Physical Layer Security Analysis of Multi-Hop Hybrid RF/FSO System in Presence of Multiple Eavesdroppers

Dipti R. Pattanayak, *Student Member, IEEE*, Vivek K. Dwivedi, *Member, IEEE*, Vikram Karwal, *Senior Member, IEEE*, Pankaj K. Yadav, and Ghanshyam Singh

***Abstract*— In this paper, the physical layer security (PLS) analysis for a decode-and-forward (DF) protocol based multi-hop hybrid radio frequency (RF)/ free space optics (FSO) is presented. Herein, two different scenarios are considered for detecting the secured information at the destination. In the first scenario, at each hop, the received signals with higher secrecy capacity are selected. However, in the second scenario, the RF and FSO signals are simply decoded and forwarded to the next hop and selection is done at the last hop only. Each node in the system is connected to its subsequent node through parallel RF and FSO links. The FSO links and RF links are characterized by Málaga ($\mathcal{M}$) and Nakagami-m composite distributions respectively. For both scenarios, the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), intercept probability (IP), and effective secrecy throughput (EST) are obtained as performance metrics. These performance metrics are obtained by considering pointing error, different optical signal detection methods, turbulence effect, and the RF link fading parameter (m). Using the results, the security and reliability trade-off analysis is discussed for two scenarios. In addition, the asymptotic results are also obtained to study the system in depth. Further, the secrecy diversity order (SDO) and secrecy coding gain (SCG) are obtained to analyse the system in depth. Finally, Monte-Carlo Simulation is performed to verify the obtained results. The results manifest that the scenario with selection at each hop provides better secrecy performance than the scenario with selection at the last hop.**

***Index Terms*—Physical layer security, multi-hop hybrid radio frequency/free space optics, Secrecy outage probability, strictly positive secrecy capacity, intercept probability, and effective secrecy throughput, secrecy diversity order, and secrecy coding gain.**

I. Introduction

The rapid growth of number of users and the increasing demand of wireless applications in fifth generation (5G) networks, motivate the researchers to provide a network connection that guarantees high information capacity, low latency, large area coverage, huge number of user/device connection, efficient network throughput, and efficient energy consumption. As a result, these networks should be built to address issues with network stability, security, and efficiency. Security is a critical issue for 5G networks in particular [1], [2], [3]. To achieve a secure communication system, the cryptographic approach is traditionally used at higher layers of the network protocol layer [4]. As an alternative, physical layer security (PLS) [1] focuses on the channel environment with random properties such as noise and fading. As a result, an eavesdropper using a more advanced decryption technique cannot compromise the network's security. PLS allows for secure communication when the quality of the legitimate channel is higher than the wiretap channel. The primary goal of the PLS approach is to increase the system's secrecy rate. This secrecy rate is simply the difference between legitimate and wiretap link capacity.

A number of works have been proposed in the literature taking the benefits of the PLS approach into consideration. The various network architectures are studied in these studies. In 1975, Wyner initially proposed the idea of PLS [5]. Researchers have been motivated by this strategy to analyse the system from a PLS perspective for various fading channels. Later, several wireless networks adopt his concept [6]-[30]. Due to the broadcast nature of RF signals making the system unsafe, PLS for networks based on RF links has received significant attention recently. PLS analysis is performed for various fading distributions such as: generalized-K [6], Fisher-Snedecor $\mathcal{F}$ [7], Fox's H-function [8], generalized Gamma [9], α-μ [10], κ-μ [11] α-η-k-μ [12] etc.

The eavesdropper, however, has a chance to wiretap the channel because of the optical irradiance fluctuation in FSO links [13] and [14]. According to the authors of [13], laser beam divergence and turbulence-induced fading together have the unfavourable consequence of compromising the security of an FSO link. Additionally, Lopez-Martinez et al. in [13] examined the PLS for an FSO channel and came up with an expression for the probability of strictly-positive-secrecy-capacity (SPSC) when an eavesdropper is located close to either the transmitter

Manuscript received 13 October 2022; revised 19 November 2022; accepted 29 November 2022. Date of publication 5 December 2022; date of current version 22 December 2022. This work was supported in part by the University of Johannesburg, South Africa. *(Corresponding author: Vivek K. Dwivedi.)*

Dipti R. Pattanayak is with the Department of Electronics and Communication Engineering, GL Bajaj Institute of Technology and Management, Greater Noida 201306, India (e-mail: diptiranjanpattanayak@gmail.com).

Vivek K. Dwivedi, Vikram Karwal, and Pankaj K. Yadav are with the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida 201309, India (e-mail: drvivekkdwivedi@gmail.com; vikram@ieee.org; pankajkyadav@gmail.com).

Ghanshyam Singh is with the Centre for Smart Information and Communication Systems, Department of Electrical and Electronic Engineering Science, Auckland Park Kingsway Campus, University of Johannesburg, Johannesburg 2006, South Africa (e-mail: ghanshyams@uj.ac.za).

Digital Object Identifier 10.1109/JPHOT.2022.3226351

or the receiver. Ruiz et al. came to the conclusion that the eavesdropper's position and orientation have a substantial impact on secrecy performance in [14].

Similar to this, Lei et al. [15] explained that a wiretap via an FSO link is feasible if the laser beam area at the receiver site is larger than the receiver detection area. This indicates that a eavesdropper positioned behind the receiver can hear the data [15]. As a result, the authors of [16] looked at the security issue in FSO links wherein an unauthorised user could overhear the private information through a scattering channel that is not in the line of sight. The outcome demonstrates that privacy is preserved under conditions of clear visibility. The PLS is also examined in [17] when Málaga ($\mathcal{M}$) faded FSO link is taken into account. The performance metrics used in this work are the secrecy outage probability (SOP), SPSC, and average secrecy capacity (ASC). The implications of path loss conditions and boresight pointing problems on system performance are not examined. By taking into account three different plausible eavesdropping situations, Authurs' in [18] studied the secrecy performance for an FSO link. The outcomes demonstrate that the performance of secrecy is less significantly impacted by atmospheric conditions when the eavesdropper is located close to the transmitter. Authurs' in this work demonstrated the secrecy performance by considering the correlation effect. They demonstrated that the correlation has a greater influence on secrecy performance.

The authors examined the PLS for mixed RF/FSO network, taking advantage of both RF and FSO channels [19], [20], [21], [22], [23], [24], [25], [26], [28], [29], [30]. The authors of [19] and [20] considered relaying methods as a means of enhancing secrecy performance. In a mixed RF/FSO scenario, the PLS is examined for both the uplink (first hop - RF and second hop - FSO) and the downlink (first hop - FSO and second hop - RF) modes of mixed RF/FSO scenario. In the literature, few works are examined for the downlink situation in the literature, while the majority of works based on PLS are explored for the uplink scenario.

[21] examines the security-reliability trade-off (SRT) analysis of the multi-user single input multiple output (MU-SIMO) mixed RF/FSO network. The system is thoroughly investigated using both selection combining and maximal ratio combining techniques at relay and eavesdropper. As a performance metric, the outage probability, average system error probability, ergodic capacity, and intercept probability (IP) are derived. In this system, [21], a friendly jammer is also suggested to improve secrecy performance. A power allocation technique is suggested to improve the secrecy performance of this system in [22], which analyses the impact of RF co-channel interference (CCI) on SRT of MU mixed RF-FSO systems. A simpler asymptotic expression is obtained by deriving the exact closed form expression for the IP. The co-operative jamming approach is also used in this work to improve secrecy performance when CCI is present. The performance of a mixed RF/FSO uplink network's secrecy in the presence of an RF antenna-based eavesdropper is examined in reference [23]. As a performance metric, the closed-form equations for SOP and ASC are obtained for relaying schemes with constant gain and variable gain. Similarly, the PLS is examined in [24] under the assumptions of η - μ and $\mathcal{M}$ distributions for RF and FSO links respectively in in a mixed RF/FSO scenario. For both fixed gain and variable gain relaying methods, the SOP and average secrecy rate (ASR) are determined as performance measures. In [25], it is examined how secrecy outage performance is impacted by channel state information (CSI) for the RF and the FSO link. Authors in [26] analyses the PLS of a mixed RF/FSO system based on SIMO simultaneous wireless information and power transfer (SWIPT) with a fixed gain relaying method.

The secrecy performance of a hybrid satellite-FSO cooperative system is explored in [27], where the satellite links are subject to Shadowed-Rician fading and the FSO link is represented by Gamma-Gamma fading distribution. The SOP and ASC in this study are obtained by taking into account both the AF and DF relaying protocols. It is discovered that the secrecy performance for both relaying techniques primarily rely on satellite link rather than FSO link. A dual hop mixed RF/FSO downlink SWIPT system was studied by Lei $et.al.$ [28]. The effect of misalignment error, various optical signal detecting techniques, SWIPT, and number of antennas are taken into account in order to achieve the exact and asymptotic SOP. For a one-way relaying (OWR) based mixed RF/FSO downlink system [29], the SOP and ST are determined by considering for pointing error, optical signal detection techniques, turbulence severity, and RF fading parameter. The study is carried out by taking into account different scenarios, and the results are then compared to determine how well the system maintains secret. Similar work was done for two-way relaying (TWR) in [30] where it was assumed that the FSO and RF links would experience $\mathcal{M}$ and Nakagami-m distribution, respectively. Three separate situations, including an eavesdropper attack on 1) RF links only, 2) FSO links only, and 3) both FSO and RF links simultaneously, are taken into account in this. For each of these scenarios, the SOP and ST are determined as performance measures. This study shows that the system is extremely vulnerable when both eavesdroppers attempt to wiretap the legitimate links.

A. Motivation and Contribution

Relaying techniques are typically used to increase network coverage, spectrum efficiency, and power efficiency. In addition to these, the system needs high-capacity, reliable communication between users [31], which is why researchers here thoroughly examined the hybrid RF/FSO structure [31], [32], [33], [34], [35], [36], [37], [38], [39]. Environmental factors do not have the same impact on RF and FSO links. Fog and atmospheric turbulence have an impact on the FSO link's quality, but not the RF link. Similar to how RF links are vulnerable to heavy rain, FSO links are not, though. Therefore, we can combine both RF and FSO lines in simultaneously to enable the system in any atmospheric situation (i.e. hybrid connection). This arrangement may be helpful in circumstances where the transmitter and receiver are separated, such as when the source and destination base stations are situated in different cities. The direct link is regarded as being severely faded as a result. The parallel hybrid RF/FSO structure is also a suitable backhaul solution. Additionally, this network gives the fading and turbulence effect robustness. As a result, we have taken the PLS analysis for this network into consideration here. In terms of security, this kind of network [38] offers higher data rates while maintaining greater security.

In light of the aforementioned reasons, we investigate the parallel FSO/RF configuration's secrecy performance. We recently looked into a secrecy issue for two distinct scenarios, such as 1) mixed RF-hybrid RF/FSO, and 2) hybrid RF-RF/RF-FSO, in [39]. From the results, it is observed that the considered scenarios [39] provide better secrecy performance as compared to the system without hybrid structure. As a result of the discussion above, we have provided the following list of the major contributions:

1) We investigated the PLS analysis for a hybrid RF/FSO system with multiple eavesdroppers. This study aims to evaluate a multi-hop hybrid RF/FSO system's secrecy performance in the presence of several RF- and FSO-based eavesdroppers. With this context, two scenarios are considered: the secrecy is performed at each relay input of the system $i.e.$ the signal with higher secrecy capacity is selected at each relay input, and the secrecy is performed at the destination only $i.e.$, the signals received at each relay input decoded and forwarded separately, and the selection of higher secrecy capacity is performed only at the destination.
2) We obtain the closed form expressions for SOP, SPSC, and IP for both scenarios by modelling the RF links as Nakagami-m fading and the FSO links as Málaga ($\mathcal{M}$) distribution.

   The results are obtained for both scenarios by considering FSO channel parameters (pointing deflection between optical transmitter and receiver, optical signal detection methods, atmospheric turbulence condition), RF fading channel parameter (m), and number of hops used between transmitter and receiver. Additionally, we have examined how these affect the security of the system in both cases. In addition to study in depth, we have considered the boresight pointing error which is a practical problem during FSO communication. By considering this effect, we can analyse the fluctuation of laser beam at the receiver from the main channel. Due to fluctuation, the eavesdropper can get a chance to intercept the secured information.
3) The analysis of effective secrecy throughput (EST) for multihop hybrid RF/FSO systems has not yet been reported in any literature. We illustrate the trade-off between secrecy outage and secrecy rate for both cases using these EST results. For all scenarios, the trade-off between security and reliability is also demonstrated.
4) The asymptotic analysis is also thoroughly examined. The secrecy diversity order (SDO) and secrecy coding gain (SCG) are derived to analyse the system under consideration.
5) Finally, Monte-Carlo simulations are used for validation.

B. Paper Organization

The notations used in this paper are depicted in Table I. The remaining of the paper is organized as follows. Section II describes the different scenarios for the considered system. Further, in this section, the statistical characters of RF and FSO channels are described. Subsequently, the secrecy performance metrics such as: SOP, SPSC, IP, and EST are obtained in Section III. Afterwards, Section IV discusses the results obtained for the considered system models. Finally, Section V concludes the paper.

TABLE I
NOTATIONS OF THE USED PARAMETERS

Notations	
Parameter	Description
γ	Instantaneous signal to noise ratio (SNR)
$\overline{\gamma}$	Average signal to noise ratio (SNR)
μ_r	Electrical SNR of FSO link
m	Fading parameter of RF channel
α and β	Large and small scale parameters of scattering process
ξ	ξ = 1.1 and ξ = 6.7 denotes high and low pointing error
r	r = 1 and r = 2 denotes HD and IM/DD technique
N	Number of relay nodes
L	Number of hops
$\psi = 2^{NR_0}$	Instantaneous signal to noise ratio (SNR)
$\Gamma(.)$	Incomplete Gamma function [40, Eq. (8.310.1)]
$G_{p,q}^{m,n}$ [.]	Meijer's G function [40, Eq. (9.301)]

II. System and Channel Models

In this section, a multi-hop hybrid RF/FSO system with two different selection techniques are considered. Firstly, we have discussed the system model for the considered scenario and secondly, the channel model is discussed. For this purpose, the channel capacities for each existing links are derived. Afterwards, theses channel capacities are used to derive the secrecy capacities which enables to analyse the secrecy performance metrics such as SOP, SPSC, IP and EST.

A. System With Selection At Each Hop

Consider the system model of a secure data transmission as shown in Fig. 1 which is termed as multi-hop hybrid FSO/RF system. The legitimate source (S) communicates with a legitimate destination (D) via serial relay nodes (R_i with $i \in \{1, 2, 3, \ldots, N\}$). Nodes S and R_i use two different links, RF and FSO, to convey data towards D. Each hop is connected with subsequent hop through a decode-and-forward (DF) based relay. The source (S) generates two copies of different formats (RF and optical) and transmitted through RF and FSO links independently. While transmission, unauthorized nodes, $E_{RF,i}$ and $E_{FSO,i}$ with $i \in \{1, 2, 3, \ldots, N\}$, are attempting to eavesdrop the signal from RF and FSO links respectively. At the first relay (R_1), the signal with highest secrecy capacity is selected. Afterwards this selected signal again generates two copies of RF and optical signals. This process continues until the signal reaches to D. The benefits of this scenario is that at each relay point the security of information is checked and then forwarded to next relay. On the other hand, the limitation of this scenario is that the system is overburdened as each relay has to take decision during communication i.e. number of decision are more during communication. This scenario is useful only when the security of information is highly necessary.

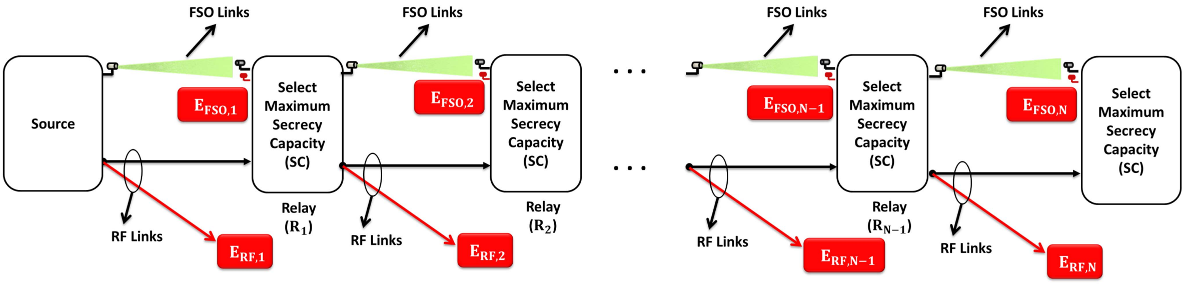

Fig. 1. Structure with the selection at each hop.

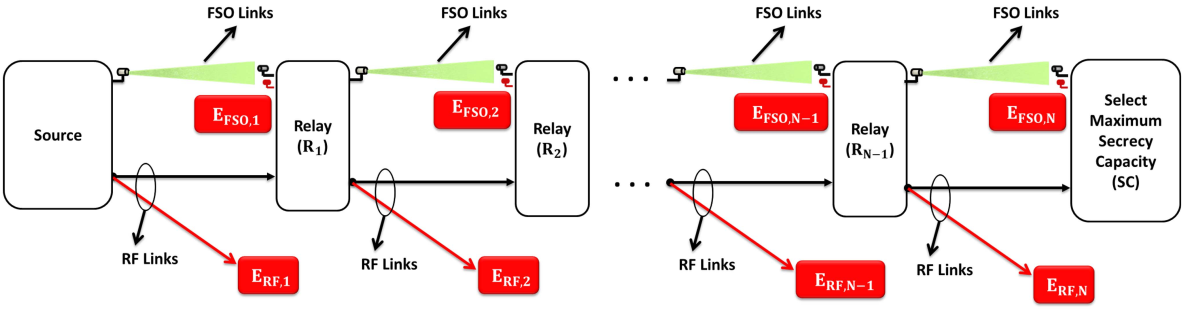

Fig. 2. Structure with the selection at destination.

B. System With Selection At Destination

Fig. 2 represents a relay assisted multi-hop RF/FSO system similar to Fig. 1. Herein, the selection of the secure signal occurs at the destination instead of each hop. More specifically, the transmitted signal is primarily received by the first relay (R_1). Thereafter, R_1 just decodes and forwards to the successive relay node. This procedure continues until both RF and optical signals reach to the destination node. Finally, at destination, between received signals, one with highest secrecy capacity is selected. In this scenario, the security of the information is not checked at each relay and due to this there is no overburden on the relay nodes. The relay nodes only decode and forward the information to the next node. This scenario is useful only when the security is not a prime concern.

C. Statistical Characteristics of RF Links

The RF links are assumed to follow the Nakagami-m distributions, m is a parameter indicating fading severity whose probability density function (*pdf*) and cumulative distribution function (*cdf*) for signal-to-noise-ratio (SNR) are given by [40]

$$f_{\gamma_j}(\gamma) = \left(\frac{m_j}{\overline{\gamma}_j}\right)^{m_j} \frac{\gamma^{(m_j-1)}}{\Gamma(m_j)} \exp\left(-\frac{m_j\gamma}{\overline{\gamma}_j}\right), \quad (1)$$

$$F_{\gamma_j}(\gamma) = 1 - \sum_{k=0}^{m_j-1} \frac{1}{k!} \left(\frac{m_j\gamma}{\overline{\gamma}_j}\right)^k \exp\left(-\frac{m_j\gamma}{\overline{\gamma}_j}\right). \quad (2)$$

where, $j \in \{R_{RF,i}, E_{RF,i}\}$.

D. Statistical Characteristics of FSO Links

The gain of FSO channel primarily consists three components: atmospheric turbulence parameter, pointing error, and path loss. In this work, we have considered the effect of non-zero boresight caused due to dynamic wind load, building sways, and thermal expansion in the high rise buildings [42]. Herein, path loss is not our prime concern. Therefore, it is considered as deterministic, which is taken as unity. FSO links are modeled by Málaga ($\mathcal{M}$) distribution with pointing errors and the *pdf* and *cdf* of γ_p can be expressed as [43]

$$f_{\gamma_p}(\gamma) = \frac{A\xi^2}{2^r\gamma} \sum_{m=1}^{\beta} b_m G_{1,3}^{3,0}\left[B\left(\frac{\gamma}{\mu_r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \xi^2+1 \\ \xi^2, \alpha, m \end{matrix}\right], \quad (3)$$

$$F_{\gamma_p}(\gamma) = \frac{A\xi^2}{2^r(2\pi)^{r-1}} \sum_{m=1}^{\beta} c_m G_{r+1,3r+1,}^{3r,1}\left[\frac{B^r\gamma}{r^{2r}\mu_r} \middle| \begin{matrix} 1, K_1 \\ K_2, 0 \end{matrix}\right]. \quad (4)$$

where $\mu_1 = \overline{\gamma}_p$ and $\mu_2 = \frac{\xi^2(1+\xi^2)^{-2}(2+\xi^2)(g+\Omega')}{\alpha^{-1}(1+\alpha)[2g(g+2\Omega')+\Omega'^2(1+\frac{1}{\beta})]}\overline{\gamma}_p$ with $p \in \{R_{FSO,i}, E_{FSO,i}\}$. $K_1 = [\Delta(r, \xi^2+1)]$, $K_2 = [\Delta(r, \xi^2)$, $\Delta(r, \alpha), \Delta(r, m)]$ where $\Delta(u, t) = \frac{t}{u}, \frac{t+1}{u}, \ldots, \frac{u+t-1}{u}$. $A = \frac{2\alpha^{\frac{\alpha}{2}}}{g^{1+\frac{\alpha}{2}} r\Gamma(\alpha)} \times \left(\frac{g\beta}{g\beta+\Omega'}\right)^{\beta+\frac{\alpha}{2}}$,$B = \frac{\xi^2\alpha\beta(g+\Omega')}{(\xi^2+1)(g\beta+\Omega')}$,$a_m =$ $\left(\begin{matrix} \beta-1 \\ m-1 \end{matrix}\right) \frac{(g\beta+\Omega')^{1-\frac{m}{2}}}{(m-1)!} (\frac{\Omega'}{g})^{m-1} (\frac{\alpha}{\beta})^{\frac{m}{2}}$,$b_m = a_m \times [\frac{\alpha\beta}{g\beta+\Omega'}]^{-\frac{\alpha+m}{2}}$, and $c_m = b_m r^{\alpha+m-1}$. The parameters used in A, B, a_m, and b_m can be obtained by referring [43].

E. Pointing Error Model With Non-Zero Boresight

The effect of boresight pointing error is significant in the analysis of FSO links [42]. The PDF of irradiance (I_P) is approximated by a modified Rayleigh distribution [42] which is given as:

$$f_p\left(I_P\right)=\frac{\xi_{mod}^2}{A_{mod}^{\xi_{mod}^2}}I_P^{\xi_{mod}^2-1} \tag{5}$$

where, $0\leq I_p\leq A_{mod}$, and $\xi_{mod}=\frac{w_{z,eq}}{2\sigma_{mod}}$. The equivalent beam radius at the receiver is given by $w_{z,eq}^2=\frac{\sqrt{\pi}erf(v)w_z^2}{2v\exp(-v^2)}$ with $erf(.)$ is the error function and $v=\frac{\sqrt{\pi}a}{\sqrt{2}w_z}$. w_z and a are the receiver plane Gaussian beam radius and receiver aperture radius respectively. $A_0=[erf(v)]^2$ is the power collected at the receiver's centre at $\mathrm{r}=0$. From [42], $\sigma_{mod}=\left(\frac{3\mu_x^2\sigma_x^4+3\mu_y^2\sigma_y^4+\sigma_x^6+\sigma_y^6}{2}\right)^{\frac{1}{6}}$. $A_{mod}=A_0exp\left(\frac{1}{\xi_{mod}^2}-\frac{1}{2\xi_x^2}-\frac{1}{2\xi_y^2}-\frac{\mu_x^2}{2\xi_x^2\sigma_x^2}-\frac{\mu_y^2}{2\xi_y^2\sigma_y^2}\right)$, where $\xi_x=\frac{w_{z,eq}}{2\sigma_x}$ and $\xi_y=\frac{w_{z,eq}}{2\sigma_y}$.

III. Secrecy Performance Analysis

To analyse the systems in depth, we have to obtain some preliminaries regarding the secrecy performance which includes instantaneous channel capacities. To do this, the secrecy capacities for each existing legitimate link is obtained. Thereafter, the global secrecy rate for these systems are obtained.

The instantaneous SNR at $R_{RF,i}, E_{RF,i}, R_{FSO,i}$, and $E_{FSO,i}$ are denoted by $\gamma_{R_{RF,i}}$, $\gamma_{E_{RF,i}}$, $\gamma_{R_{FSO,i}}$, and $\gamma_{E_{FSO,i}}$ respectively. Now, to obtain the secrecy capacity, we have to obtain the channel capacities for legitimate as well as eavesdropper links. The channel capacity for legitimate and eavesdropper links are given by:

For legitimate links:

$$C_{RF,i}=\frac{1}{N}\log_2\left(1+\gamma_{RF,i}\right), C_{FSO,i}=\frac{1}{N}\log_2\left(1+\gamma_{FSO,i}\right)$$

For eavesdropper links:

$$C_{E_{RF,i}}=\frac{1}{N}\log_2\left(1+\gamma_{E_{RF,i}}\right), C_{E_{FSO,i}}=\frac{1}{N}\log_2\left(1+\gamma_{E_{FSO,i}}\right)$$

Further, we can obtain the secrecy capacities for RF and FSO links using the channel capacities, in i^{th} hybrid hop are given below:

$$C_{RF,i}^{Sec}=max\left\{C_{RF,i}-C_{E_{RF,i}},0\right\}, \tag{6}$$

and

$$C_{FSO,i}^{Sec}=max\left\{C_{FSO,i}-C_{E_{FSO,i}},0\right\}. \tag{7}$$

A. Secrecy Outage Probability (SOP) Analysis

The SOP can be defined as the probability that the instantaneous global secrecy rate ($C_{Hyb,i}^{Sec}=max\{max\{C_{RF,i}^{Sec},C_{FSO,i}^{Sec}\},0\}$) falls below a predetermined secrecy threshold R_0 (in bps/Hz) [6] .[1]

1) System With Selection At Each Hop:

Theorem 1: The SOP for the system with selection at each hop can be expressed as (8), shown at the bottom of this page, where

$$\Phi_0=\left(\frac{m_i\psi}{\overline{\gamma}_{RF,i}}\right)^k\left(\frac{m_i}{\overline{\gamma}_{E_{RF,i}}}\right)^{m_i}\frac{\Gamma\left(m_i+k\right)}{\left(\frac{m_i\psi}{\overline{\gamma}_{RF,i}}+\frac{m_i}{\overline{\gamma}_{E_{RF,i}}}\right)^{m_i+k}},$$

$$\Phi_1=\left(\frac{\xi^2A}{2^r\left(2\pi\right)^{r-1}}\right)^2\sum_{m_1=1}^{\beta_1}b_{m_1}r^{\alpha+m_1-1}\sum_{m_2=1}^{\beta_2}b_{m_2}r^{\alpha+m_2-1}$$

Proof: The end-to-end secrecy outage for scenario-1 can be expressed as (9).

$$\begin{aligned}P_1^{SOP}\left(R_0\right)&=Pr\left\{min\left(C_{Hyb,1}^{Sec},C_{Hyb,2}^{Sec},\ldots,C_{Hyb,N}^{Sec}\right)<R_0\right\}\\&=1-\prod_{i=1}^{N}Pr\left\{C_{Hyb,i}^{Sec}\geq R_0\right\}\\&=1-\prod_{i=1}^{N}\left(1-Pr\left\{C_{Hyb,i}^{Sec}<R_0\right\}\right)\\&=1-\prod_{i=1}^{N}\left(1-Pr\left\{max\left\{C_{RF,i}^{Sec},C_{FSO,i}^{Sec}\right\}<R_0\right\}\right)\end{aligned} \tag{9}$$

Further, we can proceed as

$$\begin{aligned}&Pr\left\{max\left\{C_{RF,i}^{Sec},C_{FSO,i}^{Sec}\right\}<R_0\right\}\\&\quad=Pr\left\{C_{RF,i}^{Sec}<R_0\right\}Pr\left\{C_{FSO,i}^{Sec}<R_0\right\},\end{aligned} \tag{10}$$

Using (6) and (7) in (10), we have

$$\begin{aligned}&Pr\left\{max\left\{C_{RF,i}^{Sec},C_{FSO,i}^{Sec}\right\}<R_0\right\}\\&\quad=Pr\left\{\left(\frac{1+\gamma_{RF,i}}{1+\gamma_{E_{RF,i}}}\right)<\psi\right\}Pr\left\{\left(\frac{1+\gamma_{FSO,i}}{1+\gamma_{E_{FSO,i}}}\right)<\psi\right\}\end{aligned} \tag{11}$$

where $\psi=2^{NR_0}$, denotes the secrecy threshold. Using the tight approximation $\frac{1+m}{1+n}\backsimeq\frac{m}{n}$ [44], [45] equation (11) can be approximated as

$$\begin{aligned}&Pr\left\{max\left\{C_{RF,i}^{Sec},C_{FSO,i}^{Sec}\right\}<R_0\right\}\\&=\backsimeq Pr\left\{\gamma_{RF,i}<\psi\gamma_{E_{RF,i}}\right\}Pr\left\{\gamma_{FSO,i}<\psi\gamma_{E_{FSO,i}}\right\}\\&=\backsimeq\tau_1\times\tau_2\end{aligned} \tag{12}$$

Evaluation of τ_1*:* We can express τ_1 in the integral form as

$$\tau_1\backsimeq\int_0^\infty F_{\gamma_{RF,i}}\left(\psi\gamma_{E_{RF,i}}\right)f_{E_{RF,i}}\left(\gamma_{E_{RF,i}}\right)d\gamma_{E_{RF,i}} \tag{13}$$

$$P_1^{SOP}\left(R_0\right)=1-\prod_{i=1}^{N}\left(1-\left\{1-\sum_{k=0}^{m_i-1}\frac{1}{k!}\frac{1}{\Gamma\left(m_i\right)}\Phi_0\right\}\left\{\Phi_1G_{4r+1,4r+1}^{3r+1,3r}\left[\frac{\overline{\gamma}_{FSO,i}}{\psi\overline{\gamma}_{E_{FSO,i}}}\left|\begin{matrix}1-K_2,1,K_1\\K_2,0,1-K_1\end{matrix}\right.\right]\right\}\right) \tag{8}$$

[1] The secrecy threshold at each R_i is assumed to be equal.

Plugging (3) and (4) in (13), we have

$$\tau_1 = 1 - \sum_{k=0}^{m-1} \frac{1}{k!} \left(\frac{m\psi}{\overline{\gamma}_{RF,i}}\right)^k \left(\frac{m}{\overline{\gamma}_{E_{RF,i}}}\right)^m \frac{1}{\Gamma(m)} \int_0^\infty \gamma_{E_{RF,i}}^{(m+k-1)} \exp\left(-\frac{m\gamma_{E_{RF,i}}}{\overline{\gamma}_{E_{RF,i}}} - \frac{m\psi\gamma_{E_{RF,i}}}{\overline{\gamma}_{RF,i}}\right) d\gamma_{E_{RF,i}}, \tag{14}$$

Using the integral $\int_0^\infty x^{a-1}\exp(-bx) = \frac{\Gamma(a)}{b^a}$ in (14), the solution for τ_1 can be written as

$$\tau_1 = 1 - \sum_{k=0}^{m-1} \frac{1}{k!} \left(\frac{m\psi}{\overline{\gamma}_{RF,i}}\right)^k \left(\frac{m}{\overline{\gamma}_{E_{RF,i}}}\right)^m \frac{1}{\Gamma(m)} \times \frac{\Gamma(m+k)}{\left(\frac{m\psi}{\overline{\gamma}_{RF,i}} + \frac{m}{\overline{\gamma}_{E_{RF,i}}}\right)^{m+k}}. \tag{15}$$

Evaluation of τ_2*:* Similarly, the integral for τ_2 can be expressed as

$$\tau_2 = \int_0^\infty F_{\gamma_{FSO,i}}\left(\psi\gamma_{E_{FSO,i}}\right) f_{E_{FSO,i}}\left(\gamma_{E_{FSO,i}}\right) d\gamma_{E_{FSO,i}}, \tag{16}$$

Upon substituting (7) and (8) in (16), and Using [43, Eq. (07.34.21.0013.01)], the closed form expression of (16) can be obtained as

$$\tau_2 = \left(\frac{\xi^2 A}{2^r(2\pi)^{r-1}}\right)^2 \sum_{m_1=1}^{\beta_1} b_{m_1} r^{\alpha+m_1-1} \sum_{m_2=1}^{\beta_2} b_{m_2} r^{\alpha+m_2-1} \times G_{4r+1,4r+1}^{3r+1,3r}\left[\frac{\overline{\gamma}_{FSO,i}}{\psi\overline{\gamma}_{E_{FSO,i}}}\left|\begin{matrix} 1-K_2, 1, K_1 \\ K_2, 0, 1-K_1\end{matrix}\right.\right] \tag{17}$$

Remark 1: The SOP ($P_1^{SOP}(R_0)$) is a monotonously increasing function with respect to secrecy threshold (R_0). Thus, the minimum of the $P_1^{SOP}(R_0)$ is given by $P_1^{SOP\_min} = P_1^{SOP}(R_0 = 0)$ and the maximum of the SOP is obtained by $P_1^{SOP\_max} = P_1^{SOP}(R_0 \to \infty)$.

2) Asymptotic Secrecy Outage Probability ($P_1^{SOP,\infty}(R_0)$ *Analysis:* The derived exact SOP expression does not provide much insight. In order to obtain useful insights on the impact of different parameters on the SOP, herein, an asymptotic analysis is carried out for scenario-1. To do this, we have expanded the SOP result in high-SNR regime.

Corollary 1: The final asymptotic expression of SOP for scenario-1 is given by

$$P_1^{SOP,\infty}(R_0) = 1 - \prod_{i=1}^{N}\left(1 - \left\{\left(\frac{\overline{\gamma}_{E_{RF,i}}}{\overline{\gamma}_{RF,i}}\right)^m \frac{\psi^m\Gamma(2m)}{m!\Gamma(m)}\right\} \times \left\{\Phi_1 \times \sum_{k=1}^{3r}\left(\frac{\overline{\gamma}_{FSO,i}}{\overline{\gamma}_{E_{FSO,i}}\psi}\right)^{K_{3,k}-1} \Phi_2\right\}\right). \tag{18}$$

where

$$\Phi_2 = \frac{\prod_{l=1;l\neq k}^{3r}\Gamma\left(K_{3,k} - K_{3,l}\right)}{\prod_{l=3r+1}^{4r+1}\Gamma\left(1 + K_{3,l} - K_{4.k}\right)} \times \frac{\prod_{l=1}^{3r+1}\Gamma\left(1 + K_{4,l} - K_{3.k}\right)}{\prod_{l=3r+2}^{4r+1}\Gamma\left(K_{3,k} - K_{4.l}\right)}$$

Proof: From (9), the asymptotic expression for $P_1^{SOP}(R_0)$ is obtained as

$$P_1^{SOP,\infty}(R_0) \backsimeq 1 - \prod_{i=1}^{N}\left(1 - \tau_{1,i}^\infty \tau_{2,i}^\infty\right), \tag{19}$$

where, $\tau_{1,i}^\infty$ and $\tau_{2,i}^\infty$ are belong to i^{th} RF and FSO links respectively.

Evaluation of τ_1^∞*:* Invoking the expression of τ_1 in (13), the asymptotic expression at high SNR can be written as

$$\tau_1^\infty \backsimeq \int_0^\infty F_{\gamma_{RF,i}}^\infty\left(\psi\gamma_{E_{RF,i}}\right) f_{E_{RF,i}}\left(\gamma_{E_{RF,i}}\right) d\gamma_{E_{RF,i}}, \tag{20}$$

To obtain $F_{\gamma_{RF,i}}^\infty(\psi\gamma_{E_{RF,i}})$, first we have to use $\lim_{\overline{\gamma}_{RF,i}\to\infty}\exp(\frac{-m\gamma_{E_{RF,i}}}{\overline{\gamma}_{RF,i}}) = 1$ in (1) to get $f_{\gamma_{RF,i}}^\infty(\gamma) = (\frac{m}{\overline{\gamma}_{RF,i}})^m \frac{\gamma_{E_{RF,i}}^{m-1}}{\Gamma(m)}$. Thereafter, integrating $f_{\gamma_{RF,i}}^\infty(\gamma)$, we obtain

$$F_{RF,i}^\infty(\gamma) = \left(\frac{m}{\overline{\gamma}_{RF,i}}\right)^m \frac{\gamma_{E_{RF,i}}^m}{m!}. \tag{21}$$

Now, inserting (21) and (1) in (20), and using the identity $\int_0^\infty x^{a-1}\exp(-bx) = \frac{\Gamma(a)}{b^a}$, the final expression for τ_1^∞ is obtained as

$$\tau_1^\infty \approx \left(\frac{\overline{\gamma}_{E_{RF,i}}}{\overline{\gamma}_{RF,i}}\right)^m \frac{\psi^m\Gamma(2m)}{m!\Gamma(m)}. \tag{22}$$

Evaluation of τ_2^∞*:* Further, to determine τ_2^∞, we have to expand the Meijer's G-function involved in (17) at high SNR ($\overline{\gamma}_{FSO,i} \to \infty$). By making use of asymptotic expression of Meijer's G-function [40 41], the asymptotic expression for τ_2^∞ is obtained as

$$\tau_2^\infty \backsimeq \left(\frac{\xi^2 A}{2^r(2\pi)^{r-1}}\right)^2 \sum_{m_1=1}^{\beta_1} b_{m_1} r^{\alpha+m_1-1} \sum_{m_2=1}^{\beta_2} b_{m_2} r^{\alpha+m_2-1} \times \sum_{k=1}^{3r}\left(\frac{\overline{\gamma}_{FSO}}{\overline{\gamma}_{E_{FSO}}\psi}\right)^{K_{3,k}-1} \frac{\prod_{l=1;l\neq k}^{3r}\Gamma\left(K_{3,k} - K_{3,l}\right)}{\prod_{l=3r+1}^{4r+1}\Gamma\left(1+K_{3,l} - K_{4.k}\right)} \times \frac{\prod_{l=1}^{3r+1}\Gamma\left(1 + K_{4,l} - K_{3.k}\right)}{\prod_{l=3r+2}^{4r+1}\Gamma\left(K_{3,k} - K_{4.l}\right)} \tag{23}$$

where $K_{i,j}$ denotes the j^{th} term of K_i and $i \in \{3, 4\}$ with $K_3 = [1 - \triangle(r,\xi^2), 1 - \triangle(r,\alpha), 1 - \triangle(r,m_1), 1, \triangle(r, 1+\xi^2)]$ and $K_4 = [\triangle(r,\xi^2), \triangle(r,\alpha), \triangle(r,m_2), 0, 1 - \triangle(r, 2-\xi^2)]$. Upon substituting (22) and (23) in (19), we obtain the asymptotic expression for scenario-1.

The closed-form expressions enable us to analyze the performance of the system. As the expression contains complex function like Meijer's G function, it is difficult to scrutinize the effect of parameters involved in FSO and RF links on the overall performance of the system. Therefore, the closed form expression is derived at high SNR regime. In addition, due to the complex expressions involved, it is difficult to analyze effect of parameters related to FSO and RF links on the overall performance of the system. Thus in the sequel, the asymptotic behaviour of the overall system is derived by considering one link at a time. To do this, we have considered two different cases:

a) SOP is dominated by FSO link: This happens when FSO link is much prone to eavesdropping due to high pointing deflection and strong turbulence condition. This case arises when $\bar{\gamma}_{FSO,i} \rightarrow \infty$ by limiting the $\bar{\gamma}_{RF,i}$. In this case the hybrid model will employ the FSO link for transmitting the information confidentially. At that time the RF link is not utilized for secure information transmission. Therefore, (19) is reduced to $P_1^{SOP,\infty}(R_0) \backsimeq 1 - \prod_{i=1}^{N}(1 - \tau_{2,i}^{\infty})$. Using the binomial expansion of $(1-x)^n$ and discarding the higher order terms, the above equation can be expressed as $P_1^{SOP,\infty}(R_0) \backsimeq N \times \tau_2^{\infty}$. The asymptotic secrecy outage probability is generally expressed as $P_1^{SOP,\infty}(R_0) \approx (G_c^{Sec_{FSO}} \bar{\gamma}_{FSO})^{-G_d^{Sec_{FSO}}}$, where $G_c^{Sec_{FSO}}$ and $G_d^{Sec_{FSO}}$ are the SCG and SDO related to the system. The asymptotic expression is dominated by $\min(\frac{\xi^2}{r}, \frac{\alpha}{r}, \frac{\beta}{r})$ which is termed as SDO. Herein, it can be observed that the SDO depends on the fading parameters (α and m) and pointing error (ξ). The SCG is given by $G_c^{Sec_{FSO}} = \frac{1}{\bar{\gamma}_{E_{FSO}}\psi}\left\{N \sum_{k=1}^{3r} \Phi_1 \Phi_2\right\}^{\frac{1}{K_{3,k}-1}}$. One remarkable point is that the SCG depends on the number of relays considered in the system (N)

b) SOP is dominated by RF link: This happens when RF link is much prone to eavesdropping. When $\bar{\gamma}_{RF,i} \rightarrow \infty$ by limiting the $\bar{\gamma}_{FSO,i}$, the considered hybrid model utilizes the RF link for transmitting the information confidentially. Therefore, (19) is reduced to $P_1^{SOP,\infty}(R_0) \backsimeq N \times \tau_1^{\infty}$. Following the general expression of asymptotic form *i.e.* $P_1^{SOP,\infty}(R_0) \approx (G_c^{Sec_{RF}} \bar{\gamma}_{RF})^{-G_d^{Sec_{RF}}}$, we can obtain $G_d^{Sec_{RF}} = m$ and $G_c^{Sec_{RF}} = \frac{1}{\bar{\gamma}_{E_{RF,i}}}(\frac{N\Gamma(2m)}{m!\Gamma(m)})^{-\frac{1}{m}}$. Herein, the SDO depends on the fading parameter of RF link (m). As mentioned in earlier case, herein also the SCG depends on the number of relays considered in the system (N).

3) System With Selection At the Destination:

Theorem 2 : The end-to-end secrecy outage for this scenario can be expressed as (25)

$$P_2^{SOP}(R_0) = \left[1 - \prod_{i=1}^{N}\left(\sum_{k=0}^{m_i-1} \frac{1}{k!}\left(\frac{m_i\psi}{\overline{\gamma}_{RF,i}}\right)^{k}\left(\frac{m_i}{\overline{\gamma}_{E_{RF,i}}}\right)^{m_i}\Phi_0\right)\right] \times \left[1 - \prod_{i=1}^{N}\left(1 - \Phi_1 \times \sum_{k=1}^{3r}\left(\frac{\overline{\gamma}_{FSO,i}}{\overline{\gamma}_{E_{FSO,i}}\psi}\right)^{K_{3,k}-1}\Phi_2\right]\right) \tag{24}$$

Proof: The SOP for scenario-2, is derived as given in (25), shown at the bottom of this page. Further, (25) can be expressed in integral form as

$$P_2^{SOP}(R_0) \backsimeq \left[1 - \prod_{i=1}^{N}\left(1 - \int_0^{\infty} F_{\gamma_{RF,i}}\left(\psi\gamma_{E_{RF,i}}\right) f_{E_{RF,i}}(\gamma_{E_{RF,i}})\, d\gamma_{E_{RF,i}}\right)\right] \times \left[1 - \prod_{i=1}^{N}\left(1 - \int_0^{\infty} F_{\gamma_{FSO,i}}\left(\psi\gamma_{E_{FSO,i}}\right) f_{E_{FSO,i}}\left(\gamma_{E_{FSO,i}}\right) d\gamma_{E_{FSO,i}}\right)\right] \tag{26}$$

or

$$P_2^{SOP}(R_0) \backsimeq \left[1 - \prod_{i=1}^{N}(1 - \tau_{1,i})\right]\left[1 - \prod_{i=1}^{N}(1 - \tau_{2,i})\right] \tag{27}$$

Using the solution involved in (15) and (17) in (27), we obtain the closed form solution for $P_2^{SOP}(R_0)$.

4) Asymptotic Secrecy Outage Probability ($P_2^{SOP,\infty}(R_0)$) Analysis: From (27), the asymptotic expression for $P_2^{SOP}(R_0)$ is obtained as

$$P_2^{SOP,\infty}(R_0) \backsimeq \left[1 - \prod_{i=1}^{N}\left(1 - \tau_{1,i}^{\infty}\right)\right]\left[1 - \prod_{i=1}^{N}\left(1 - \tau_{2,i}^{\infty}\right)\right] \tag{28}$$

Afterwards, plugging (22) and (23) in (28), we can get the necessary asymptotic result for scenario-2. In a similar manner, we can obtain the diversity order and coding gain for this case as well which are omitted due to space limitations.

B. Strictly Positive Secrecy Capacity (SPSC) Analysis

The SPSC Probability occurs when the SNR of the legitimate channels has a better SNR than the eavesdropper channel [6].

$$\begin{aligned} P_2^{SOP}(R_0) &= Pr\left\{max\left\{min\left(C_{RF,1}^{Sec}, C_{RF,2}^{Sec}, \ldots, C_{RF,N}^{Sec}\right), min\left(C_{FSO,1}^{Sec}, C_{FSO,2}^{Sec}, \ldots, C_{FSO,N}^{Sec}\right)\right\} < R_0\right\} \\ &= Pr\left\{min\left(C_{RF,1}^{Sec}, C_{RF,2}^{Sec}, \ldots, C_{RF,N}^{Sec}\right) < R_0\right\} Pr\left\{min\left(C_{FSO,1}^{Sec}, C_{FSO,2}^{Sec}, \ldots, C_{FSO,N}^{Sec}\right) < R_0\right\} \\ &= \left[1 - \prod_{i=1}^{N}\left(1 - Pr\left\{C_{RF,i}^{Sec} < R_0\right\}\right)\right]\left[1 - \prod_{i=1}^{N}\left(1 - Pr\left\{C_{FSO,i}^{Sec} < R_0\right\}\right)\right] \\ &\backsimeq \left[1 - \prod_{i=1}^{N}\left(1 - Pr\left\{\gamma_{RF,i} < \psi\gamma_{E_{RF,i}}\right\}\right)\right]\left[1 - \prod_{i=1}^{N}\left(1 - Pr\left\{\gamma_{FSO,i} < \psi\gamma_{E_{FSO,i}}\right\}\right)\right] \end{aligned} \tag{25}$$

This metric is used to emphasize the existence of secrecy capacity in the system.

1) System With Selection At Each Hop: From the expression of SOP, we can obtain the SPSC for scenario-1 as [6]

$$P_1^{SPSC} = 1 - P_1^{SOP} \left(R_0 = 0\right) \tag{29}$$

Correspondingly, the asymptotic expansion is expressed as

$$P_1^{SPSC,\infty} \simeq 1 - P_1^{SOP,\infty} \left(R_0 = 0\right) \tag{30}$$

2) System With Selection At the Destination: Herein, the SPSC for scenario-2 can be formulated as

$$P_2^{SPSC} = 1 - P_2^{SOP} \left(R_0 = 0\right) \tag{31}$$

The asymptotic expression of SPSC for scenario-2 can be obtained

$$P_2^{SPSC,\infty} \simeq 1 - P_2^{SOP,\infty} \left(R_0 = 0\right) \tag{32}$$

C. Intercept Probability (IP) Analysis

Intercept Probability is defined as the probability that the main link capacity falls below that of the eavesdropper link channel capacity [47]. In other words, intercept event occurs when the secrecy capacity falls below zero [48]. Moreover, this metric provides the information regarding the probability of successful eavesdropping in the system.

1) System With Selection At Each Hop: From the expression of SOP, we can obtain the IP for scenario-1 as [6]

$$P_1^{IP} = P_1^{SOP} \left(R_0 = 0\right) \tag{33}$$

Correspondingly, the asymptotic expansion is expressed as

$$P_1^{IP,\infty} = P_1^{SOP,\infty} \left(R_0 = 0\right) \tag{34}$$

2) System With Selection At the Destination: The IP for scenario-2 can be formulated as

$$P_2^{IP} = P_2^{SOP} \left(R_0 = 0\right) \tag{35}$$

The asymptotic expression of IP for scenario-2 can be obtained

$$P_2^{IP,\infty} = P_2^{SOP,\infty} \left(R_0 = 0\right) \tag{36}$$

D. Effective Secrecy Throughput (EST) Analysis

The effective secrecy throughput is defined as the average rate of secure information transmitted from one legitimate node to another [49]. In other words, this metric quantifies the average amount of securely transmitted information. It also provides the trade-off between secrecy outage and secrecy rate which is depicted in the result section.

1) System With Selection At Each Hop: EST can be defined as the product of secrecy rate and secure transmission probability. Mathematically, EST for this scenario is expressed as [49]

$$EST_1 = R_0 \left(1 - P_1^{SOP} \left(R_0\right)\right), \tag{37}$$

2) System With Selection At Destination: For scenario-2, the EST is obtained as

$$EST_2 = R_0 \left(1 - P_2^{SOP} \left(R_0\right)\right) \tag{38}$$

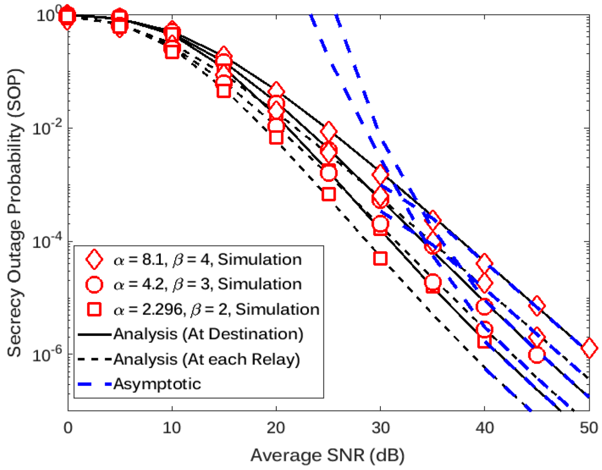

Fig. 3. SOP versus $\overline{\gamma}$ with $m = 1$, $L = 3$.

Remark 2: From (37) and (38), it can be noticed that EST first increases and then decreases with respect to increase in R_0. Here we can observe that the EST is influenced by the tradeoff between secrecy rate and SOP i.e. when the R_0 is too small, the SOP is also small but the EST is still low. Again when R_0 is too large, the system cannot afford a reliable and secure communication which leads to poor EST.

Remark 3: For $N = 1$, one can easily find that the selection of signal at each hop is same as the selection at destination for all performance metrics (SOP, SPSC, IP, and EST).

IV. Result and Discussion

In this section, we present the analytical results for two different scenarios of multi-hop hybrid RF/FSO systems. The results are obtained by assuming the best signal detection at each hop and destination separately and also compared among two considered scenarios. Additionally, to get more insight, the asymptotic and Monte-Carlo simulation results are obtained. Without loss of generality, it is assumed that: $\overline{\gamma}_{RF,i} = \overline{\gamma}_{FSO,i} = \overline{\gamma}_i$ and $\overline{\gamma}_{E_{RF,i}} = \overline{\gamma}_{E_{FSO,i}} = \overline{\gamma}_{E,i} = 0$ dB if not mentioned. Performance of the scenarios are investigated by assuming different fading parameters, optical signal detection schemes, pointing error, and number of hops used for information transmission. For Monte-carlo simulation purpose, referring [43], [50] and [51], the FSO link is modeled with a link length of $l = 1$ km and wavelength of $\lambda = 785$ nm that gives $k_w = 2\pi/\lambda$. The refraction structure parameter C_n^2 is taken as $C_n^2 = 1.23 \times 10^{-13} m^{-2/3}$, $C_n^2 = 10^{-11} m^{-2/3}$, and $C_n^2 = 2.8 \times 10^{-14} m^{-2/3}$. Utilizing these values, we can obtain the Rytov variance as $\sigma_R^2 = C_n^2 k_w^{7/6} l^{11/6}$. Subsequently the atmospheric fading parameter is obtained as ($\alpha = 2.296; \beta = 2$), ($\alpha = 4.2; \beta = 3$) and ($\alpha = 8.1; \beta = 4$). Unless otherwise stated, R_0 is set to be 1 bits/sec/Hz. During analysis, we assumed two different optical signal detection techniques (IM/DD and HD) and pointing error ($\xi = 6.7$ (negligible pointing error) and $\xi = 1.1$ (high pointing error)).

Fig. 3 is plotted for SOP versus $\overline{\gamma}$. This figure illustrates how atmospheric turbulence condition influences the secrecy

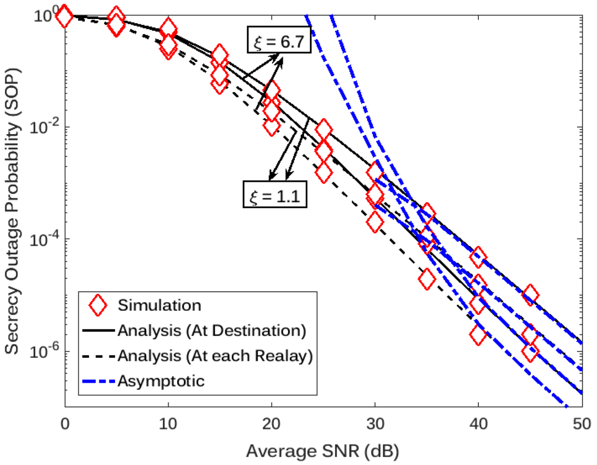

Fig. 4. SOP versus $\overline{\gamma}$ for different value of ξ .

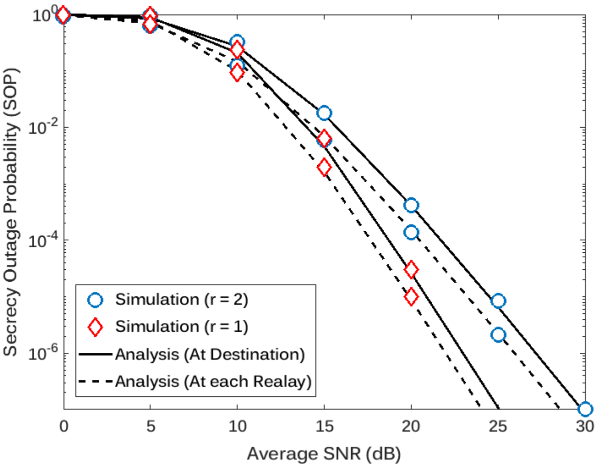

Fig. 5. SOP versus $\overline{\gamma}$ for different value of r.

of the considered scenarios. From this figure, it can be observed that, for both scenarios secrecy performance gets better with decrease in turbulence strength. This is due to the atmospheric turbulence induces a random fluctuation on the optical irradiance at the receiver. Stronger turbulence implies a larger fluctuation in the SNR; thus, the eavesdropper can get a chance to receive the secured optical signal. Furthermore, it is shown that the system with selection at each hop has better performance than the system with selection at destination. This is because, in scenario-1, between FSO and RF signals, the signal with higher secrecy capacity is detected at each hop and then forwarded to next hop. On the other hand, in scenario-2, selection of best signal among FSO and RF signals occurs at destination, rather than in each hop.

In Fig. 4, the SOP is investigated with respect to $\overline{\gamma}$ by considering different values of ξ. The results in Fig. 4 again show that the scenario-1 provides better performance as compared to other one for both $\xi = 1.1$ and $\xi = 6.7$. This is due to the same reason as analyzed for the Fig. 3. This figure also shows that, for both scenarios, the secrecy performance gets better when the value of ξ is more (low pointing error). For example, in scenario-1, when the pointing error decreases (i.e. value of ξ increases from 1.1 to 6.7) the SOP of scenario-1 decreases from 1.053×10^{-4} to 2.246×10^{-5} and the SOP of scenario-2 decreases from 3.070×10^{-4} to 6.692×10^{-5}. This is because, high pointing deflection makes a favourable condition for eavesdropper to detect the secured information. In other words, the higher value of ξ means less pointing deflection between transmitter and receiver ends. Therefore, the intended receiver will get more optical power and the eavesdropper node hardly gets the optical power from the main channel.

Fig. 5 depicts the SOP for different values of r. The plots for this figure is obtained by considering $\alpha = 4.2$, $\beta = 3$, $m = 3$, $\xi = 1.1$, and $L = 3$. It can be observed that the SOP decreases for less value of r (i.e. HD scheme). Moreover it is noticed that the scenario-1 has better performance as compared to scenario-2 for both IM/DD and HD schemes.

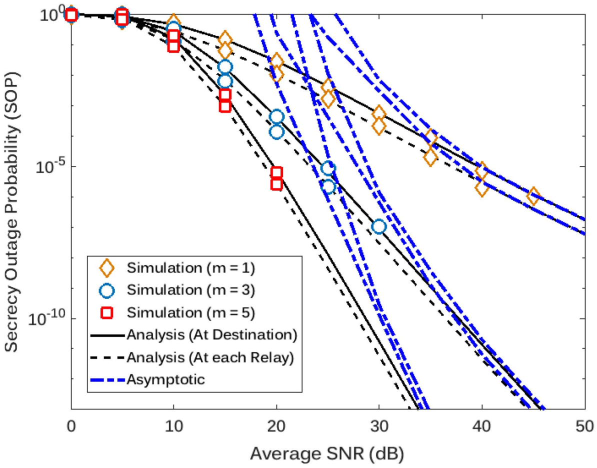

Fig. 6. SOP versus $\overline{\gamma}$ for different level of fading severity.

Further, the SOP is obtained by considering the effect of RF channel parameter m. To do this, in Fig. 6, the SOP is obtained for different values of m. The parameters for this plot is set to be $\alpha = 4.2$, $\beta = 3$, $r = 2$, $\xi = 6.7$, and $L = 3$. The result shows that the secrecy performance gets better with respect to increase in the value of m. This is because the value of m defines the shadowing level of the RF link. As the value of m increases the shadowing phenomenon gets lighter in the system.

Moreover, the secrecy performance is analysed by considering number of hops used in the system. Therefore, in Fig. 7, we obtain the SOP versus $\overline{\gamma}$ for $L = 1, 3, 5$ with $\alpha = 2.296$, $\beta = 2$, $r = 2$, $m = 2$, and $\xi = 1.1$. As can be seen, the SOP of scenario-1 and scenario-2 degrades by increasing the number of hops. According to the definition of SOP in series relaying scenario, the system is in outage even if one hop undergoes outage. Thus, increase in number of hops increases the probability of secrecy outage. It can also be noticed that, for a target SOP, the average SNR difference between the case $L = 1$ and $L = 3$ is more than the case $L = 3$ and $L = 5$. For a particular value of SOP, it can be observed that the $\overline{\gamma}$ difference is considerably

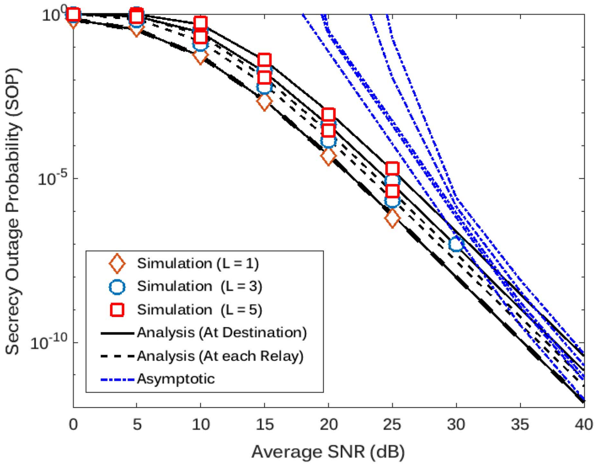

Fig. 7. SOP versus $\overline{\gamma}$ for various number of hops.

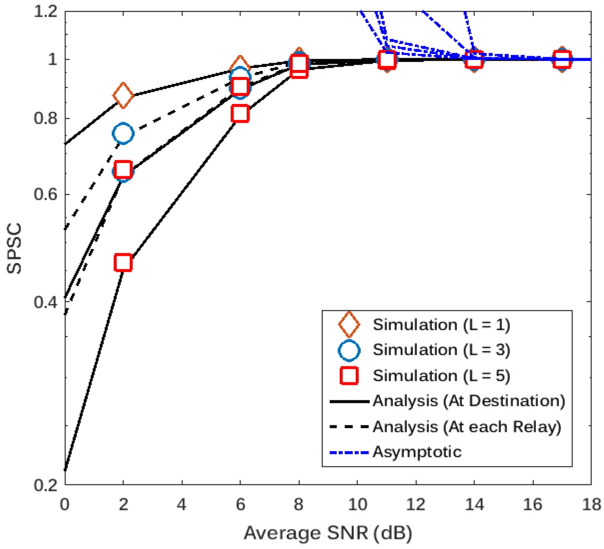

Fig. 8. SPSC versus $\overline{\gamma}$ for various number of hops.

less as number of hops are increasing. At wide range of target SOP, the same SOP difference values can be observed. In series relaying structure, the secrecy performance degrades by relay addition. However, because $\overline{\gamma}$ difference values at different target SOP are the same, only constant amount of consumed power should be added to compensate this performance degradation, and additional processing is not required to adjust this amount of power adaptively.

From Fig. 3–Fig. 7, it is observed that the SOP improves as $\overline{\gamma}$ increases because the channel condition of legitimate links are superior than eavesdropper links. Moreover, in these plots the asymptotic results fits with the analytical result at higher SNR regime.

Fig. 8 illustrates the SPSC versus $\overline{\gamma}$ for $\alpha = 2.296$, $\beta = 2$, $r = 2$, $m = 3$, $\xi = 6.7$ and $\overline{\gamma}_E = 0$ dB. This figure is plotted for various number of hops (L). As discussed before, herein also the SPSC gets better as legitimate links gets better than eavesdropper links. It is worth to notify that the SPSC degrades with increase in number of hops. As number of hop increases, proportionally number of eavesdroppers also increases and thus maintaining positive secrecy capacity is very difficult for the system. This again confirms that the presence of more number of eavesdroppers creates unfavourable condition for secure data transmission. Moreover, from this figure, the result shows that the SPSC for scenario-1 is superior than scenario-2. Finally, at higher SNR, the asymptotic results are obtained for this figure. From Fig. 8, it can be seen that the performance of scenario-1 is better than scenario-2 at low regime of SNR. However, as SNR is more than 10 dB, the performance gap of both scenarios are small. Thus, it concludes that the constant SPSC is achieved at high SNR.

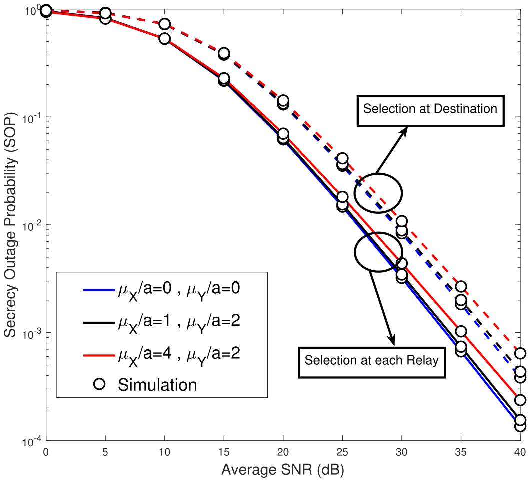

Fig. 9. Effect of boresight point on SOP.

Fig. 9 represents the effect of boresight pointing error on the SOP for both scenarios. During analysis, the parameters are set to be $r = 2$, L=3, $\alpha = 2.296$, $\beta = 2$, and $m = 1$. From this figure, it is observed that the security performance deteriorates as boresight increases from $\mu_X/a, \mu_Y/a = (0,0)$ to $(1,2)$ to $(4,2)$. This happens because the centre of the laser beam misaligned with respect to FSO receiver plane. Due to this, the instantaneous SNR of the legitimate link fluctuates. Consequently, eavesdropper will get a chance to intercept the secure data. Further, from the plot it can be observed that the system provides more security when selection of the secure data takes place at each relay as compared to selection at the destination only.

The impact of number of hops on the intercept probability is examined in Fig. 10. To do this, we obtain the IP versus $\overline{\gamma}$ for both scenarios setting $\alpha = 2.296$, $\beta = 2$, $r = 2$, $m = 1$, $\xi = 6.7$ and $\overline{\gamma}_E = 0$ dB. It is obvious from this figure that increasing the number of hops enhances the intercept probability of the system and thus reduces the system secrecy performance. To get more insight, the asymptotic results are also provided and it can be seen that both results fit in the higher SNR regimes. From this figure, it is also concluded that the scenario-1 provides better secrecy performance as compared to other one.

Fig. 11 illustrates the impact of increasing R_s on the EST. Fig. 11 plots the EST versus R_s for different number of hops.

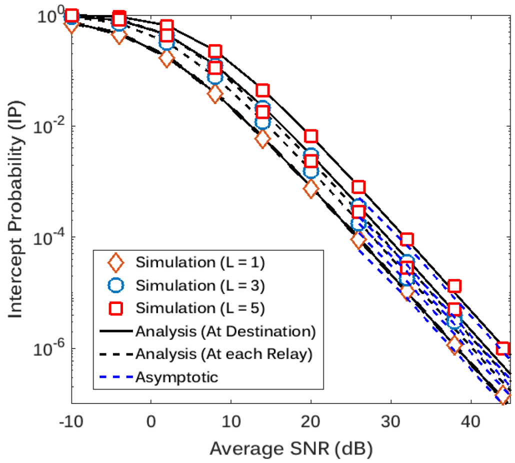

Fig. 10. IP versus $\overline{\gamma}$ for various number of hops.

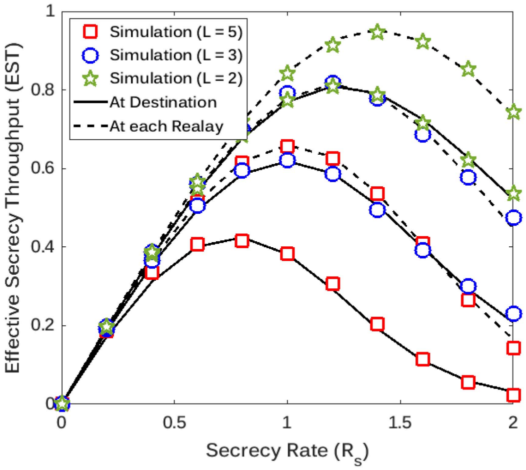

Fig. 11. EST versus R_s for various number of hops.

During analysis, we set the parameter values as $\alpha = 2.296$, $\beta = 2$, $r = 2$, $\xi = 1.1$, and $\overline{\gamma} = 5$ dB. The results reveal that the highest value of EST is achieved for lower value of L for both scenarios. Lastly, from all of theses figures, it can be observed that scenario-1 achieves higher EST as compared to scenario-2.

Finally, one of the most important analysis $i.e.$ SRT analysis of the considered system is presented in Fig. 12. In this figure, we present the results of intercept and outage probabilities to show the trade-off between security and reliability for the multihop hybrid RF/FSO system in the presence of eavesdropping attack. While analysis, we set the parameter values as $\alpha = 2.296$, $\beta = 2$, $r = 2$, $\xi = 6.7$, and $\overline{\gamma} = 5$ dB, $L = 2$. One can observe from Fig. 12 that as the outage probability increases from 0 to 1, the intercept probabilities of both scenarios in the multihop hybrid RF/FSO system both decrease from 1 to 0. This shows that the security performance improves if reliability requirement is less concern. This implies that the wireless security can be improved at the cost of a reliability degradation and vice versa. In addition, it is shown from Fig. 12 that the SRT performance of the multihop hybrid RF/FSO system with selection at each hop always outperforms the hybrid system with selection at the destination only.

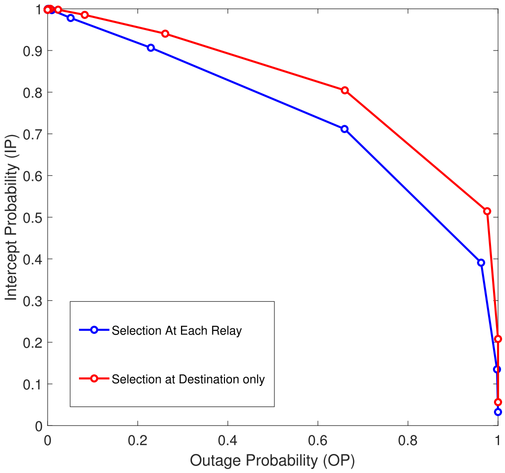

Fig. 12. SRT versus IP for considered scenarios.

Moreover, the analytical results obtained in Fig. 3 to Fig. 11 are validated through the Monte-carlo simulation results.

V. Conclusion

In this paper, for first time a multi-hop hybrid RF/FSO system is analysed from PLS perspective. To analyse the system, we have considered two different scenarios such as: selection at each hop (makes decision at each hop) and selection at destination (makes decision directly at destination). For the first time, the closed form solutions are obtained for secrecy performance metrics such as SOP, SPSC, IP, and EST are obtained for both scenarios and also compared. Moreover, the results are obtained for different atmospheric turbulence conditions, HD or IM/DD techniques, for different values of m, and number of hops. In addition, the non zero boresight pointing error analysis is also carried out for analyse the system more deeply. To analyse the system in depth, asymptotic results are also obtained. From this, we obtained the SCG and SDO for analysing the system in depth. It can be concluded that the increase in number of hops makes the system insecure for both scenarios. However, It can be observed that the secrecy performance gap reduces with increase in number of hops. For both scenarios, it concludes that, the secrecy performance gap is reduced with increase in the the number of hops. Further, it is observed that the system with selection at each hop provides better performance than the system with selection only at destination. Moreover, in EST results, we have demonstrated the security reliability trade-off analysis for both scenarios. Finally, the results are verified by Monte-Carlo simulation. The considered structure is particularly applicable for reliable, long-range and high capacity communication links.

References

[1] Y. Gao et al., “Physical layer security in 5G based large scale social networks: Opportunities and challenges,” *IEEE Access*,, vol. 6, pp. 26350–26357, 2018.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[3] 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.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY, USA: Prentice Hall, 2008.

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

[6] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO Generalized-K fading channels," *IEEE Trans. Veh. Techn.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[7] L. Kong and G. Kaddoum, "On physical layer security over the fisher-snedecor ($\mathcal{F}$) wiretap fading channels," *IEEE Access*, vol. 6, pp. 39466–39472, 2018.

[8] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over fox's H-Function wiretap fading channels," *IEEE Trans. Veh. Tech.*, vol. 68, no. 7, pp. 6608–6621, Jul. 2019.

[9] 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.

[10] L. Kong, H. Tran, and G. Kaddoum, "Performance analysis of physical layer security over α - μ fading channel," *Electron. Lett.*, vol. 52, no. 1, pp. 45–47, Jan. 2016.

[11] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[12] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of α-η-κ-μ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[13] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[14] R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and K. Qaraqe, "Secure communication for FSO links in the presence of eavesdropper with generic location and orientation," *Opt. Exp.* 27, pp. 34211–34229, 2019.

[15] 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.

[16] D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–9, Oct. 2016.

[17] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over málaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, Apr. 2017.

[18] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, pp. 1–17, Dec. 2020.

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

[20] M. Obeed and W. Mesbah, "Efficient algorithms for physical layer security in one-way relay systems," *Wireless Netw.*, vol. 25, no. 3, pp. 1327–1339, 2019.

[21] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5904–5918, Sep. 2016.

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

[23] H. Lei, Z. Dai, I. S. Ansari, K. H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photon. J.*, vol. 9, no. 4, pp. 1–14, Aug. 2017.

[24] 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. Techn.*, vol. 67, no. 12, pp. 12427–12431, Dec. 2018.

[25] H. Lei, H. Luo, K.-H. Park, G. Pan, Z. Ren, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems with channel imperfection," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–13, Jun. 2018.

[26] 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 System J.*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[27] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photon. J.*, vol. 11, no. 1, pp. 1–14, Feb. 2019.

[28] H. Lei, Z. Dai, K. 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.

[29] D. R. Pattanayak, V. K. Dwivedi, V. Karwal, I. S. Ansari, H. Lei, and M.-S. Alouini, "On the physical layer security of a decode and forward based mixed FSO/RF co-operative system," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1031–1035, Jul. 2020.

[30] 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.

[31] W. M. R. Shakir and M. Alouini, "Secrecy performance analysis of parallel FSO/mm-wave system over unified fisher-snedecor channels," *IEEE Photon. J.*, vol. 14, no. 2, pp. 1–13, Apr. 2022.

[32] R. Singh, M. Rawat, and A. Jaiswal, "On the physical layer security of mixed FSO-RF SWIPT system with non-ideal power amplifier," *IEEE Photon. J.*, vol. 13, no. 4, pp. 1–17, Aug. 2021.

[33] W. M. R. Shakir, "Physical layer security performance analysis of hybrid FSO/RF communication system," *IEEE Access*, vol. 9, pp. 18948–18961, 2021.

[34] M. Usman, H. Yang, and M. Alouini, "Practical switching-based hybrid FSO/RF transmission and its performance analysis," *IEEE Photon. J.*, vol. 6, no. 5, pp. 1–13, Oct. 2014.

[35] L. Kong, W. Xu, L. Hanzo, H. Zhang, and C. Zhao, "Performance of a free-space-optical relay-assisted hybrid RF/FSO system in generalized M. -Distributed Channels," *IEEE Photon. J.*, vol. 7, no. 5, pp. 1–19, Oct. 2015, Art. no. 7903319.

[36] M. A. Amirabadi and V. T. Vakili, "Performance comparison of two novel relay-assisted hybrid FSO/RF communication systems," *IET Commun.*, vol. 13, no. 11, pp. 1551–1556, Jul. 2019.

[37] M. A. Amirabadi and V. T. Vakili, "On the performance of a multi-user multi-hop hybrid FSO/RF communication system," *Opt. Commun.*, vol. 444, pp. 172–183, 2019.

[38] Y. Ai, A. Mathur, H. Lei, M. Cheffena, and I. S. Ansari, "Secrecy enhancement of RF backhaul system with parallel FSO communication link," *Opt. Commun.*, vol. 475, 2020, Art. no. 126193.

[39] D. R. Pattanayak, V. K. Dwivedi, and V. Karwal, "On the physical layer security of hybrid RF-FSO system in presence of multiple eavesdroppers and receiver diversity," *Opt. Commun.*, vol. 477, 2020, Art. no. 126334.

[40] M. K. Simon and M.-S. Alouini, *Digital Communications Over Fading Channels.*New York, NY, USA: Wiley, 2005.

[41] S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*. New York, NY, USA: Academic Press, 2000.

[42] G. D. Verma, A. Mathur, Y. Ai, and M. Cheffena, "Secrecy performance of FSO communication systems with nonzero boresight pointing errors," *IET Commun.*, vol. 15, no. 1, pp. 155–162, Jan. 2021.

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

[44] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2086–2089, Dec. 2015.

[45] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[46] I. Wolfram, *Mathematica Edition: Version 8.0*. Champaign, IL, USA: Wolfram Research Inc., 2010.

[47] E. Illi, F. El Bouanani, D. B. Da Costa, F. Ayoub, and U. S. Dias, "Dual-hop mixed RF-UOW communication system: A. PHY security analysis," *IEEE Access*, vol. 6, pp. 55345–55360, 2018.

[48] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[49] D. Chen, Y. Cheng, X. Wang, W. Yang, J. Hu, and Y. Cai, "Energy-efficient secure multiuser scheduling in energy harvesting untrusted relay networks," *J. Commun. Netw.*, vol. 21, no. 4, pp. 365–375, Aug. 2019.

[50] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, "Understanding the performance of free-space optics," *J. Opt. Netw.*, vol. 2, pp. 178–200, 2003.

[51] I. I. Kim et al., "Wireless optical transmission of fast ethernet, FSSI, STM, and escon protocol data using the terralink laser communication system," *Opt. Eng.*, vol. 37, no. 12, pp. 3143–3155, 1998.