (11) as

$$f_{\gamma_{de}}(\gamma) = \frac{B_1}{s_0 \gamma} \gamma^{\lambda_1 + \lambda_2 + 1,0} \left( \frac{B_2 \gamma}{U_d} \right)^{7} 1, j_2 \mid j_1 \right] \tag{16}$$

where $s_e$ represents detection types for $E_2$ ($s_e = 1$ for HD and $s_e = 2$ for IM/DD). The electrical SNR of this link is addressed as $U_e = \left( \frac{P_e}{\Lambda_e L_e I_e} \right)$. Here, $\Lambda_e$, $I_e$, and $P_e$ denote photoelectric conversion coefficient, irradiance, and number of sample apertures, respectively, for the $R$–$E_2$ link. Similar to (12), the CDF of $\gamma_{de}$ is defined as

$$F_{\gamma_{de}}(\gamma) = B_5 G_{s_e + 1, \delta_e + 1} \left[ B_6 \left( \frac{\gamma}{U_d} \right)^{7} 1, j_5 \mid j_6, 0 \right] \tag{17}$$

where $B_5 = \frac{\beta_5^{\varepsilon_5} \lambda_1 + \lambda_2 + 1,0}{s_e^{\delta_e + 1}} \left( \frac{B_2 \gamma}{U_d} \right)^{7} 1, j_5 \mid j_6, 0 \right]$.

F. PDF and CDF of SNR for Dual-Hop RF–FSO Link

Utilizing order statistics, the CDF of $\gamma_d$ is expressed as [20, eq. (5)]

$$F_{\gamma_d}(\gamma) = \Pr \left[ \min(\gamma_{ro}, \gamma_{do}) < \gamma \right] = F_{\gamma_{ro}}(\gamma) + F_{\gamma_{do}}(\gamma) - F_{\gamma_{ro}}(\gamma) F_{\gamma_{do}}(\gamma). \tag{18}$$

Placing (10) and (12) into (18) and performing some arithmetic simplifications, the CDF of $\gamma_d$ is written as

$$F_{\gamma_{de}}(\gamma) = 1 - A \sum_{N=1}^{2} \sum_{x=0}^{\infty} \gamma_{se} \gamma^{\mu_0 - 1, \mu_0 - 1} e^{-l_0 \gamma_{se} \gamma} \sum_{x=0}^{\infty} \gamma_{se} \gamma^{\mu_0 - 1, \mu_0 - 1} e^{-l_0 \gamma_{se} \gamma} \tag{19}$$

The PDF of $\gamma_d$ is defined as [12, eq. (4)]

$$f_{\gamma_{de}}(\gamma) = f_{\gamma_{ro}}(\gamma) + f_{\gamma_{do}}(\gamma) - f_{\gamma_{ro}}(\gamma) f_{\gamma_{do}}(\gamma). \tag{20}$$

Substituting (9)–(12) into (20) and doing some simplifications, the PDF of $\gamma_d$ is obtained as

$$f_{\gamma_{de}}(\gamma) = A \sum_{N=1}^{2} \sum_{x=0}^{\infty} \gamma_{se} \gamma^{\mu_0 - 1, \mu_0 - 1} e^{-l_0 \gamma_{se} \gamma} \gamma_{se} \gamma^{\mu_0 - 1, \mu_0 - 1} e^{-l_0 \gamma_{se} \gamma} \tag{21}$$

III. PERFORMANCE ANALYSIS

In this section, we derive 1) novel closed-form expressions of the SOP and PSPSC for the three scenarios; 2) asymptotic expressions for the SOP to obtain better intuition on our analysis; and 3) EST expression in the case of Scenario-3 for analyzing the trade-off between security and reliability.

A. Secure Outage Probability

SOP is a decisive performance metric for secrecy analysis. It demonstrates the reverse mechanism to evaluate secrecy performance. $T_D$ and $T_C$ are addressed as the SC and target secrecy rate of the system, respectively. When $T_D$ falls below $T_C$, the exact closed-form SOP expression can be defined as [53, eq. (14)]

$$SOP = \Pr \{ T_D \leq T_C \} = \Pr \{ \gamma_d \leq \varphi \gamma_{se} + \varphi - 1 \} \tag{22}$$
where $\varphi = 2\pi c$. Mathematically, the term in (22) can be described as [54]

$$SOP = 1 - \int_0^\infty \int_0^\infty f_d(\gamma_d) f_r(\gamma_r) d\gamma_d d\gamma_r$$

$$= \int_0^\infty F_{\gamma_d}(\varphi + \varphi - 1) f_r(\gamma_r) d\gamma_r.$$  \(23\)

Unfortunately, due to the shift in Meijer’s G function, the exact closed-form expression mentioned in (23) is not available in any literature [32], [33]. Hence, for DF relaying scheme, we often consider lower-bound SOP as [55, eq. (6)]

$$SOP \geq SOP_L = \int_0^\infty F_{\gamma_d}(\varphi + \varphi - 1) f_r(\gamma_r) d\gamma_r.$$  \(24\)

Based on (24), lower bound SOP expressions for three different scenarios of Fig. 1 are derived in the following parts.

1) Scenario-1: Considering $T_c$, the target secrecy rate for Scenario-1, the lower-bound SOP for the first scenario can be introduced as

$$SOP_1 \geq SOP_{1,L} = \int_0^\infty F_{\gamma_d}(\varphi + \varphi - 1) f_r(\gamma_r) d\gamma_r,$$  \(25\)

where $\varphi_1 = 2^TC_1$. Substituting (14) and (19) into (25), the SOP for scenario-1 is expressed as

$$SOP_{1,L} = 1 - AC \sum_{N_0=1}^2 \sum_{N_1=1}^{\mu_0-1} \sum_{\mu_1=1}^{\mu_1-1} \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{r_1 N_0 \times \nu_0 \times x_0}{x!}$$

$$\times X_{N_0,N_1} Y_{N_0,v} (Q_1 - B_{3} Q_2).$$  \(26\)

Performing integration operation utilizing [49, eq. (3.51.3)], the term $Q_1$ in (26) is obtained as

$$Q_1 = \int_0^\infty \gamma_r e^{-\gamma_r} \varphi_1 e^{-\gamma_r} d\gamma_r = \frac{\varphi_1^2 \Gamma(\varphi_1)}{(\varphi_1)^2}.$$  \(27\)

where $\varphi = \varphi_1 t_{C,N_0} + t_{e,N_1}$, and $z_1 = \mu_e - \nu + x$. Subsequently, performing integration via applying [56, eq. (2.24.1.1)], the term $Q_2$ in (26) is obtained as

$$Q_2 = \int_0^\infty \gamma_r e^{-\gamma_r} \varphi_1 e^{-\gamma_r} d\gamma_r = \frac{\varphi_1^2 \Gamma(\varphi_1)}{(\varphi_1)^2}.$$  \(28\)

where $\varphi_2 = 2^TC_2$ and $T_{1C_2}$ is the target SC for Scenario-2. Placing (10), (12), and (16) into (31) and performing some integration and simplifications via utilizing [56, eq. (2.24.1.1)], (31) is obtained as

$$SOP_{2,L} = 1 - A \sum_{N_0=1}^2 \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{(\varphi_2-1)^x e^{-\gamma_r N_0 (\varphi_2-1)}}{x!}$$

$$\times \frac{\varphi_2^2 \Gamma(\varphi_2)}{(\varphi_2)^2}.$$  \(32\)

where $\varphi_2 = 2^TC_2$ and $T_{1C_2}$ is the target SC for Scenario-2. Placing (10), (12), and (16) into (31) and performing some integration and simplifications via utilizing [56, eq. (2.24.1.1)], (31) is obtained as

$$SOP_{2,L} = 1 - A \sum_{N_0=1}^2 \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{(\varphi_2-1)^x e^{-\gamma_r N_0 (\varphi_2-1)}}{x!}$$

$$\times \frac{\varphi_2^2 \Gamma(\varphi_2)}{(\varphi_2)^2}.$$  \(32\)

It is observed that the derived expression in (32) can be utilized to generate Rayleigh–IT distribution [40, eq. (19)] while considering the conditions $\eta_0 = 1$, and $\mu_0 = 1$, $a_1 = 0 = \Omega_1 = 2 = 0$.

Asymptotic Expression: Similar to (30), we define the asymptotic expression of (32) by making use of [8, eq. (41)] as

$$SOP_{2,\infty} = 1 - A \sum_{N_0=1}^2 \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{(\varphi_2-1)^x e^{-\gamma_r N_0 (\varphi_2-1)}}{x!}$$

$$\times \frac{\varphi_2^2 \Gamma(\varphi_2)}{(\varphi_2)^2}.$$  \(32\)

The expression in (26) can be utilized to obtain Rayleigh–IT distribution [34, eq. (15)] by setting $\eta_0 = \tau_e = 1$, $\mu_0 = \mu_e = 1$, and $a_1 = 0 = \Omega_1 = 2 = 0$. It can also be reformulated as (Nakagami-m)–IT distribution [32, eq. (13)] via setting $\eta_0 \geq 1$, $\eta_e \geq 1$, $\mu_0 \geq 1$, $\mu_e \geq 1$, and $a_1 = 0 = \Omega_1 = 2 = 0$.

Asymptotic Expression: To gain better understanding of the secrecy incident of our proposed model, we derive asymptotic SOP expression by setting $U_d \rightarrow \infty$. By converting the Meijer’s G term described in (26) via utilizing [57, eq. (6.2.2)] and [8, eq. (19)], the asymptotic SOP for Scenario-1 is expressed as

$$SOP_{1,\infty} = 1 - AC \sum_{N_0=1}^2 \sum_{N_1=1}^{\mu_0-1} \sum_{\mu_1=1}^{\mu_1-1} \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{r_1 N_0 \times \nu_0 \times x_0}{x!}$$

$$\times X_{N_0,N_1} Y_{N_0,v} (Q_1 - B_{3} Q_2).$$  \(30\)

2) Scenario-2: For the DF-based relaying configuration setup in Scenario-2 of Fig. 1, lower bound SOP is defined as

$$SOP_2 \geq SOP_{2,L} = \int_0^\infty F_{\gamma_d}(\varphi_2 \gamma_r) f_r(\gamma_r) d\gamma_r$$

$$\times \{ 1 - F_{\gamma_r}(\varphi_2 \gamma_r) \} + F_{\gamma_r}(\varphi_2 \gamma_r)$$  \(31\)

where $\varphi_2 = 2^TC_2$ and $T_{1C_2}$ is the target SC for Scenario-2. Placing (10), (12), and (16) into (31) and performing some integration and simplifications via utilizing [56, eq. (2.24.1.1)], (31) is obtained as

$$SOP_{2,L} = 1 - A \sum_{N_0=1}^2 \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{(\varphi_2-1)^x e^{-\gamma_r N_0 (\varphi_2-1)}}{x!}$$

$$\times \frac{\varphi_2^2 \Gamma(\varphi_2)}{(\varphi_2)^2}.$$  \(32\)

It is observed that the derived expression in (32) can be utilized to generate Rayleigh–IT distribution [40, eq. (19)] while considering the conditions $\eta_0 = 1$, and $\mu_0 = 1$, $a_1 = 0 = \Omega_1 = 2 = 0$.

Asymptotic Expression: Similar to (30), we define the asymptotic expression of (32) by making use of [8, eq. (41)] as

$$SOP_{2,\infty} = 1 - A \sum_{N_0=1}^2 \sum_{\nu_0=0}^{\mu_0-1} \sum_{x_0=0}^{\nu_0-1} \frac{(\varphi_2-1)^x e^{-\gamma_r N_0 (\varphi_2-1)}}{x!}$$

$$\times \frac{\varphi_2^2 \Gamma(\varphi_2)}{(\varphi_2)^2}.$$  \(32\)

where $J_1 = (1 - j_4, 1, j_5)$, and $J_2 = (j_6, 0, 1 - j_3)$.

3) Scenario-3: The lower bound SOP for Scenario-3 is defined as

$$SOP_3 \geq SOP_{3,L} = 1 - (1 - S_1)(1 - S_2)$$  \(34\)
where $\varphi_3 = 2^{TC_3}$, and $TC_3$ is defined as the target SC for the third scenario in Fig. 1. The two integration terms $S_1$ and $S_2$ are denoted as

$$S_1 = \int_0^\infty F_{\gamma_{ro}}(\varphi_3 \gamma) f_{\gamma_{ro}}(\gamma) d\gamma$$

(35)

$$S_2 = \int_0^\infty F_{\gamma_{ro}}(\varphi_3 \gamma) f_{\gamma_{ro}}(\gamma) d\gamma.$$ 

(36)

Placing (10) and (14) into (35), performing integration via utilizing [49, eq. (3.351.3)], and applying algebraic simplifications, (35) is obtained as

$$S_1 = C \sum_{N_e=1}^{N_e} \sum_{v=0}^{\mu_e-1} X_{N_e,v,w} \left( l_{e,N_e} \right)^{w-\mu_e} \Gamma(\mu_e - w)$$

$$- A \sum_{N_0=1}^{N_0} \sum_{v=0}^{\mu_0-1} \sum_{x=0}^{\mu_0-v-1} \frac{\varphi_3 l_{ro} l_{ro}}{x! e^{x}} Y_{N_0,v}.$$ 

(37)

Likewise, substituting (12) and (16) into (36) while performing arithmetic integration and simplification utilizing [49, eq. (3.351.3)], we obtain

$$S_2 = B_3 B_5 G_{s_0+1,0} \left( l_{ro} \right)^{1-\delta_3} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3}.$$ 

(38)

**Asymptotic Expression:** The asymptotic expression of SOP for Scenario-3 is expressed as

$$SOP_{3,\infty} = 1 - (1 - S_1)(1 - S_3)$$ 

(39)

where $S_1$ can be obtained by modifying the Meijer’s $G$ function in (38) via utilizing [8, eq. (41)] as

$$S_3 = B_3 B_5 G_{s_0+1,0} \left( l_{ro} \right)^{1-\delta_3} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3}.$$ 

(40)

**B. Probability of Strictly Secure Capacity**

The PSPSC is the inverse probable term of outage probability that is a positive volume of SC. In this subsection, we derive expressions of PSPSC for all three scenarios described in Fig. 1.

1) Scenario-1: Considering Scenario-1 wherein eavesdropper $E_1$ is located near the $S-R$ link, PSPSC can be expressed as [58]

$$PSPSC_1 = \Pr(T_{D_1} > 0) = \Pr(\gamma_d > \gamma_{ro})$$

$$= \int_0^\infty f_{\gamma_{ro}}(\gamma) G_{\gamma_{ro}}(\gamma) d\gamma.$$ 

(41)

Substituting (15) and (21) into (41) and employing mathematical simplifications, PSPSC for Scenario-1 is obtained as

$$PSPSC_1 = A \sum_{N_0=1}^{\mu_0-1} \sum_{v=0}^{\mu_0-v-1} \left( X_{N_0,v,\nu} \right) R_1 + \sum_{x=0}^{\mu_0-v-1} \frac{l_{e,N_0}}{x!} Y_{N_0,v}.$$ 

(42)

where $R_1$, $R_2$, $R_3$, and $R_4$ are four integration terms such as

$$R_1 = \int_0^\infty \frac{B_3^{s_0+1,0}}{e^{l_{ro} \gamma} \tau_0} G_{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma$$ 

(43)

$$R_2 = \int_0^\infty \frac{B_3^{s_0+1,0}}{e^{l_{ro} \gamma} \tau_0} G_{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma$$ 

(44)

$$R_3 = \int_0^\infty \frac{B_3^{s_0+1,0}}{e^{l_{ro} \gamma} \tau_0} G_{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(45)

$$R_4 = \int_0^\infty \frac{B_3^{s_0+1,0}}{e^{l_{ro} \gamma} \tau_0} G_{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(46)

Performing mathematical calculations in (43)–(46) by utilizing the formulas explained in [56, eq. (2.24.1.11)] and (29), the final expressions of those integration terms are presented as

$$R_1 = \int_0^\infty B_3^{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(47)

$$R_2 = \int_0^\infty B_3^{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(48)

$$R_3 = \int_0^\infty B_3^{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(49)

$$R_4 = \int_0^\infty B_3^{s_0+1,0} \left[ \frac{B_6}{B_4} \left( \frac{U_{d}}{U_{e,\nu}} \right)^{T} \right]_{j6,0,1,-j3} d\gamma.$$ 

(50)

where $z_d = \mu_0 - v, z_3 = z_2 + y, z_4 = x + y, and H = l_{e,N_0}$.

2) Scenario-2: For the DF-based system in Scenario-2, PSPSC can be defined as [59, eq. (9)]

$$PSPSC_2 = \Pr(\min(T_S, T_R) > 0) = \Pr(T_S > 0) \Pr(T_R > 0).$$ 

(51)

For $S-R$ link, in the case of Scenario-2, the positive probability term is expressed as

$$\Pr(T_S > 0) = \Pr \left[ \frac{1}{2} \log_2(1 + \gamma_{ro}) > 0 \right] = \Pr(\gamma_{ro} > 0) = 1.$$ 

(52)

For second-hop, the probability term is defined as

$$\Pr(T_R > 0) = \Pr \left[ \frac{1}{2} \log_2(1 + \gamma_{ro}) - \log_2(1 + \gamma_{ro}) > 0 \right] > 0.$$
Substituting (52) and (53) into (51), the PSPSC can be denoted as

$$PSPSC_2 = 1 - \int_0^\infty F_{\gamma_{d\gamma}}(\gamma)d\gamma.$$

(54)

Setting the values of (12) and (16) into (54), and performing integration utilizing [56, eq. (2.25.1.1)], (54) is obtained as

$$PSPSC_2 = 1 - B_3B_5\int_0^\infty \frac{B_d}{U_c} \left[ 1 - j_4,1,j_5 \right].$$

(55)

It can be noted that by setting the fading parameter values to \( \eta_0 = 1, \mu_0 = 1, \) and \( a_1 = a_2 = \Omega_1 = \Omega_2 = 1, \) the expression derived in (55) matches with [40, eq. (25)] of the Rayleigh-\( \Gamma \) fading distribution.

3) Scenario-3: Similar to (51), the PSPSC for Scenario-3 is defined as

$$PSPSC_3 = Pr \{ T_{D3} > 0 \} \Pr \{ T_{SR} > 0 \} \Pr \{ T_{RD} > 0 \}.$$  

(56)

Substituting (10), (12), (14), and (16) into (56), we obtain a similar type of expression like (34) as

$$PSPSC_3 = \left( 1 - U_1 \right) \left( 1 - U_2 \right)$$

(57)

where the two integration terms \( U_1 \) and \( U_2 \) are denoted as

$$U_1 = \int_0^\infty F_{\gamma_{d\gamma}}(\gamma)d\gamma$$

(58)

$$U_2 = \int_0^\infty F_{\gamma_{d\gamma}}(\gamma)d\gamma.$$  

(59)

Similar to (37), the integration term \( U_1 \) is written as

$$U_1 = C \sum_{N_e=1}^{2} \sum_{\nu=0}^{\mu_e-1} X_{N_e,v} \left[ (l_{e,N_e})^{w-\mu_e} \Gamma(\mu_e - w) \right]$$

$$- A \sum_{N_0=1}^{2} \sum_{v=0}^{\mu_0-1} \sum_{w=0}^{\mu_0-w-1} \frac{(l_{r,N_0})^{z} \Gamma(z)}{z! \Gamma(z)} Y_{N_0,v}.$$  

(60)

Likewise, following similar integration process to (38) and (55), \( U_2 \) is obtained as

$$U_2 = B_3B_5\int_0^\infty \frac{B_d}{U_c} \left[ 1 - j_4,1,j_5 \right].$$

(61)

C. EST for Scenario-3

EST is an important performance index for the wireless channel which relates security with reliability in terms of the average rate of secure data transmitted from source to end user without being wiretapped. For the simultaneous wiretapping scenario of our proposed model, i.e., Scenario-3, EST can be measured as [35, eq. (5)]

$$EST = T_{C3}(1 - SOP3).$$

(62)

IV. NUMERICAL RESULTS

In this section, we present some analytical results utilizing the derived expressions of the secrecy metrics, namely lower bound and asymptotic SOP, PSPSC, and EST. To corroborate our analytical outcomes, we also demonstrate MC simulations via generating \( \eta-\mu \) and DGG random variables in MATLAB and averaging 100,000 channel realizations. It is noteworthy in the figures that the analytical and simulation results are in good agreement with each other. The analysis is performed by assuming some parametric values such as \( \eta_0, \mu_0, \) and \( a_1 = a_2 = \Omega_1, \Omega_2, \) \( 0.01 \) bits/sec/Hz, \( s_0 = s_o = (1,2) \), and \( \epsilon \in \{ 1,6,7 \} \). To analyze natural turbulence levels over the DGG link, we set up the following values for turbulence parameters [44].

1) \( a_1 = 1.86, a_2 = 1, b_1 = 0.5, b_2 = 1.8, \Omega_1 = 1.51, \Omega_2 = 1, \lambda_1 = 17, \) and \( \lambda_2 = 9 \) for strong turbulence (ST).
2) \( a_1 = 2.17, a_2 = 1, b_1 = 0.55, b_2 = 2.35, \Omega_1 = 1.58, \Omega_2 = 0.97, \lambda_1 = 28, \) and \( \lambda_2 = 13 \) for moderate turbulence (MT).
3) \( a_1 = a_2 = 2.1, b_1 = 4, b_2 = 4.5, \Omega_1 = 1.07, \Omega_2 = 1.06, \) and \( \lambda_1 = \lambda_2 = 1 \) for weak turbulence (WT).
Fig. 4. EST versus $T_{C_3}$ for selected values of $\phi_{s,e}$ with $\eta_0 = \mu_e = 30$, $\mu_0 = \mu_e = 1$, $\phi_{s,e} = U_e = -5$ dB, $U_r = 15$ dB, MT, $s_0 = s_e = 1$, and $\epsilon = 0.7$.

Fig. 2 indicates relationship between PSPSC$_1$ and $\phi_{s,e}$ for Scenario-1. Meanwhile, PSPSC$_2$ is plotted against $U_d$ in Fig. 3 for Scenario-2. It is observed that in both cases, PSPSC increases when the average SNR of $S$–$E_1$ or $R$–$E_2$ link decreases. This analysis is performed by taking the range of $\phi_{s,e}$ from 10 to −10 dB in Fig. 2, and by changing $U_r$ from −10 to 30 dB in Fig. 3. These two events reveal that decrease in $\phi_{s,e}$ and $U_r$ renders the eavesdropper channels weaker relative to the main channel, thereby the PSPSC performance improves as reported in [38] and [60].

Fig. 4 displays a concave down-shaped curve of EST against $T_{C_3}$ for Scenario-3. It is observed that for different $\phi_{s,e}$ ranging from −5 to 10 dB, the EST increases up to certain values of $T_{C_3}$; ranging between 1.8 and 3.8 bits/sec/Hz. This event represents the trade-off between limited security resources and $T_{C_3}$. As $T_{C_3}$ grows higher, more prerequisites for wiretap protection are needed. Meanwhile, higher $T_{C_3}$ introduces several drawbacks; such as forcing additional computation time, slowing down transmission speed, and offering unwanted noise and interference to the system. For such reasons, EST in Fig. 4 faces a continuous decline from the peak for larger $T_{C_3}$. Supposedly, Fig. 4 thoroughly exhibits the optimization of the secrecy trade-off between resources required for security maintenance and the target secrecy rate.

A comparative analysis between two detection techniques at FSO receiver is demonstrated in Fig. 5 for Scenario-3 against $U_d$. The result implies that utilizing the HD technique ($s_0 = s_e = 1$) for signal detection provides better secrecy output relative to the IM/DD technique ($s_0 = s_e = 2$), since HD provides higher SNR than IM/DD via implying better encryption method. The results demonstrated in [39] and [40] also agree with our finding that validates our analysis.

The influence of pointing errors in FSO links is demonstrated in Figs. 6–8. Herein, Fig. 6 illustrates SOP$_1$ that is applicable to Scenario-1. Additionally, Fig. 7 demonstrates SOP$_2$ for Scenario-2 and Fig. 8 showcases SOP$_3$ representing Scenario-3. Results demonstrate that secrecy performance of each eavesdropping scenario notably increases when $R$–$D$ link undergoes from severe ($\epsilon = 1$) to negligible ($\epsilon = 6.7$) pointing error. This outcome is expected as higher $\epsilon$ devise significant line-of-sight (LoS) misalignment of the signal. Evidently, similar results were obtained in [32] and [40] that corroborate our investigations. Moreover, asymptotic outputs are demonstrated in these figures for SOP$_1$, SOP$_2$, and SOP$_3$ that reveal the asymptotic lower bound SOP results can tightly approximate our derived lower bound SOP results in the high SNR regime.

Besides the detection technique types and pointing errors, DGG turbulence parameters also place notable influences on the secrecy performance. Figs. 5–8 indicate the effects of three turbulence conditions, namely, ST, MT, and WT. Our demonstrated outcomes show the expected results similar to [32], [38], [40] that secrecy performance with weaker turbulence in Figs. 5–8 clearly outperforms that under stronger turbulence.

**Generalization Demonstrated via the Proposed Model:** In our proposed model, we assume $\eta$–$\mu$ distribution over the RF hop and unified DGG model over the FSO hop. The $\eta$–$\mu$ distribution has an outstanding generic nature that can emerge several
TABLE II

SOME RESEARCH STUDIES AS SPECIAL CASES OF OUR PROPOSED MODEL

| Reference | RF link | PSO link | Eavesdroppers |
|-----------|---------|----------|---------------|
|           | Rayleigh (q = 1, μ = 1) | A distribution (a₁ = a₂ = b₁ = b₂ = Ω₁ = λ₁ = 1, b₂ = 1.8) | - |
|           | Rayleigh (q = 1, μ = 1) | Double Weibull (a₁ = a₂ = 2.1, b₁ = b₂ = 1, Ω₁ = 1.07, Ω₂ = 1.06, λ₁ = λ₂ = 1) | - |
| [32]      | Nakagami-m (q = 20, μ = 2) | Log-normal (a₁ = a₂ = 0.01, b₁ = 4, b₂ = 4.5, Ω₁ = Ω₂ = 1.07, λ₁ = λ₂ = 1) | - |
| [34]      | Nakagami-m (q = 100, μ = 2) | DOG (G₁ = 2.17, a₁ = 2, b₁ = 0.55, b₂ = 3.05, Ω₁ = 1.56, Ω₂ = 0.97, λ₁ = 2b, λ₂ = 13) | - |
| [33]      | Nakagami-m (q = 20, μ = 2) | FFN (a₁ = a₂ = Ω₁ = Ω₂ = 1 = λ₁ = 1, b₁ = 2.236, b₂ = 1.822) | RF |
| [34]      | Nakagami-m (q = 20, μ = 2) | FFN (a₁ = a₂ = Ω₁ = Ω₂ = 1 = λ₁ = 1, b₁ = 2.236, b₂ = 1.822) | RF |
| [30]      | Rayleigh (q = 1, μ = 1) | FFN (a₁ = a₂ = Ω₁ = Ω₂ = 1 = λ₁ = 1, b₁ = 2.236, b₂ = 1.822) | PSO |

multopath fading channels as special cases that are indicated in Table I. Meanwhile, unified DGG is also a generalized FSO turbulent model from which multiple classical FSO models can be generated as special cases, as listed in [52, Table (II)]. It is observed that the demonstrated channel models in [32] and [34] can be addressed as the special cases of Scenario-1. Likewise, the secure models denoted in [40] can be identified as a special case of our proposed Scenario-2. Additionally, we investigate the secrecy performance in simultaneous eavesdropping condition as proposed under Scenario-3 wherein both eavesdroppers near RF and FSO links are active concurrently. We also summarize other special cases of our proposed system in Table II that are not available in the literature till date. All those special cases are graphically represented in Figs. 9–11 for all three wiretapping scenarios of Fig. 1.
A comparative analysis of three different scenarios of Fig. 1 is investigated in Fig. 12, where SOP is plotted against $\phi_{s,t}$. It is observed that for the proposed scenario in Fig. 12, Scenario-3 demonstrates the worst secrecy performance as simultaneous wiretapping of $E_1$ and $E_2$ highly weakens the main $S-R-D$ channel. Meanwhile, Scenario-2 exhibits comparatively better secrecy performance than Scenario-1 since FSO signals have lower susceptibility to eavesdropping compared to RF signals. Furthermore, MC simulation is performed in Fig. 12 for the reverse FSO-RF model of Fig. 1 assuming the first hop experiences FSO DGG link and the second hop experiences RF $\eta-\mu$ link. Consequently, $E_2$ eavesdrops near the $S-R$ link in Reverse Scenario-1 and $E_1$ wiretaps near the $R-D$ link in Reverse Scenario-2. The outcome shows that Reverse Scenario-1 is the worst case and Reverse Scenario-2 displays the best performance as usual. Concurrently, Reverse Scenario-3 (FSO-RF) shows the same output as Actual Scenario-3 (RF-FSO) as simultaneous wiretapping ability of both eavesdroppers remain consistent. In RF-FSO research field, such diverse analysis of ours for every communication scenarios indicates profound uniqueness and novelty.

V. CONCLUSION

This study examines how well an RF–FSO hybrid framework maintains secrecy when being intercepted across RF or FSO networks. The secrecy assessments are carried out by deriving closed-form expressions for PSPSC, EST, and lower bound SOP and collecting further insightful information by developing asymptotic SOP expressions. All analytical expressions are verified by MC simulations as well. Through the use of the derived expressions, the effects of fading, mild to severe atmospheric turbulence, and pointing errors are noted. The optimization between target secrecy rate and security requirements for the proposed system is studied via EST for simultaneous eavesdropping condition. As may be observed, the diverse reported outcomes in the literature are generalized by the results we have shown. The mathematical analysis also shows that Scenario-3 is the least secure of the three scenarios under consideration. To demonstrate the diversification of secrecy analysis, a simulation study is also presented for the proposed model’s reverse (FSO-RF) scenario. Furthermore, a comparison of HD and IM/DD techniques shows that, when compared to the suggested system, the HD technique delivers better and more secure outage performance than the IM/DD technique.

REFERENCES

[1] W. Fawaz, C. Abou-Rjeily, and C. Assi, “UAV-aided cooperation for FSO communication systems,” IEEE Commun. Mag., vol. 56, no. 1, pp. 70–75, Jan. 2018.
[2] S. H. Islam et al., “On secrecy performance of mixed generalized Gamma and Mälaga RF–FSO variable gain relaying channel,” IEEE Access, vol. 8, pp. 104127–104138, 2020.
[3] X. Zhu and J. M. Kahn, “Free-space optical communication through atmospheric turbulence channels,” IEEE Trans. Commun., vol. 50, no. 8, pp. 1293–1300, Aug. 2002.
[4] S. M. Haas and J. H. Shapiro, “Capacity of wireless optical communications,” IEEE J. Sel. Areas Commun., vol. 21, no. 8, pp. 1346–1357, Oct. 2003.
[5] A. A. Farid and S. Hranilovic, “Outage capacity optimization for free-space optical links with pointing errors,” J. Lightw. Technol., vol. 25, no. 7, pp. 1702–1710, Jul. 2007.
[6] A. Belmonte and J. M. Kahn, “Capacity of coherent free-space optical links using diversity-combining techniques,” Opt. Exp., vol. 17, no. 15, pp. 12601–12611, 2009.
[7] A. A. Farid and S. Hranilovic, “Diversity gain and outage probability for MIMO free-space optical links with misalignment,” IEEE Trans. Commun., vol. 60, no. 2, pp. 479–487, Feb. 2012.
[8] I. S. Ansari, F. Yilmaz, and M.-S. Alouini, “Performance analysis of free-space optical links over Mälaga ($\mu$) turbulence channels with pointing errors,” IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 91–102, Jan. 2016.
[9] M. Safari and M. Uysal, “Relay-assisted free-space optical communication,” IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 5441–5449, Dec. 2008.
[10] R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and C. Castillo-Vázquez, “Ergodic capacity analysis of decode-and-forward relay-assisted FSO systems over Alpha-Mu fading channels considering pointing errors,” IEEE Photon. J., vol. 8, no. 1, Feb. 2016, Art. no. 7900611.
[11] L. Yang, M.-S. Alouini, and I. S. Ansari, “Asymptotic performance analysis of two-way relaying FSO networks with nonzero boresight pointing errors over double-generalized Gamma fading channels,” IEEE Trans. Veh. Technol., vol. 67, no. 8, pp. 7800–7805, Aug. 2018.
[12] J. Gupta, V. K. Dwivedi, and V. Karwal, “On the performance of RF–FSO system over Rayleigh and Kappa-Mu/Inverse Gaussian fading environment,” IEEE Access, vol. 6, pp. 4186–4198, 2018.
[13] Y. F. Al-Eryan, A. M. Salhah, S. A. Zummo, and M.-S. Alouini, “Two-way multiuser mixed RF/FSO relaying: Performance analysis and power allocation,” J. Opt. Commun. Netw., vol. 10, no. 4, pp. 396–408, 2018.
[14] M. I. Petkovic and Z. Txpovski, “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. 6002814.
[15] L. Yang, M. O. Hasna, and X. Gao, “Performance of mixed RF/FSO with variable gain over generalized atmospheric turbulence channels,” IEEE J. Sel. Areas Commun., vol. 33, no. 9, pp. 1913–1924, Sep. 2015.
[16] E. Balti, M. Guizani, B. Hamdaoui, and B. Khalfi, “Aggregate hardware impairments over mixed RF/FSO relaying systems with outdated CSI,” IEEE Trans. Commun., vol. 66, no. 3, pp. 1110–1123, Mar. 2018.
[17] G. T. Djordjevic, M. I. Petkovic, A. M. Cvetkovic, and G. K. Karagiannidis, “Mixed RF/FSO relay network with opportunistic scheduling and outdated channel information,” J. Lightw. Technol., vol. 34, no. 13, pp. 3259–3272, Jul. 2016.
[18] A. M. Salhah, 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 channel estimation errors,” submitted for publication.
[19] O. M. S. Al-Ebraheemy, A. M. Salhah, A. Chaaban, S. A. Zummo, and M.-S. Alouini, “Precise performance analysis of dual-hop mixed RF/FSO relay system with point-to-point FSO communication,” arXiv:1806.09666v1 [cs.IT].
[20] 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.

[21] D. R. Pattanayak, S. Rai, V. K. Dwivedi, and G. Singh, “A statistical channel model for a decode-and-forward based dual hop mixed RF/FSO relay network,” Opt. Quantum Electron., vol. 50, no. 6, pp. 1–17, 2018.

[22] N. Sharma, A. Bansal, and P. Garg, “Decode-and-forward relaying in mixed η-μ and Gamma-Gamma dual hop transmission system,” IET Commun., vol. 10, no. 14, pp. 1769–1776, 2016.

[23] L. Yang, M. O. Hasna, and I. S. Ansari, “Unified performance analysis for multiuser mixed η-μ and M-distribution dual-hop RF/FSO systems,” IEEE Trans. Commun., vol. 65, no. 8, pp. 3601–3613, Aug. 2017.

[24] Y. Zou, J. Zhu, X. Wang, and V. M. C. Leung, “Improving physical-layer security in free-space optical communications using diversity techniques,” IEEE Netw., vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[25] F. J. López-Martínez, 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. 7901017.

[26] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, “On secrecy performance of mixed η-μ fading mixed RF–FSO channel,” IEEE Photon. J., vol. 9, no. 4, Aug. 2017, Art. no. 7904814.

[27] L. Yang, T. Liu, J. Chen, and M.-S. Alouini, “Physical-layer security for mixed η-μ and M-distribution dual-hop RF/FSO systems,” IEEE Trans. Veh. Technol., vol. 67, no. 12, pp. 12427–12431, Dec. 2018.

[28] A. H. Abd El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, “Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference,” in Proc. IEEE Wireless Commun. Netw. Conf., 2017, pp. 1–6.

[29] 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.

[30] 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.

[31] N. A. Sarker and M. F. Samad, “Capacity and outage performance analysis of secure cooperative RF–FSO relay system in the presence of multiple eavesdroppers,” Phys. Commun., vol. 49, 2021, Art. no. 101477.

[32] 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.

[33] N. A. Sarker et al., “On the intercept probability and secure outage analysis of mixed (α−κ−μ)-shadowed and Málaga turbulent models,” IEEE Access, vol. 9, pp. 133849–133860, 2021.

[34] 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.

[35] H. AlQuwaiee, I. S. Ansari, and M.-S. Alouini, “On the performance of free-space optical communication systems over double generalized Gamma channel,” IEEE J. Sel. Areas Commun., vol. 33, no. 9, pp. 1829–1840, Sep. 2015.

[36] N. D. Chatzidiamantis, H. G. Sandalidis, G. K. Karagiannidis, S. A. Kotsopoulos, and M. Matthaiou, “New results on turbulence modeling for free-space optical systems,” in Proc. 17th Int. Conf. Telecommun., 2010, pp. 487–492.

[37] M. D. Yacoub, “The κ – μ distribution and the κ−μ distribution,” IEEE Antennas Propag. Mag., vol. 49, no. 1, pp. 68–81, Feb. 2007.

[38] M. A. Kashani, M. Uysal, and M. Kaveh, “A novel statistical channel model for turbulence-induced fading in free-space optical systems,” J. Lightw. Technol., vol. 33, no. 11, pp. 2303–2312, Jun. 2015.

[39] 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.

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

[41] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhattacharjee, and H. Lei, “Physical layer security of hybrid satellite-FSO cooperative systems,” J. Opt., vol. 11, no. 1, Feb. 2019, Art. no. 7900814.

[42] 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.

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

[44] A. El-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. 1554–1563, 2001.

[45] T. A. Tsiftsis, H. G. Sandalidis, G. K. Karagiannidis, and M. Uysal, “Optical wireless links with spatial diversity over strong atmospheric turbulence channels,” IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 951–957, Feb. 2009.

[46] 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.

[47] 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.

[48] A. S. M. Badrudduzza et al., “Security at the physical layer over GG fading and mEGG turbulence induced RF-UOWC mixed system,” IEEE Access, vol. 9, pp. 18123–18136, 2021.

[49] 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.

[50] A. Prudnikov, Y. Brychkov, and O. Marichev, Integrals and Series: More Special Functions, vol. 3, Pennsylvania, USA: Gordon And Breach Science Publishers, 1992.

[51] H. J. Malik, “The algebra of random variables (md springer),” New York, NY, USA: Academic, 2014.

[52] A. Badrudduzza, M. 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. 101777.

[53] 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.

[54] 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.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.