IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 30, 2020, accepted December 12, 2020, date of publication December 31, 2020, date of current version February 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048614

Physical Layer Security Performance Analysis of Hybrid FSO/RF Communication System

WAFAA MOHAMMED RIDHA SHAKIR, (Student Member, IEEE)
Department of Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil 51015, Iraq
e-mail: inb.wfa@ atu.edu.iq

ABSTRACT In this paper, the secrecy performance of the physical layer security (PLS) of the hybrid free-space optical/radio frequency (FSO/RF) communication system is analyzed. The transmission protocol of the considered system is performed under the eavesdropper's attempt to overhear the RF link between the transmitter and legitimate receiver of the hybrid system. The FSO link is characterized by Málaga-M distribution while the RF links are modeled by Nakagami-*m* distribution. The two practical eavesdropping modes considered in this paper include: colluding and non-colluding. Exact closed-form expressions for the system's secrecy outage probability (SOP), the asymptotic of the SOP (SOP^{∞}), the probability of strictly positive secrecy capacity (SPSC), the average secrecy capacity (ASC), and the asymptotic of the ASC (ASC^{∞}), are specifically derived under the influence of both eavesdropper modes. Our derived analytical expressions present an efficient tool to investigate the impact of some channel parameters on the secrecy performance, namely the fading severity of the RF links, atmospheric turbulence severity, pointing error of the FSO link, number of eavesdroppers, and the power of the eavesdropper links. The results show that the increase of the eavesdroppers' number under both modes profoundly degrades the considered system secrecy performance. The accuracy of the numerical results obtained is validated by Monte-Carlo simulations.

INDEX TERMS Physical layer security, hybrid FSO/RF system, secrecy outage probability, asymptotic of the secrecy outage probability, probability of strictly positive secrecy capacity, average secrecy capacity.

I. INTRODUCTION

A. BACKGROUND AND RELATED WORKS

Along with the massive increasing demands of the fifth-generation (5G) wireless networks for the high-data rates technology, the scientific community has witnessed a huge growth of interest in the optical wireless communications (OWC) that satisfies the 5G broad bandwidth specifications [1]. Free-space optical (FSO) is considered to be one of the most promising WOC techniques due to its merit specifications. The extensive bandwidth, free licenses, strong security, low implementation costs, and many other attractive properties make the FSO technology permits the realization of many potential applications in the front-haul access network, building communications, emergency disaster recovery, and military applications [2]. However, the FSO link is susceptible to atmospheric turbulence, pointing error, and adverse weather effects that can create an optical-beam signal divergence and significantly attenuate the optical signal [3]. For example, a moderate fog condition may attenuate the optical beam by 40 dB/Km [4].

Hybrid free-space optical/radio frequency (FSO/RF) communication is one proposed approach to improve the reliability and availability of the FSO link by enabling the benefits of both technologies [5], [6]. The overarching idea of the hybrid FSO/RF system is to transmit identical signals simultaneously over both links and combining the received signals using one diversity combining technique. This is logical because the two links exhibit compatible characteristics to atmospheric and weather effects; whereas the RF link is not prone to atmospheric turbulence or fog as the case of the FSO link, but rather to heavy rain [7]. It should be noted that the considered hybrid FSO/RF system in this paper significantly differs from the mixed FSO-RF systems since the FSO link is only part of the mixed FSO–RF relay system [8]. However, the differences in the system configurations of the hybrid FSO/RF and mixed FSO–RF systems make them have different methods of analysis and advantages.

Recently, due to the broadcasting nature of the wireless medium, makes the RF channel vulnerable to eavesdropping

The associate editor coordinating the review of this manuscript and approving it for publication was Sukhdev Roy.

attack, there is an enormous amount of private information leakage from legitimate channels [9]. On other hand, FSO communication is more secure due to the highly directional optical beam, but it is highly susceptible to atmospheric conditions and adverse weather effects and may experience transmission outage when the channel quality of the FSO link is poor [10]. The physical layer security (PLS) has been widely considered as a companion tool to the conventional higher layer's cryptography schemes. The PLS aims for enabling significantly improve security level of communications as well as offer low computing complexity for devices with fewer resources in the 5G networks [11]. Interestingly, the PLS paradigm, introduced pioneeringly by Wyner in [12], aims at establishing perfectly secure communication, by exploiting the random characteristics of the wireless channel (e.g., fading, noise, interference, etc.) in the presence of an eavesdropper. In practice, all eavesdroppers may jointly process their received message to a central data processing unit as in the case of the colluding eavesdropper mode. For a non-colluding mode, the eavesdroppers individually overhear the communication without centralized control. Inherently, the colluding case is more efficient where multiple eavesdroppers appear and work in a cooperative manner [13]. Therefore, the latest developments in PLS along with the tremendous capability of the hybrid FSO/RF system in different applications have motivated us to investigate the PLS performance of such a system in this research work. A comprehensive open literature review confirms that the current research works on the PLS of such systems are mostly limited to either the single FSO link systems [14]–[17] or mixed FSO–RF systems [18]–[30], and the PLS of hybrid FSO/RF system is not yet explored despite the enormous potential of this system in different current and future applications. In [5], the secrecy performance analysis of the hybrid FSO/RF system is restricted to the secrecy outage probability only. Recently authors' in [31] investigated the PLS for an RF backhaul system with a parallel FSO link. In this work [31], the authors' considered an eavesdropper which is trying to intercept data from the RF link only. The scenario of [31] can be considered as our special case because the investigation of both eavesdropping modes unifies the performance evaluation of PLS of the hybrid FSO/RF system. More recently, in [32], the communication over hybrid FSO and MMW links is assumed to be secure by optimizing the resource allocation of each link concerning the system's power budget. It is noteworthy to point out that, all the aforesaid studies never focus on a general security performance of the physical layer of the hybrid FSO/RF systems that is influenced by both modes of eavesdropping.

B. MOTIVATION AND CONTRIBUTIONS

The secrecy performance of the hybrid FSO/RF systems is still, an open topic, as there are very few studies that carried out the secrecy analysis of these systems. Again, in the open literature, secrecy performances were analyzed mostly for mixed FSO-RF systems. To the best of our knowledge, the general security performance analysis of the hybrid FSO/RF system has not yet been fully investigated. In this paper, in addition to considering a PLS analysis of the hybrid FSO/RF system configuration, we address the secrecy performance of this considered configuration under the effects of the non-colluding and colluding eavesdropping modes, with the presence of multiple eavesdroppers for the first time for this type of configuration. Moreover, since the wireless channels vary frequently with time, hence assuming Nakagami-m channel model in the RF links will provide a more realistic secrecy analysis of hybrid FSO/RF systems. On the other hand, the Málaga-M fading model of the FSO link of the investigated system can also accurately make intelligible outcomes amid intense atmospheric turbulence and pointing error impairment circumstances. Inspired by these conveniences, we present a secure scenario over the Málaga-M/Nakagami-m hybrid FSO/RF fading channel. We also assume an eavesdropper can wiretap transmitted data utilizing RF link only. In summary:

- We first obtain the cumulative distribution function (CDF) of selective combining (SC) scheme-based hybrid FSO/RF system using the CDF of each link.
- We analyze the secrecy characteristics when the legitimate RF link is subjected to colluding and non-colluding attacks by eavesdroppers considering popular secrecy metrics. More precisely, new exact expressions of the secrecy outage probability (SOP), the asymptotic SOP (SOP^{∞}), the probability of strictly positive secrecy capacity (SPSC), the average secrecy capacity (ASC), and the asymptotic of the ASC (ASC^{∞}) are deduced. These expressions are novel compared to the existing works as the effect of colluding and non-colluding attacks is not reported in the exiting hybrid FSO/RF literature.
- We exploit these expressions to drive the numerical results with selected figures. Moreover, Monte-Carlo simulations further verify the accuracy of the derived analytical results.
- As our proposed model ascertains security at the physical layer, we exhibit all consequences regarding effects of fading/scintillation severity, pointing error, the number of eavesdroppers, and SNR of the eavesdropper link parameters are investigated to gain further insight into the behavior of the PLS of the investigated system.

The outline of this paper is as follows: Section-II introduces models of the adopted system and channel, while in Section-III, an analytical expression for the two eavesdropper modes is derived for the SOP, SOP^{∞}, SPSC, ASC, and ASC^{∞}. Section-IV contains several illustrative numerical examples accompanied by insightful discussions. Section-V concludes the paper.

II. SYSTEM AND CHANNEL MODELS

As shown in Fig. 1, we consider a hybrid FSO/RF system operating under parallel FSO and RF legitimate

transmission links in the presence of N eavesdroppers (Eve) intended to overhear the legitimate RF link. In such a scenario, the transmitter (T) of the considered system transmits a private message to the desired receiver (R) over both links simultaneously. At the receiver, the selective combiner (SC) selects the signal of the best link (i.e., the signal with the highest signal-to-noise ratio (SNR)). Here, the hybrid FSO/RF link is considered the main channel, while the transmitter-to-eavesdroppers (T-Eve) link is named the wiretap channel.

A. THE MAIN CHANNEL MODEL

The FSO link is characterized by the Málaga-M distribution [33], whereas the atmospheric turbulence and pointing error impairments of the FSO link have been described are very accurately by this model. Considering the intensity modulation/direct detection (IM/DD) and heterodyne detection (HD) schemes for optical signal detection, the probability density function (PDF) and cumulative distribution function (CDF) of instantaneous SNR γ_f are as the following [34]

$$f_{\gamma_f}(\gamma) = \frac{\xi^2 A}{2^r \gamma} \sum_{t=1}^{\beta} c_t G_{1,3}^{3,0}\left(B\left(\frac{\gamma}{\bar{\gamma}_f^r}\right)^{\frac{1}{r}} \middle| \begin{matrix} \xi^2+1 \\ \xi^2, \alpha, t \end{matrix}\right) \quad (1)$$

$$F_{\gamma_f}(\gamma) = \mathcal{D} G_{r+1,3r+1}^{3r,1}\left(E\frac{\gamma}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1,\kappa_1 \\ \kappa_2, 0 \end{matrix}\right) \quad (2)$$

In (1) and (2), $G_{p,q}^{m,n}$ is the Meijer's G-function, and

$$A \triangleq \frac{2\alpha^{\alpha/2}}{h^{1+\alpha/2}\Gamma(\alpha)}\left(\frac{h\beta}{h\beta+\Omega'}\right)^{\beta+\alpha/2}$$

$$c_t = a_t\left[\frac{\alpha\beta}{(h\beta+\Omega')}\right]^{(-\alpha+t)/2},$$

$$a_t \triangleq \binom{\beta-1}{t-1}\frac{(h\beta+\Omega')^{1-t/2}}{(t-1)!}\left(\frac{\Omega'}{h}\right)^{t-1}\left(\frac{\alpha}{\beta}\right)^{t/2}$$

and $B = \xi^2\alpha\beta\left(h+\Omega'\right)/\left[\left(\xi^2+1\right)\left(h\beta+\Omega'\right)\right]$, while h denotes the average power of the scattering component received by off-axis eddies, Ω' represents the average power from the coherent contributions, ξ represents the ratio between the equivalent beam radius at the receiver and the pointing error displacement standard deviation (jitter), r is the parameter defining the type of detection technique (i.e., $r = 1$, represents the HD and $r = 2$, represents the IM/DD), γ_f^r is the average SNR of the FSO link, for the HD technique case ($r = 1$): $\bar{\gamma}_f^1 = \mathbb{E}\left[\gamma_f\right]$, and for the IM/DD case ($r = 2$):

$$\bar{\gamma}_f^2 = \bar{\gamma}_f^1 \alpha\beta\xi^2 \times (\xi^2+1)/\left[(\alpha+1)(\beta+1)(\xi^2+1)^2\right],$$

with $\mathbb{E}[.]$ denoting the expectation operator, α and β denote the severity of fading resulting from the turbulent flow.

$\mathcal{D} = \frac{\xi^2 A\sum_{t=1}^{\beta} b_t}{\left[2^r(2\pi)^{r-1}\right]}$, $b_t = c_t r^{\alpha+t-1}$, $E = \frac{B^r}{r^{2r}}$, $B = h\alpha\beta$, $\kappa_1 = \frac{\xi^2+1}{r}, \ldots, \frac{\xi^2+r}{r}$ comprises of r terms and $\kappa_2 = \frac{\xi^2}{r}, \ldots, \frac{\xi^2+r-1}{r}, \ldots, \frac{\alpha}{r}, \ldots, \frac{\alpha+r-1}{r}, \ldots, \frac{\alpha t}{r}, \ldots, \frac{t+r-1}{r}$ comprises of $3r$ terms.

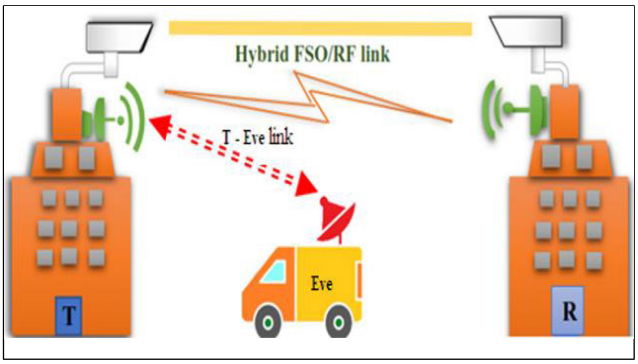

FIGURE 1. Hybrid FSO/RF system model depicting the transmitter (T), receiver (R), and the eavesdropper (Eve) with their respective links between them.

In addition, the legitimate RF link is independent and identically distributed (i.i.d.) and characterized by the Nakagami-m distribution. The choice of this distribution to characterize the RF links is mainly due to the ability of this distribution to approach other widely used fading models very well. For a legitimate RF link between the transmitter T and receiver R, the PDF and CDF of the instantaneous SNR γ_r are given by [35]

$$f_{\gamma_r}(\gamma) = \Omega_r^{m_r}\frac{\gamma^{m_r-1}}{\Gamma(m_r)}exp(-\Omega_r\gamma) \quad (3)$$

$$F_{\gamma_r}(\gamma) = \frac{\Gamma_{inc}(m_r, \Omega_r\gamma)}{\Gamma(m_r)} \quad (4)$$

where $\Omega_r = \frac{m_r}{\bar{\gamma}_r}$, and m_r and $\bar{\gamma}_r$ denote the fading severity parameter, the average SNR of the legitimate RF link between transmitter T and receiver R respectively, whereas $\Gamma_{inc}(.,.)$ and Γ are represented the lower incomplete Gamma function and the Gamma function [35] respectively.

B. THE WIRETAP CHANNEL MODEL

The fading in the wiretap channel i.e., the T-Eve$_i$ links between the transmitter T and eavesdropper Eve$_i$, $1 \le i \le N$, are supposed to under Nakagami-m fading with m_e fading severity parameter. Firstly, let us consider the non-colluding mode, the instantaneous SNR γ_e^{nc} of the T-Eve link can be written as [36]

$$\gamma_e^{nc} = \max_{1\le i<N}\bar{\gamma}_{e_i} \quad (5)$$

where $\bar{\gamma}_{e_i}$ denotes the average SNR of the T- Eve$_i$ links.

The PDF and CDF of the T-Eve$_i$ links between the transmitter T and the eavesdropper Eve$_i$ among the N eavesdroppers are expressed as [37]

$$f_{\gamma_e^{nc}}(\gamma) = \frac{N}{\Gamma(m_e)}\sum_{g=0}^{N-1}\binom{N-1}{g}(-1)^g \times e^{-(g+1)\Omega_e\gamma}\,\Xi_g.\Omega_e^{m_e+\Upsilon_e}\gamma^{m_e+\Upsilon_e+1} \quad (6)$$

$$F_{\gamma_e^{nc}}(\gamma) = \sum_{g=0}^{N}\binom{N}{g}(-1)^g e^{-g\Omega_e\gamma}\,\Xi_g\,(\Omega_e\gamma)^{\Upsilon_e} \quad (7)$$

where $\Xi_g = \sum_{u_1=0}^{g}\sum_{u_2=0}^{u_1}\cdots\sum_{u_{m_e}=0}^{u_{m_e}-2}\frac{g!}{(u_{m_e}-1)}\prod_{v=1}^{m_e-1}\frac{(v!)^{u_{v-1}-u_v}}{(u_{v-1}-u_v)!}$, with $u_0 = g$, $u_{m_e} = 0$ and $\Upsilon_e = \sum_{s=1}^{m_e-1} u_s$, where the scale parameter $\Omega_e = \frac{m_e}{\bar{\gamma}_e}$, with m_e refer to the fading severity parameter of the T-Eve link.

Secondly, for the colluding eavesdropping mode, the eavesdroppers cooperated to exchange their observations to decode the confidential message overhearing from the legitimate RF link using maximum ratio combining (MRC). Thus, the instantaneous received SNR γ_e^c for the T-Eve link can be expressed as [36]

$$\gamma_e^c = \sum_{i=0}^{N} \bar{\gamma}_{e_i} \tag{8}$$

Accordingly, the PDF and CDF of the SNR γ_e^c at the MRC output can be expressed as the following [36]

$$f_{\gamma_e}^c(\gamma) = \Omega_e^{Nm_e}\frac{\gamma^{Nm_e-1}}{\Gamma(Nm_e)}exp(-\Omega_e\gamma) \tag{9}$$

$$F_{\gamma_e}^c(\gamma) = \frac{\Gamma_{inc}(Nm_e, \Omega_e\gamma)}{\Gamma(Nm_e)} \tag{10}$$

C. STATISTIC CHARACTERISTICS OF THE HYBRID FSO/RF SYSTEM

With the receiver of the hybrid FSO/RF system employing the SC scheme, the equivalent SNR γ_{eq} of the considered system relies upon the SNRs of both links. Thus, the CDF $F_{\gamma_{eq}}$ of the instantaneous SNR γ_{eq} is obtained as [6]

$$F_{\gamma_{eq}}(\gamma) = F_{\gamma_f}(\gamma) F_{\gamma_r}(\gamma) \tag{11}$$

By substituting (2) and (4) in (11), (11) can be rewritten as the following

$$F_{\gamma_{eq}}(\gamma) = \mathcal{D}G_{r+1,3r+1}^{3r,1}\left(\frac{E\gamma}{\bar{\gamma}_f^r}\middle|\begin{matrix}1,\kappa_1\\ \kappa_2, 0\end{matrix}\right)\frac{1}{\Gamma(m_r)}\Gamma_{inc}(m_r, \Omega_r\gamma) \tag{12}$$

When $\bar{\gamma}_r \to \infty$, the asymptotic CDF $F_{\gamma_{eq}}^{\infty}(.)$ of the instantaneous SNR γ_{eq} is found by utilizing the asymptotic property of lower incomplete Gamma function [38, eq. (06.06.06.0004.02)] as

$$F_{\gamma_{eq}}^{\infty}(\gamma) \cong \frac{\mathcal{D}(\Omega_r)^{m_r}}{m_r\Gamma(m_r)}G_{r+1,3r+1}^{3r,1}\left(\frac{E\gamma}{\bar{\gamma}_f^r}\middle|\begin{matrix}1,\kappa_1\\ \kappa_2, 0\end{matrix}\right) \tag{13}$$

III. SECRECY PERFORMANCE EVALUATION

In order to quantify the considered systems' PLS level, this section is devoted to presenting the secrecy performance metrics, namely SOP, SOP$^{\infty}$, SPSC, ASC, and ASC$^{\infty}$. In this work, we assume that the FSO communication is secure while RF confidential information transmission is subject to eavesdropping of N malicious eavesdropper.

A. SECRECY OUTAGE PROBABILITY (SOP) ANALYSIS

This security metric is defined as the probability that the security capacity C_s falls below a predetermined information transmission rate $\mathcal{R}_s$ of the system [39]. In this case, the capacity of the main channel is lower than that of the wiretap channel which leads to the system being security outage.

$$\begin{aligned} SOP &= P_r(C_s \le \mathcal{R}_s)\\ &= P_r(\gamma_{eq} \le \gamma_e)\\ &= \int_0^{\infty} f_e(\gamma) F_{eq}((1+\gamma)\emptyset - 1)d\gamma \end{aligned} \tag{14}$$

In (14), $\emptyset = exp(\mathcal{R}_s)$ [39].

Theorem 1: The SOP for the non-colluding and colluding eavesdropping modes is expressed in exact closed-form expressions as stated in (15) and (16), respectively, as shown at the bottom of next page.

Proof: See Appendix A.

B. ASYMPTOTIC ANALYSIS OF SOP

The closed-form expressions for secrecy outage probability is complex to study the effect of various system parameters. Hence, to gain more insights understandings on the PLS performance of the investigated system, we study hereafter the asymptotic behavior of SOP under the effect of both eavesdropper modes. At high SNR i.e., when $\bar{\gamma}_r \to \infty$, the hybrid FSO/RF system will always utilize the radio channel for confidential information transmission, and the eavesdropper will also continuously intercept the information through the RF link. In this case, the SOP$^{\infty}$ can be represented in mathematical terms as [31]

$$SOP^{\infty} \cong \int_0^{\infty} F_{\gamma_{eq}}^{\infty}(\gamma) f_e(\gamma) d\gamma \tag{17}$$

Theorem 2: The SOP^{∞} under non-colluding and colluding eavesdropping modes namely, SOP_{nc}^{∞} and SOP_c^{∞}, as stated in (18) and (19), respectively, as shown at the bottom of the next page. It is worth mentioning that, the diversity order is decided by the least exponent of $\bar{\gamma}_r$ in (18)-(19), it is that the secrecy diversity order is m_r in terms of $\bar{\gamma}_r$.

Proof: See Appendix B.

C. PROBABILITY OF STRICTLY POSITIVE SECRECY CAPACITY (SPSC) ANALYSIS

The SPSC [39], which refers to the probability of positive secrecy capacity, is a crucial criterion for secure communications. Therefore, it can be determined by [39, eq. (23)]

$$\begin{aligned} SPSC &= P_r\{C_s(\gamma_{eq}, \gamma_e) > 0\}\\ &= P_r(\gamma_{eq} > \gamma_e)\\ &= 1 - \int_0^{\infty} f_e(\gamma) F_{eq}(\gamma) d\gamma \end{aligned} \tag{20}$$

Thus,

$$SPSC = 1 - SOP, \quad for \quad \emptyset = 1 \tag{21}$$

The exact expression of SPSC under the non-colluding $SPSC^{nc}$, and colluding $SPSC^{c}$ eavesdropping modes are evaluated directly by substituting $\emptyset = 1$ in corresponding SOP expression of (15) and (16) respectively, then inserting the results into (21).

D. AVERAGE SECRECY CAPACITY (ASC) ANALYSIS

Average secrecy capacity, defined as the maximum information rate at which the transmitter may transmit to the receiver without the eavesdropper being able to acquire any information. The information-theoretic mathematically describes the secrecy capacity C_s as the difference between the capacity of the main channel C_{eq} and the wiretap one C_e [40] as

$$C_s = C_{eq} - C_e \tag{22}$$

where C_{eq} is the instantaneous capacity of the main channel

$$C_{eq} = \log\left(1 + \gamma_{eq}\right) \tag{23}$$

while C_e is the instantaneous capacity of the wiretap channel

$$C_e = \log(1 + \gamma_e) \tag{24}$$

The average value of the secrecy capacity can be expressed as [19]

$$ASC = \frac{1}{\ln(2)} \int_0^\infty \frac{F_{\gamma_e}(\gamma)}{1+\gamma} \left(1 + F_{\gamma_{eq}}(\gamma)\right) d\gamma \tag{25}$$

Theorem 3: The exact closed-form expression for the non-colluding and colluding eavesdropping modes namely, ASC^{nc} and ASC^{c}, respectively are as state in (26) and (27), as shown at the bottom of the next page.

Proof: See Appendix C.

E. ASYMPTOTIC ANALYSIS OF ASC

The asymptotic expression of ASC, ASC^{∞}, for the investigated system when $\bar{\gamma}_r \to \infty$ is expressed as

$$ASC^{\infty} \cong \frac{1}{\ln(2)} \int_0^\infty \frac{F_{\gamma_e}(\gamma)}{1+\gamma} \left(1 + F^{\infty}_{\gamma_{eq}}(\gamma)\right) d\gamma \tag{28}$$

Theorem 4: The ASC^{∞} for the non-colluding and colluding eavesdropping modes namely, ASC^{∞}_{nc} and ASC^{∞}_{c},, as the as shown in (29) and (30), respectively, as shown at the bottom of the next page.

Proof: See Appendix D.

To the best of the author's knowledge based on the open literature, the expressions in (15), (16), (18), (19), (26), (27),

$$\begin{aligned} SOP^{nc} = {} & \mathcal{H}_1 \emptyset^{-(m_e+\Upsilon_e+2)} e^{\left(\frac{-(g+1)(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{m=0}^{m_e+\Upsilon_e+1} \binom{m_e+\Upsilon_e+1}{m} (1-\emptyset)^{m_e+\Upsilon_e+1-m} (m_r-1)! \\ & \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s [(g+1)\Omega_e + \Omega_r]}{s!} [(-1)^{-(m+s+1)} G^{3r,2}_{r+2,3r+1}\left(\frac{E}{\bar{\gamma}_f^r [(g+1)\Omega_e + \Omega_r]}\middle| \begin{matrix} -(m+s), 1, \kappa_1 \\ \kappa_2, 0 \end{matrix}\right) \\ & - \sum_{w=0}^{\infty} \frac{(-1)^{-w} (\emptyset-1)^{m+s+w+1}}{w!} G^{3r,2}_{r+2,3r+2}\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix} -(m+s+w), 1, \kappa_1 \\ \kappa_2, 0, -(m+s+w+1) \end{matrix}\right)\Bigg] \end{aligned} \tag{15}$$

$$\begin{aligned} SOP^{c} = {} & \mathcal{H}_4 \emptyset^{-Nm_e} e^{\left(\frac{-(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{k=0}^{Nm_e-1} \binom{Nm_e-1}{k} (1-\emptyset)^{Nm_e+1-k} (m_r-1)! \\ & \times \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s \Omega_e + \Omega_r)}{s!} [(-1)^{-(k+s+1)} G^{3r,2}_{r+2,3\ r+1}\left(\frac{E}{\bar{\gamma}_f^r [\Omega_e + \Omega_r]}\middle| \begin{matrix} -(k+s), 1, \kappa_1 \\ \kappa_2, 0 \end{matrix}\right) \\ & - \sum_{w=0}^{\infty} \frac{(-1)^{-w} (\emptyset-1)^{m+s+w+1}}{w!} G^{3r,2}_{r+2,3r+2}\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix} -(k+s+w), 1, \kappa_1 \\ \kappa_2, 0, -(k+s+w+1) \end{matrix}\right)\Bigg] \end{aligned} \tag{16}$$

$$\begin{aligned} SOP^{\infty}_{nc} \cong {} & \frac{\mathcal{H}_1 (\Omega_r)^{m_r}}{m_r} e^{\left(\frac{-(g+1)(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{m=0}^{m_e+\Upsilon_e+1} \binom{m_e+\Upsilon_e+1}{m} \frac{(1-\emptyset)^{m_e+\Upsilon_e+1-m}}{\emptyset^{(m_e+\Upsilon_e+2)}} \\ & \times \Bigg[\sum_{q=0}^{m_r-1} \frac{(m_r-1)! (\Omega_r)^q}{q!} [(g+1)\Omega_e + \Omega_r]^{-(m+q+1)} G^{3r,2}_{r+2,3r+1}\left(\frac{E}{\bar{\gamma}_f^r [(g+1)\Omega_e + \Omega_r]}\middle| \begin{matrix} -(m+q), 1, \kappa_1 \\ \kappa_2, 0 \end{matrix}\right) \\ & - \sum_{q=0}^{m_r-1} \frac{1}{q!} \left[\frac{(g+1)\Omega_e}{\emptyset}\right]^q (\emptyset-1)^{m_r+m+q+1} G^{3r,2}_{r+2,3r+2}\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix} -(m_r+m+q), 1, \kappa_1 \\ \kappa_2, 0, -(m_r+m+q+1) \end{matrix}\right)\Bigg] \end{aligned} \tag{18}$$

$$\begin{aligned} SOP^{\infty}_{c} \cong {} & \frac{\mathcal{H}_4 (\Omega_r)^{m_r}}{m_r} e^{\left(\frac{(\emptyset-1)\Omega_e}{\emptyset}\right)} \sum_{k=0}^{Nm_e-1} \binom{Nm_e-1}{k} \frac{(\emptyset-1)^{Nm_e-1+k}}{\emptyset^{Nm_e}} \\ & \times \Bigg[\sum_{q=0}^{m_r-1} \frac{(m_r-1)! (\Omega_r)^q}{q!} [\Omega_e + \Omega_r]^{-(m_r+k+q+1)} G^{3r,2}_{r+2,3r+1}\left(\frac{E}{\bar{\gamma}_f^r [\Omega_e + \Omega_r]}\middle| \begin{matrix} -(m_r+k+q), 1, \kappa_1 \\ \kappa_2, 0 \end{matrix}\right) \\ & - \sum_{q=0}^{m_r-1} \frac{1}{q!} \left[\frac{\Omega_e}{\emptyset}\right]^q (\emptyset-1)^{m_r+m+q+1} G^{3r,2}_{r+2,3r+2}\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix} -(m_r+k+q), 1, \kappa_1 \\ \kappa_2, 0, -(m_r+k+q+1) \end{matrix}\right)\Bigg] \end{aligned} \tag{19}$$

(29), and (30) corresponding to our considered system are new and never found before, and hence our derived expressions are novel.

IV. NUMERICAL RESULTS

In this section, the PLS performance analysis of the considered hybrid system having varying channel conditions under both non-colluding and colluding eavesdropper modes is presented. Without loss of generality, it is assumed that the average SNRs for both the legitimate links are equal ($\bar{\gamma}_f = \bar{\gamma}_r$) and the average SNR of the hybrid system is set as (10 dB). The results are obtained by assuming HD optical signal detection technique, weak ($\alpha = 3.78, \beta = 3.74, \xi = 6.0$), moderate ($\alpha = 2.50, \beta = 2.06, \xi = 3.1$) and strong ($\alpha = 2.04, \beta = 1.10, \xi = 1.0$) scenarios of the atmospheric turbulence strength and pointing error effect, turbulent, ($\Omega = 1.3265, b_o = 0.1079$), $\rho = 0.596$, and $\varphi_A - \varphi_B = \pi/2$. Moreover, the secrecy rate for information transmission is set to be 0.1 bit/s/Hz. In MATLAB, the Málaga-M channel random variable was generated via squaring the absolute value of a Rician-shadowed random variable [33]. Also, for all cases, 10^6 realizations of the random variable were generated to perform the Monte-Carlo (MC) simulations in MATLAB.

Figure 2 shows the SOP performance of the considered system under different atmospheric turbulence conditions for the colluding and non-colluding eavesdropping modes. From this figure, it can be seen that the system's overall SOP performance is deteriorated with atmospheric turbulence strength shifting from weak to strong. It can be deduced that the secrecy outage probability under colluding is degraded further compared with the non-colluding mode under the same turbulence condition. Whereas, the hybrid system loses around 18 dB at SOP of 10^{-5}, as the turbulence increases from weak to strong in the non-colluding eavesdropping mode.

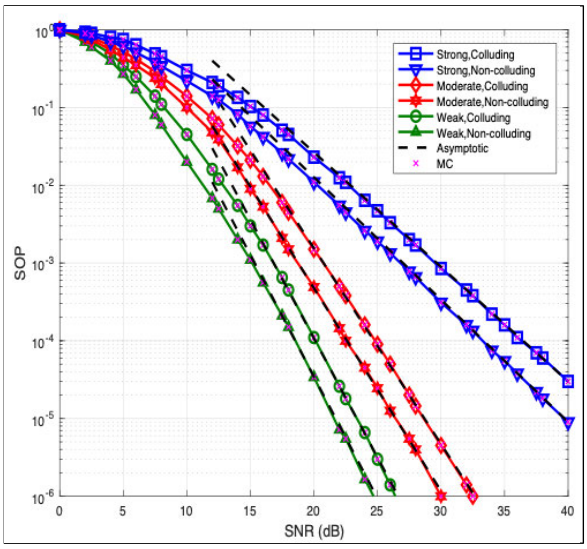

FIGURE 2. SOP versus the average SNR under different turbulence effects where $\varepsilon = 6$, $\gamma_e = 1dB$, $m_r = m_e = 2$, and $N = 4$.

The plot of SOP versus the average SNR of the investigated hybrid system for chosen values of N and ξ is displayed in Fig. 3. It can be inferred from the results of this figure that the smaller the values of ξ, the greater the effect of pointing error on the system's secrecy performance under both eavesdropper modes. Also, it can be deduced in comparison with the non-colluding and the same number of eavesdroppers that

$$ASC^{nc} = \frac{1}{\ln(2)} \sum_{g=0}^{N} \binom{N}{g} (-1)^g \, \Xi_g \Omega_e^{\Upsilon_e} [\Gamma(\Upsilon_e + 1)\, \psi(\Upsilon_e + 1, \Upsilon_e + 1; g\Omega_e) + \mathcal{D} \times \sum_{n=0}^{m_r - 1} \frac{(m_r - 1)!}{n!(\Omega_r + g\Omega_e)} G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1} \left(\begin{matrix} 1 \\ 0 \end{matrix} \middle| \begin{matrix} m_r + \Upsilon_e \\ m_r + \Upsilon_e \end{matrix} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \middle| \frac{1}{(\Omega_r + g\Omega_e)}, \frac{E}{\bar{\gamma}_f^r (\Omega_r + g\Omega_e)} \right) \right] \tag{26}$$

$$ASC^{c} = \frac{1}{\ln(2)} \left[\left[\sum_{k=0}^{Nm_e - 1} \frac{(Nm_e - 1)!}{k!} \Gamma(k+1)\, \psi(k+1, k+1; \Omega_e) \right] + \mathcal{D} \times \sum_{n=0}^{m_r - 1} \sum_{k=0}^{Nm_e - 1} \frac{(Nm_e - 1)!\,(m_r - 1)!}{(\Omega_r + \Omega_e) k! n!} G_{1,0;1,1;r+1,3r+1}^{1,0;1,1;3r,1} \left(\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} n+k \\ n+k \end{matrix} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \middle| \frac{1}{\Omega_r + \Omega_e}, \frac{E}{\bar{\gamma}_f^r (\Omega_r + \Omega_e)} \right) \right] \tag{27}$$

$$ASC_{nc}^{\infty} \cong \frac{1}{\ln(2)} \sum_{g=0}^{N} \binom{N}{g} (-1)^g \, \Xi_g \Omega_e^{\Upsilon_e} [\Gamma(\Upsilon_e + 1)\, \psi(\Upsilon_e + 1, \Upsilon_e + 1; g\Omega_e) + \frac{\mathcal{D}\,(\Omega_r)^{m_r}}{(g\Omega_e) m_r \Gamma(m_r)} G_{1,0:1,1:r+1,3r+1}^{1,0:1,1:3r,1} \left(\begin{matrix} 1 \\ 0 \end{matrix} \middle| \begin{matrix} \Upsilon_e \\ \Upsilon_e \end{matrix} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \middle| \frac{1}{(g\Omega_e)}, \frac{E}{\bar{\gamma}_f^r (g\Omega_e)} \right) \right] \tag{29}$$

$$ASC_{c}^{\infty} \cong \frac{(Nm_e - 1)!}{\ln(2)\Gamma(Nm_e)} \sum_{k=0}^{Nm_e - 1} \frac{(\Omega_e)^k}{k!} \left[\left[\frac{1}{\Gamma(m_e)} \Gamma(k+1)\, \psi(k+1, k+1; \Omega_e) \right] + \frac{\mathcal{D}\,(\Omega_r)^{m_r}}{\Omega_e m_r \Gamma(m_r)} G_{1,0;1,1;r+1,3r+1}^{1,0;1,1;3r,1} \left(\begin{matrix} 1 \\ - \end{matrix} \middle| \begin{matrix} k \\ k \end{matrix} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \middle| \frac{1}{\Omega_e}, \frac{E}{\bar{\gamma}_f^r (\Omega_e)} \right) \right] \tag{30}$$

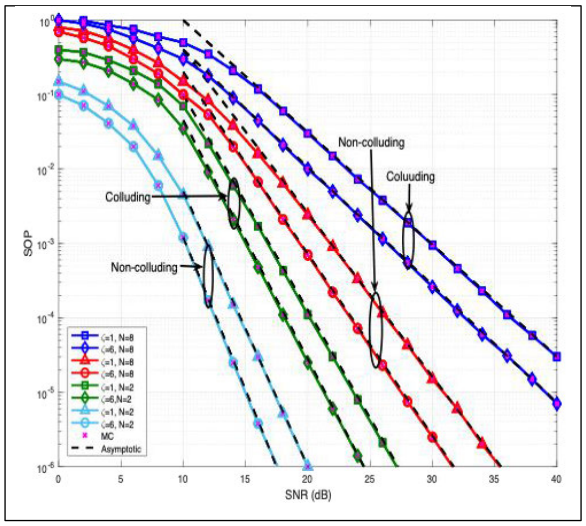

FIGURE 3. SOP versus the average SNR for selected values of ξ and N where $\alpha = 2.04$, $\beta = 1.10$, $\gamma_e = 1dB$, $m_r = m_e = 2$.

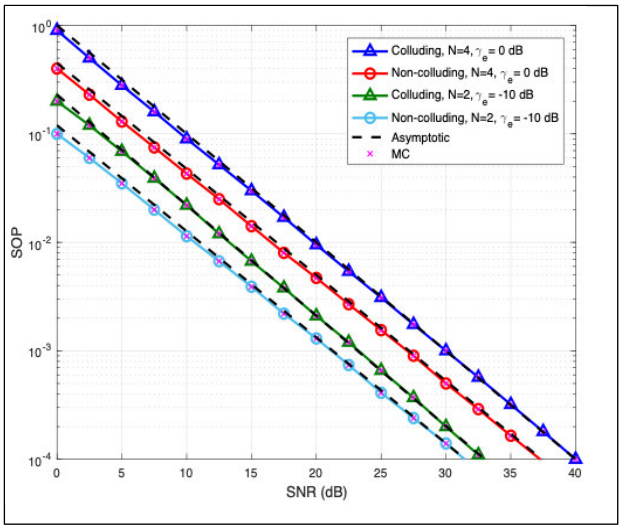

FIGURE 4. SOP versus the average SNR for selected values of γ_e and N where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $m_r = m_e = 2$.

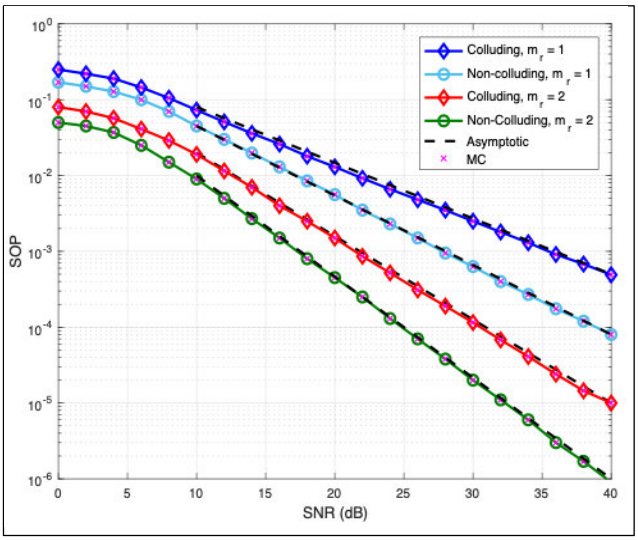

FIGURE 5. SOP versus the average SNR for selected values of m_r where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $\gamma_e = 1dB$, $m_e = 2$, and $N = 4$.

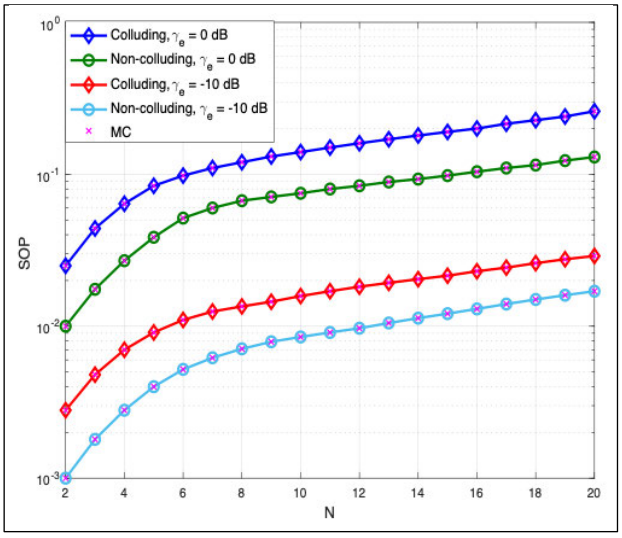

FIGURE 6. SOP versus the number of the eavesdroppers N, where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $m_r = m_e = 2$, and $N = 4$.

the colluding mode had a strongly negative impact on SOP performance. In addition, the obvious degradation in SOP performance of the system can be noted with the increasing of N. For the analytical curve corresponding to the low value of pointing error, $\xi = 6$, and N increases from 2 to 8, the investigated system loses approximately 13 dB at SOP of 10^{-5} under non-colluding eavesdropping scenario. While under the colluding scenario, the system loses about 15 dB for the same values of ξ and N.

Figure 4 illustrates the SOP performance for selected values of the wiretap links' average SNR γ_e, and N. This figure shows that the case with a greater number of eavesdroppers $N = 4$ and high value of γ_e, $\gamma_e = 0$ dB, provides poor secrecy performance in both eavesdropping scenarios.

Moreover, it can be observed that for the same values of N and γ_e, the investigated system provides better results in a non-colluding case. For example, with SOP of 10^{-4}, there is about 7 dB SNR losses as γ_e and N shifted from -10 dB and 2 to 0 dB and 4 respectively in the colluding case.

The SOP versus the average SNR of the considered system under selected values of the legitimate RF link's fading severity parameter, m_r at strong turbulence condition is shown in Fig. 5. We find that the system's secrecy performance has greatly deteriorated when the main channel experiences significant fading (i.e., lower values of the fading severity parameter m_r), particularly under the colluding eavesdropping mode.

Furthermore, the asymptotic curves (SOP^{∞}) match tightly the exact ones (SOP), which proves the accuracy of the retrieved expressions in high SNR values (i.e., $\geq$10) as can be seen all in the previous figures.

Figure 6 depicts the SOP performance against the various numbers of the eavesdroppers N for selected values of γ_e. As expected, the rise in the number of eavesdroppers

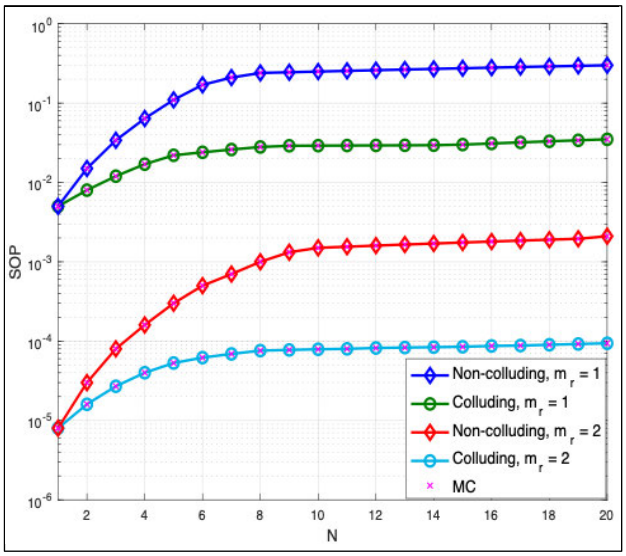

FIGURE 7. SOP versus the number of eavesdroppers and selected $\mathbf{m_r}$ where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $\gamma_e = 1dB$, $m_e = 2$, and $N = 4$.

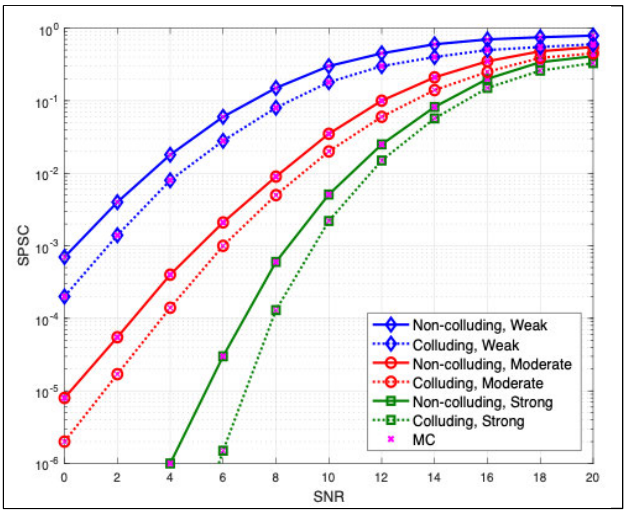

FIGURE 8. SPSC versus the average SNR under different turbulence effects where $\gamma_e = 1dB$, $\varepsilon = 6$, $m_r = m_e = 2$, and $N = 4$.

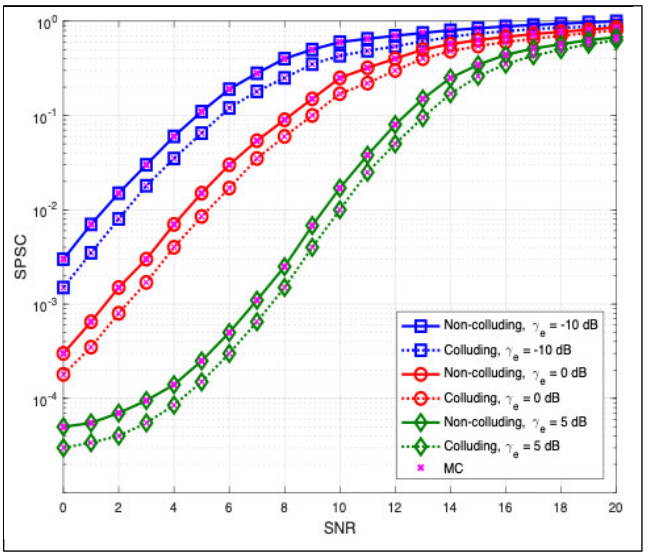

FIGURE 9. SPSC versus the average SNR for selected γ_e where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $m_r = m_e = 2$, and $N = 4$.

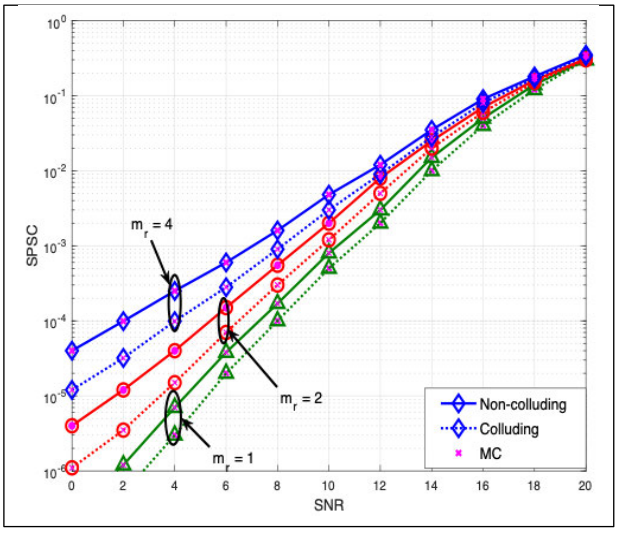

FIGURE 10. SPSC versus average SNR for selected values of $\mathbf{m_r}$ where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $\gamma_e = 1dB$, $m_e = 2$, and $N = 4$.

triggered a clear decrease in the system's SOP performance, which is more pronounced under the colluding mode. Also, for both modes, increasing γ_e causes a considerable loss of secrecy performance, especially for colluding case. For example, at the low value of γ_e, $\gamma_e = -10\ dB$, and $N = 20$, the system achieves SOP of 1.8×10^{-2} under the non-colluding case which reduces to 3×10^{-2} under the colluding one. While under a high value of γ_e, $\gamma_e = 0\ dB$, the SOP deteriorates to 1.4×10^{-1} and 2.6×10^{-1} under the non-colluding and colluding mode respectively. As is apparent, the probability of the system being secrecy outage increases as the number of eavesdroppers rises, highlighting the negative impact of a large number of eavesdroppers on the PLS performance of the investigated system.

Then we continue to evaluate the effect of the eavesdropper's number N and fading severity parameter m_r on the SOP performance in Fig. 7. As we can see, with the increasing of N, the probability of the investigated system being outage is significantly increased. Also, it is observed that, for the non-colluding mode, the influence of N on the SOP is limited. While, for the colluding mode, the rise in N would cause considerable losses in the SOP. Increasing in fading severity has also led to a clear deterioration of the system's security performances because the eavesdroppers received low SNR values at higher m_r. It is also noticed from the results that the analytical results agree with simulation results which validate the accuracy of the derived SOP expression.

Now shifting to the probability of strictly positive secrecy capacity of the considered system, three figures (Fig. 8, Fig. 9, and Fig.10) are provided. Fig. 8 illustrates the SPSC versus the average SNR under various atmospheric turbulence conditions that affected the legitimate FSO link of the main channel. From this figure, we can see that the SPSC performance

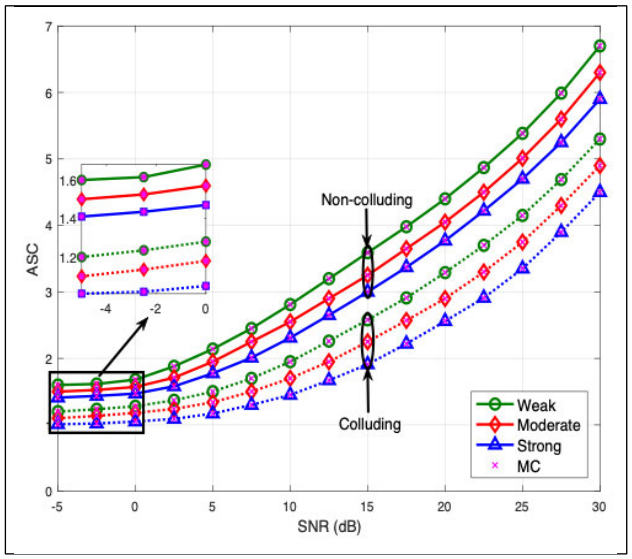

FIGURE 11. ASC versus the average SNR for different turbulence conditions where $\varepsilon = 6$, $m_r = m_e = 2$, $\gamma_e = 1dB$, and $N = 4$.

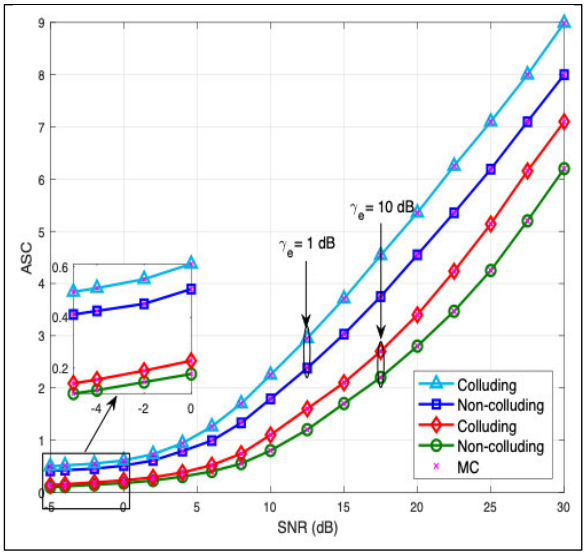

FIGURE 12. ASC versus the average SNR for selected values of γ_e where $\alpha = 2.04$, $\beta = 1.10$, $\varepsilon = 6$, $m_r = m_e = 2$, and $N = 4$.

deteriorates further as the influence of turbulence has become stronger. The degradation of secrecy performance is more apparent in the case of a colluding mode of eavesdropping.

Figure 9 demonstrates the SPSC versus the average SNR for the selected values of γ_e. As expected, a clear improvement can be noticed in the SPSC performance when γ_e decreases. This can be related to the huge deterioration in the wiretap channel with the decreasing of power received by the eavesdroppers with the reduction of γ_e. For instance, at SNR of 10 dB, the SPSC for $\gamma_e = -10, 0, 5$ dB is 7×10^{-1}, 3×10^{-1} and 2×10^{-2} respectively under the non-colluding eavesdropping mode.

Figure 10 shows the SPSC versus the average SNR for selected values of the fading severity parameter, m_r. As the results in the figure indicate, the obvious improvement in the

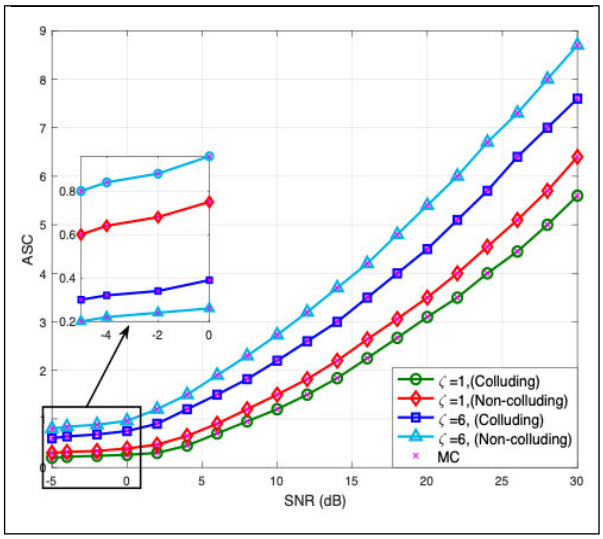

FIGURE 13. ASC versus the average SNR for selected values of ε where $\alpha = 2.04$, $\beta = 1.10$, $\gamma_e = 1dB$, $m_r = m_e = 2$, and $N = 4$.

SPSC performances can be noticed with the reduction of m_r and the enhancement is more obvious in the non-colluding case. The reason behind that is related to the increasing of the SNR values received by the legitimate receiver with the decreasing of the fading severity over the RF link of the main channel.

Figure 11 depicts the average secrecy capacity versus the average SNR under different atmospheric turbulence conditions. It can be seen that the worst ASC performance is obtained for a strong turbulence effect compared to weak turbulence under both eavesdropping modes, although the colluding scenario shows deeper adverse effects. This indicates that stronger turbulence affects the SNR received by the legitimate receiver more significantly than the weaker turbulence. And as mentioned before, in the case of colluding eavesdropping mode, more eavesdroppers can exchange and combine the received information to decode the confidential message over the main channel.

The impact of the average SNR of the wiretap channel, γ_e on the ASC performance of the investigated system is seen in Fig. 12. As can be seen in this figure, the higher value of γ_e induced a decrease in ASC performance under both modes with a more serious effect in the case of colluding mode. This is due to the channel quality of legitimate link gets worse than eavesdropper link which is related to high values of SNR at the eavesdropper terminal with higher γ_e, $\gamma_e = 10dB$.

In Fig. 13, the impact of the pointing error over the FSO link on ASC performance under both eavesdropper modes is analyzed. From this figure, it is indicated that ASC performance improves as the value of ε increases. Also, the ASC variations due to the pointing error caused by jitter are further obvious in the case of the colluding eavesdropping.

From Fig. 11- Fig. 13, it can be observed at low SNR values, i.e., > 10 dB, the ASC performance curves converges quite fast to each other under all channel conditions. As can be readily observed, the analytical results are in perfect

agreement with the simulation results, which confirm the accuracy of the closed-form analytical expressions of (26) and (27). In general, the ability of colluding eavesdroppers to share their observations and decode confidential messages together resulted in more detrimental in system secrecy compared to the case of non-colluding eavesdroppers.

V. CONCLUSION

In this paper, a hybrid FSO/RF system is analyzed from the physical layer secrecy performance perspective. To analyze the system in-depth, the colluding and non-colluding eavesdropping modes are considered. The analytical closed-form expressions for both mode in terms of SOP, SOP$^{\infty}$, SPSC, ASC and ASC$^{\infty}$ are obtained and verified by simulation. From the given results, a reduction in the value of the SOP, SOP$^{\infty}$, SPSC, and ASC can be observed when the value of α, β, γ, m_r of the main channel decrease or/and m_e of the wiretap channel increase. Moreover, the secrecy performances of the system improve when γ_e of the eavesdropper reduces because the legitimate link ''occupy'' the ''best'' signal. However, one can be concluded that colluding eavesdropping has a significant negative effect on the secrecy behavior of the physical layer of the considered system compared with a non-colluding case. Also, it can de deduce that under both eavesdropping modes, increasing of N deteriorates profoundly the system's secrecy performance.

APPENDIX A
PROOF OF THEOREM 1

The *SOP* of the hybrid FSO/RF system under non-colluding eavesdropping mode, SOP^{nc} can be written as follows:

$$SOP^{nc} = \int_0^{\infty} f_{\gamma_e^{nc}}(\gamma)\, F_{eq}\left((1+\gamma)\,\emptyset - 1\right) d\gamma \tag{31}$$

Substituting the expressions of $f_{\gamma_e^{nc}}(\gamma)$ in (6) and $F_{eq}(\gamma)$ in (12) into (31), SOP^{nc} can be further expressed as

$$\begin{aligned} SOP^{nc} = {} & \frac{N}{\Gamma(m_e)} \sum_{g=0}^{N-1} \binom{N-1}{g} (-1)^g\, \Xi_g \Omega_e^{m_e+\Upsilon_e} \mathcal{D} \\ & \int_0^{\infty} \gamma^{m_e+\Upsilon_e+1} e^{-(g+1)\Omega_e\gamma} G_{r+1,3r+1}^{3r,1} \\ & \times \left(\frac{E((1+\gamma)\,\emptyset - 1)}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) \\ & \times \frac{1}{\Gamma(m_r)} \Gamma_{inc}\left(m_r, \Omega_r((1+\gamma)\,\emptyset - 1)\right) d\gamma \end{aligned} \tag{32}$$

After some manipulation, (32) can be expressed as

$$\begin{aligned} SOP^{nc} = {} & \mathcal{H}_1 \int_0^{\infty} \gamma^{m_e+\Upsilon_e+1} e^{-((g+1)\Omega_e)((1+\gamma)\emptyset - 1)} \\ & \times G_{r+1,3r+1}^{3r,1} \left(\frac{E((1+\gamma)\,\emptyset - 1)}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) \\ & \times \Gamma_{inc}\left(m_r, \Omega_r((1+\gamma)\,\emptyset - 1)\right) d\gamma \end{aligned} \tag{33}$$

where

$$\mathcal{H}_1 = \frac{N\mathcal{D}}{\Gamma(m_e)\Gamma(m_r)} \sum_{g=0}^{N-1} \binom{N-1}{g} (-1)^g\, \Xi_g \Omega_e^{m_e+\Upsilon_e} \tag{34}$$

The integral of (33) is solved by using the following modification: $[x = (1+\gamma)\,\emptyset - 1]$, and making use of the following equality: $[(1-\emptyset)+x]^{m_e+\Upsilon_e+1} = \sum_{m=0}^{m_e+\Upsilon_e+1} \left(\frac{m_e+\Upsilon_e+1}{m}\right) x^m (1-\emptyset)^{m_e+\Upsilon_e+1-m}$ [41. eq. (1.111)] to obtain,

$$\begin{aligned} SOP^{nc} = {} & \mathcal{H}_1 e^{\left(\frac{-(g+1)(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{m=0}^{m_e+\Upsilon_e+1} \left(\frac{m_e+\Upsilon_e+1}{m}\right) \\ & \times \frac{(1-\emptyset)^{m_e+\Upsilon_e+1-m}}{\emptyset^{(m_e+\Upsilon_e+2)}} \left[\mathcal{H}_2 + \mathcal{H}_3\right] \end{aligned} \tag{35}$$

where

$$\begin{aligned} \mathcal{H}_2 = {} & \int_0^{\infty} x^m exp\left(-(g+1)\,\Omega_e.x\right) \\ & \times G_{r+1,3r+1}^{3r,1} \left(\frac{Ex}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) \Gamma_{inc}\left(m_r, \Omega_r x\right) dx \end{aligned} \tag{36}$$

$$\begin{aligned} \mathcal{H}_3 = {} & \int_{\emptyset-1}^{\infty} x^m exp\left(-(g+1)\,\Omega_e.x\right) \\ & \times G_{r+1,3r+1}^{3r,1} \left(\frac{Ex}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) \Gamma_{inc}\left(m_r, \Omega_r x\right) dx \end{aligned} \tag{37}$$

The integral of (36) can be computed in the following way: first we express the lower incomplete Gamma function in terms of [38, eq. (06.06.06.0005.01)] as:

$\Gamma_{inc}(n,x) = (n-1)!e^{-x} \sum_{w=0}^{n-1} \frac{x^w}{w!}$, and by further expressing the exponential function in terms of Taylor series: $e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!}$ [41, eq. (1.211.1)], (i.e., $\sum_{j=0}^{\infty} f_j(x)$ on $\mathbb{R}$ included an infinite series that converges for any x [41]) and utilize [42], eq. (8.4.3.3)] and further involve [38], eq. (07.34.21.0011.01)] to obtain

$$\begin{aligned} \mathcal{H}_2 = {} & (m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} \int_0^{\infty} x^{m+s} \\ & G_{0,1}^{1,0} \left(\left((g+1)\,\Omega_e + \Omega_r\right) x \middle| \begin{matrix} - \\ 0 \end{matrix} \right) \\ & G_{r+1,3r+1}^{3r,1} \left(\frac{Ex}{\bar{\gamma}_f^r} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) dx \\ = {} & (m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} [(g+1)\,\Omega_e + \Omega_r]^{-(m+s+1)} \\ & \times G_{r+2,3r+1}^{3r,2} \left(\frac{E}{\bar{\gamma}_f^r [(g+1)\,\Omega_e + \Omega_r]} \middle| \begin{matrix} -(m+s), 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \right) \end{aligned} \tag{38}$$

Next, we compute the closed-form solution of $\mathcal{H}_3$ by expressing the exponential term in using the same equality of [41], eq. (1.211.1)], then solve the resultant integral by utilizing the antiderivative:

$$\int x^{\alpha-1} G_{p,q}^{m,n}\left(wx \mid \begin{matrix}\mathcal{A}\\ \mathcal{B}\end{matrix}\right) dx = x^{\alpha} G_{p+1,q+1}^{m,n+1}\left(wx \mid \begin{matrix}1-\alpha, \mathcal{A}\\ \mathcal{B}, -\alpha\end{matrix}\right)$$

[38], eq. (07.34. 21. 0013.01)], the integral of $\mathcal{H}_3$ is solved as

$$\begin{aligned}\mathcal{H}_3 &= (m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} \int_{\emptyset-1}^{0} x^{m+s} exp(-(g+1)\\ &\times \Omega_e x - \Omega_r x) G_{r+1,3r+1}^{3r,1}\left(\frac{Ex}{\bar{\gamma}_f^r}\middle| \begin{matrix}1, \kappa_1\\ \kappa_2, 0\end{matrix}\right) dx\\ &= -(m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} \sum_{w=0}^{\infty} \frac{(\emptyset-1)^{m+s+w+1}}{w!}\\ &\times [-(g+1)\Omega_e - \Omega_r]^{-w} G_{r+2,3r+2}^{3r,2}\\ &\times \left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix}-(m+s+w), 1, \kappa_1\\ \kappa_2, 0, -(m+s+w+1)\end{matrix}\right) \end{aligned} \quad (39)$$

Substitutions (38) and (39) in (35), we obtain the exact expression of SOP under the non-colluding mode, SOP^{nc} as given in (15).

To find the SOP in the colluding mode SOP^{c}, we substitute (9) and (12) into (14) as

$$\begin{aligned}SOP^{c} &= \frac{D(\Omega_e)^{Nm_e}}{\Gamma(Nm_e)\Gamma(m_r)} \int_{0}^{\infty} \gamma^{Nm_e}\\ &\times exp(-\Omega_e\gamma)\, G_{r+1,3r+1}^{3r,1}\left(\frac{E((1+\gamma)\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix}1, \kappa_1\\ \kappa_2, 0\end{matrix}\right)\\ &\times \Gamma_{inc}(m_r, \Omega_r((1+\gamma)\emptyset-1))\, d\gamma \end{aligned} \quad (40)$$

Follow the same rational of finding SOP^{nc}, then we have SOP^{c} as

$$\begin{aligned}SOP^{c} &= \mathcal{H}_4 \emptyset^{-Nm_e} e^{\left(\frac{-(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{k=0}^{Nm_e-1}\left(\frac{Nm_e-1}{k}\right)\\ &\times (1-\emptyset)^{Nm_e+1-k}(\mathcal{H}_5+\mathcal{H}_6) \end{aligned} \quad (41)$$

here

$$\mathcal{H}_4 = \frac{D(\Omega_e)^{Nm_e}}{\Gamma(Nm_e)\Gamma(m_r)} \quad (42)$$

Now, by following the same previous steps of finding $\mathcal{H}_2$ and $\mathcal{H}_3$ to find $\mathcal{H}_5$ and $\mathcal{H}_6$, we have the following

$$\begin{aligned}\mathcal{H}_5 &= (m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} [\Omega_e+\Omega_r]^{-(k+s+1)}\\ &\times G_{r+2,3r+1}^{3r,2}\left(\frac{E}{\bar{\gamma}_f^r[\Omega_e+\Omega_r]}\middle| \begin{matrix}-(k+s), 1, \kappa_1\\ \kappa_2, 0\end{matrix}\right) \end{aligned} \quad (43)$$

$$\begin{aligned}\mathcal{H}_6 &= -(m_r-1)! \sum_{s=0}^{m_r-1} \frac{(\Omega_r)^s}{s!} \sum_{w=0}^{\infty} \frac{(\emptyset-1)^{k+s+w+1}}{w!}\\ &[-\Omega_e-\Omega_r]^{-w} G_{r+2,3r+2}^{3r,2}\\ &\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix}-(k+s+w), 1, \kappa_1\\ \kappa_2, 0, -(k+s+w+1)\end{matrix}\right) \end{aligned} \quad (44)$$

By plugging (43) and (44) into (41), we have the final expression of the SOP^{c} as provided in (16) which completes the proof.

APPENDIX B
PROOF OF THEOREM 2

Inserting the expressions of (6) and (13) into (17) and utilizing a similar rationale as in (36)-(39) to derive SOP^{nc}, the asymptotic SOP under the non-colluding mode, SOP_{nc}^{∞} can be expressed by

$$\begin{aligned}SOP_{nc}^{\infty} &\cong \frac{\mathcal{H}_1 (\Omega_r)^{m_r}}{m_r} e^{\left(\frac{-(g+1)(1-\emptyset)\Omega_e}{\emptyset}\right)} \sum_{m=0}^{m_e+\Upsilon_e+1}\\ &\times \left(\frac{m_e+\Upsilon_e+1}{m}\right) \frac{(1-\emptyset)^{m_e+\Upsilon_e+1-m}}{\emptyset^{(m_e+\Upsilon_e+2)}} [\mathcal{H}_7-\mathcal{H}_8] \end{aligned} \quad (45)$$

here $\mathcal{H}_1$ is previously calculated by (34) and

$$\begin{aligned}\mathcal{H}_7 &= \sum_{q=0}^{m_r-1} \frac{(m_r-1)!(\Omega_r)^q}{q!} [(g+1)\Omega_e+\Omega_r]^{-(m+q+1)}\\ &\times G_{r+2,3r+1}^{3r,2}\left(\frac{E}{\bar{\gamma}_f^r[(g+1)\Omega_e+\Omega_r]}\middle| \begin{matrix}-(m+q), 1, \kappa_1\\ \kappa_2, 0\end{matrix}\right) \end{aligned} \quad (46)$$

$$\begin{aligned}\mathcal{H}_8 &= \sum_{q=0}^{m_r-1} \frac{1}{q!} \left[\frac{(g+1)\Omega_e}{\emptyset}\right]^{q} (\emptyset-1)^{m_r+m+q+1}\\ &\times G_{r+2,3r+2}^{3r,2}\left(\frac{E(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix}-(m_r+m+q), 1, \kappa_1\\ \kappa_2, 0, -(m_r+m+q+1)\end{matrix}\right) \end{aligned} \quad (47)$$

Substituting (46) and (47) into (45), we obtain the asymptotic expression for SOP_{nc}^{∞} as in (18).

For the colluding eavesdropping case, SOP^{∞} is indicating here as SOP_{c}^{∞} and can be calculated by plugging (9) and (13) in (17) and using a similar argument as in (40)-(44) to derive

the SOP^{c} expression, as

$$SOP_{c}^{\infty} \cong \frac{\mathcal{H}_4\,(\Omega_r)^{m_r}}{m_r} e^{\left(\frac{(\emptyset-1)\Omega_e}{\emptyset}\right)} \sum_{k=0}^{Nm_e-1} \binom{Nm_e-1}{k} \times \frac{(\emptyset-1)^{Nm_e-1+k}}{\emptyset^{Nm_e}} \left[\mathrm{H}_9 - \mathrm{H}_{10}\right] \tag{48}$$

where $\mathcal{H}_4$ is previously defined by (42) and

$$\mathcal{H}_9 = \sum\nolimits_{q=0}^{m_r-1} \frac{(m_r-1)!\,(\Omega_r)^q}{q!} [\Omega_e+\Omega_r]^{-(m_r+k+q+1)} \times G_{r+2,3r+1}^{3r,2}\left(\frac{E}{\bar{\gamma}_f^r[\Omega_e+\Omega_r]}\middle| \begin{matrix} -(m_r+k+q),\,1,\,\kappa_1 \\ \kappa_2,\,0 \end{matrix}\right) \tag{49}$$

$$\mathcal{H}_{10} = \sum_{q=0}^{m_r-1} \frac{1}{q!}\left[\frac{\Omega_e}{\emptyset}\right]^q (\emptyset-1)^{m_r+m+q+1} \times G_{r+2,3r+2}^{3r,2}\left(\frac{E\,(\emptyset-1)}{\bar{\gamma}_f^r}\middle| \begin{matrix} -(m_r+k+q),\,1,\,\kappa_1 \\ \kappa_2,\,0,\,-(m_r+k+q+1) \end{matrix}\right) \tag{50}$$

Thus, by substituting (49) and (50) in (48), we obtained the final expression of SOP_{c}^{∞} as in (19), and this completes the proof.

APPENDIX C
PROOF OF THEOREM 3

For the non-colluding eavesdropping mode, the average secrecy capacity can be calculated by inserting (7) and (12) in (25) as

$$ASC^{nc} = \frac{1}{\ln(2)}\left(\mathcal{H}_{11}+\mathcal{H}_{12}\right) \tag{51}$$

where $\mathcal{H}_{11} = \int_0^{\infty} \frac{F_{\gamma_e}^{nc}(\gamma)}{1+\gamma} d\gamma$ and $\mathcal{H}_{12} = \int_0^{\infty} \frac{F_{\gamma_e}^{nc}(\gamma) F_{\gamma_{eq}}(\gamma)}{1+\gamma} d\gamma$. Now,

$$\mathcal{H}_{11} = \sum_{g=0}^{N} \binom{N}{g} (-1)^g\, \Xi_g\, \Omega_e^{\Upsilon_e} \underbrace{\int_0^{\infty} \frac{\gamma^{\Upsilon_e} exp^{(-g\Omega_e\gamma)}}{1+\gamma} d\gamma}_{\mathcal{H}_{13}} \tag{52}$$

and

$$\mathcal{H}_{13} = \int_0^{\infty} \frac{\gamma^{\Upsilon_e} e^{(-g\Omega_e\gamma)}}{1+\gamma} d\gamma \tag{53}$$

Based on (2.3.6.9) of [43], (53) can be simplified to

$$\mathcal{H}_{13} = \Gamma\left(\Upsilon_e+1\right)\psi\left(\Upsilon_e+1,\,\Upsilon_e+1;\,g\Omega_e\right) \tag{54}$$

Then by substituting (54) in (52), we have $\mathcal{H}_{11}$ of (52).

In (54), $\psi\,(\mathrm{a},\,\mathrm{b};c) = \frac{1}{\Gamma(\mathrm{a})} \int_0^{\infty} e^{-ct} t^{a-1} (1+t)^{b-a-1} dt$ represented the confluent hypergeometric function, as defined by (9.211.4) of [41]. Now we have H_{12} of (51) as

$$\mathcal{H}_{12} = \sum_{g=0}^{N} \binom{N}{g} \frac{(-1)^g\, \Xi_g\, \Omega_e^{\Upsilon_e} D}{\Gamma\,(m_r)} \underbrace{\int_0^{\infty} \frac{1}{1+\gamma} \gamma_e e^{-g\Omega_e\gamma} G_{r+1,3r+1}^{3r,1}\left(\frac{E\gamma}{\bar{\gamma}_f^r}\middle| \begin{matrix} 1,\,\kappa_1 \\ \kappa_2,\,0 \end{matrix}\right) \Gamma_{inc}(m_r.\Omega_r\gamma) dr}_{\mathcal{H}_{14}} \tag{55}$$

and

$$\mathcal{H}_{14} = \int_0^{\infty} \frac{1}{1+\gamma} \gamma^{\Upsilon_e} e^{-g\Omega_e\gamma} \times G_{r+1,3r+1}^{3r,1}\left(\frac{E\gamma}{\bar{\gamma}_f^r}\middle| \begin{matrix} 1,\,\kappa_1 \\ \kappa_2,\,0 \end{matrix}\right) \Gamma_{inc}\left(m_r,\,\Omega_r\gamma\right) d\gamma \tag{56}$$

By using (10) and (11) of [44], (06.06.06.005.01) of [38], and (20) of [45], together to simplify the integration of (56), we have

$$\mathcal{H}_{14} = \sum_{n=0}^{m_r-1} \frac{(m_r-1)!}{n!(\Omega_r+g\Omega_e)} G_{1,0:1,1:3r,1}^{1,0:1,1:r+1,3r+1} \left(\begin{matrix} 1 \\ 0 \end{matrix}\middle| \begin{matrix} m_r+\Upsilon_e \\ m_r+\Upsilon_e \end{matrix}\middle| \begin{matrix} 1,\,\kappa_1 \\ \kappa_2,\,0 \end{matrix}\middle| \frac{1}{(\Omega_r+g\Omega_e)},\,\frac{E}{\bar{\gamma}_f^r(\Omega_r+g\Omega_e)}\right) \tag{57}$$

where $G_{p1,q1;p2,q2;p3,q3}^{m1,n1;m2,n2;m3,n3}$ is the extended generalized bivariate Meijer's G-function (EGBMGF), as defined by (8) of [46]. This function can be conveniently evaluated using mathematical software such as MATLAB. Now, by inserting (54) in (52) and (57) in (55), we have the final analytical expression for the non-colluding mode ASC^{nc} as in (26).

In the same way, by plugging (10) and (12) in (25) and making use of (10) and (11) of [44], (06.06.06.005.01) of [38], and (20) of [45], we have the accurate expression for the colluding mode ASC^{c} as provided in (27) and in this case, the proof is completed.

APPENDIX D
PROOF OF THEOREM 4

For the non-colluding eavesdropping mode, the asymptotic of the average secrecy capacity ASC_{nc}^{∞} can be obtained by substituting (7) and (13) in (28) as

$$ASC_{nc}^{\infty} \cong \frac{1}{\ln(2)}\left(\mathcal{H}_{15}+\mathcal{H}_{16}\right) \tag{58}$$

where $\mathcal{H}_{15} = \int_0^{\infty} \frac{F_{\gamma_e}^{nc}(\gamma)}{1+\gamma} d\gamma$ and $\mathcal{H}_{16} = \int_0^{\infty} \frac{F_{\gamma_e}^{nc}(\gamma) F_{\gamma_{eq}}^{\infty}(\gamma)}{1+\gamma} d\gamma$.

Now, we have

$$\mathcal{H}_{15} = \mathcal{H}_{11} = \sum_{g=0}^{N} \binom{N}{g} (-1)^g\, \Xi_g\, \Omega_e^{\Upsilon_e} \left[\Gamma\left(\Upsilon_e+1\right)\psi\left(\Upsilon_e+1,\,\Upsilon_e+1;\,g\Omega_e\right)\right] \tag{59}$$

And by making use of (10) and (11) of [43], (9.31.5) of [41], and (20) of [45], we have

$$\mathcal{H}_{16} = \sum_{g=0}^{N} \binom{N}{g} \frac{(-1)^g \, \Xi_g \Omega_e^{\Upsilon_e} \Omega_r^{m_r} \mathcal{D}}{g\Omega_e m_r \Gamma(m_r)} G_{1,0:1,1:3r,1}^{1,0:1,1:r+1,3r+1} \left(\begin{matrix} 1 \\ 0 \end{matrix} \middle| \begin{matrix} m_r + \Upsilon_e \\ m_r + \Upsilon_e \end{matrix} \middle| \begin{matrix} 1, \kappa_1 \\ \kappa_2, 0 \end{matrix} \middle| \frac{1}{(\Omega_r + g\Omega_e)}, \frac{E}{\bar{\gamma}_f^r (\Omega_r + g\Omega_e)} \right) \tag{60}$$

Finally, by substituting (59) and (60) in (58), an asymptotic expression for ASC for non-colluding case of the investigated system can be seen in (29).

For the colluding eavesdropping mode, the average secrecy capacity ASC_{nc}^{∞} can be find by substituting (10) and (13) in (28) as

$$ASC_{nc}^{\infty} \cong \frac{1}{\ln(2)} \int_0^{\infty} \frac{F_{\gamma_e}^c(\gamma)}{1+\gamma} \left(1 + F_{\gamma_{eq}}^{\infty}(\gamma)\right) d\gamma \tag{61}$$

Following the same steps of (29), the proof of ASC_{nc}^{∞} in (30) can be accomplished.

REFERENCES

[1] A. M. Abdalla, J. Rodriguez, I. Elfergani, and A. Teixeira, *Optical and Wireless Convergence for 5G Networks*. Hoboken, NJ, USA: Wiley, 2020.

[2] A. K. Majumdar, Z. Ghassemlooy, and A. A. B. Raj, *Principles and Applications of Free Space Optical Communications* (IET Telecommunications Series). London, U.K.: IET, 2019.

[3] W. M. R. Shakir and A. S. Mahdi, "Errors rate analysis of the hybrid FSO/RF systems over foggy-weather fading-induced channel," in *Proc. IEEE 4th Sci. Int. Conf. Najaf (SICN)*, Al-Najef, Iraq, Apr. 2019, pp. 156–160.

[4] F. Nadeem, V. Kvicera, M. Awan, E. Leitgeb, S. Muhammad, and G. Kandus, "Weather effects on hybrid FSO/RF communication link," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1687–1697, Dec. 2009.

[5] K. O. Odeyemi and P. A. Owolawi, "Selection combining hybrid FSO/RF systems over generalized induced-fading channels," *Opt. Commun.*, vol. 433, pp. 159–167, Feb. 2019.

[6] W. M. R. Shakir, "On performance analysis of hybrid FSO/RF systems," *IET Commun.*, vol. 13, no. 11, pp. 1677–1684, Jul. 2019.

[7] W. M. R. Shakir, "Performance analysis of the hybrid MMW RF/FSO transmission system," *Wireless Pers. Commun.*, vol. 109, no. 4, pp. 2199–2211, Dec. 2019.

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

[9] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[10] D. Wang, W. Xu, X. Fan, and J. Cheng, "Privacy preserving with adaptive link selection for hybrid radio-frequency and free space optical networks," *Opt. Exp.*, vol. 27, no. 3, pp. 3121–3135, 2019.

[11] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-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.

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

[13] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[14] 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.

[15] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–10, Feb. 2016.

[16] 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.

[17] 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.*, vol. 27, no. 23, pp. 34211–34229, Nov. 2019.

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

[19] 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.

[20] 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. Lightwave Techn.*, vol. 35, no. 9, pp. 1490–1505, May 1, 2017.

[21] L. Yang, T. Liu, J. Chen, and M.-S. Alouini, "Physical-layer security for mixed $\eta - \mu$ and M-distribution dual-hop RF/FSO systems," *IEEE Trans. Veh. Techn.*, vol. 67, no. 12, pp. 12427–12431, Dec. 2018.

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

[23] 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.

[24] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[25] 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.

[26] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "On secrecy analysis of DF based dual hop mixed RF-FSO systems," *IEEE Access*, vol. 7, pp. 66725–66730, 2019.

[27] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020, doi: 10.1109/TCOMM.2020.2985028.

[28] J. Zhang, X. Pan, G. Pan, and Y. Xie, "Secrecy analysis for multi-relaying RF-FSO systems with a multi-aperture destination," *IEEE Photon. J.*, vol. 12, no. 2, pp. 1–11, Apr. 2020.

[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 cooperative system," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 1031–1035, Jul. 2020.

[30] 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, Dec. 2020, Art. no. 126334.

[31] 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, Nov. 2020, Art. no. 126193.

[32] M. Kafafy, Y. Fahmy, M. Khairy, and M. Abdallah, "Secure backhauling over adaptive parallel mmWave/FSO link," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/ICCWorkshops49005.2020.9145354.

[33] A. J. Navas, J. M. G. Balsells, J. F. Paris, and A. P. Notario, "A unifying statistical model for atmospheric optical scintillation," in *Numerical Simulations of Physical and Engineering Processes*, J. Awrejcewicz, Ed. Rijeka, Croatia: InTech, 2011, pp. 181–206.

[34] 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.

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

[36] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8009–8024, Dec. 2016.

[37] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion," *Opt. Quantum Electron.*, vol. 50, no. 7, pp. 1–19, Jul. 2018.
[38] *The Wolfram Functions Site*. Accessed: Oct. 1, 2020. [Online]. Available: http://functions.wolfram.com/
[39] H. Al-Hmood and H. Al-Raweshidy, "Performance analysis of physical-layer security over fluctuating Beckmann fading channels," *IEEE Access*, vol. 7, pp. 119541–119556, 2019.
[40] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Burlington, MA, USA: Academic, 2007.
[42] A. P. Prudnikov, I. A. Brychkov, and O. I. Marichev, *Integrals and Series: More Special Functions*, vol. 3. New York, NY, USA: CRC Press, 1992.
[43] A. P. Prudnikov, I. A. Brychkov, and O. I. Marichev, *Integrals and Series: Elementary Functions*, vol. 1. New York, NY, USA: Gordon & Breach, 1986.
[44] V. Adamchik and O. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. Int. Symp. Symbolic Algebr. Comput.*, Tokyo, Japan, 1990, pp. 212–224.
[45] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. Qaraqe, "On physical layer security over SIMO generalized-K fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.
[46] S. C. Gupta, "Integrals involving products of G-function," *Proc. Nat. Acad. Sci. USA*, vol. 39, no. 2, pp. 193–200, Apr. 1969.