Secrecy Performance Analysis of Parallel FSO/mm-wave System Over Unified Fisher-Snedecor Channels

Wafaa Mohammed Ridha Shakir, *Member, IEEE*, and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—This paper presents a secrecy performance analysis of a parallel free-space optical/millimeter-wave (mm-wave) communication system with a selection-combining receiver over a unified Fisher-Snedecor $\mathcal{F}$-distribution channel. The $\mathcal{F}$-distribution model, with the proper parameters, may be used to describe both the mm-wave and optical channels. The security performance is specifically evaluated by deriving closed-form expressions for the average secrecy capacity, secrecy outage probability, and strictly positive secrecy capacity. We examine the three following distinct security scenarios: 1) An FSO-link eavesdropping attack, 2) mm-wave-link eavesdropping attacks, and 3) eavesdropping attacks on FSO and mm-wave links at the same time. Furthermore, to better understand the influence of various system and channel parameters, asymptotic analysis is performed at high signal-to-noise ratio values. Our developed analytical expressions provide an efficient tool for examining the influence of various system and channel parameters on the secrecy performance, including the atmospheric turbulence severity, pointing errors of the FSO link, fading severity, the shadowing parameters, as well as the number of diversity branches of the mm-wave links. Monte-Carlo simulations are used to verify the correctness of the numerical findings.**

***Index Terms*—Parallel FSO/mm-wave system, $\mathcal{F}$-distribution, average secrecy capacity (ASC), secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), selection-combining receiver.**

I. Introduction

A. Background

THE increased requirement for extremely high data rates in next-generation mobile systems (5G and beyond) demands backhaul networks that are far more powerful and dependable than previous systems [1]. Due to its low capacity, traditional radio frequency (RF) backhaul might be limited by latency difficulties, although it has the advantage of being weather insensitive. Due to the broadcasting nature of radio wave propagation, RF communication is also vulnerable to eavesdropping attacks. Free space optical (FSO) communication, on the other hand, allows for high-rate and low-latency transmission while being very susceptible to atmospheric conditions and adverse weather impacts [2]. Furthermore, academic, and industrial communities believe that the extremely narrow divergence of FSO beams makes a physical interception and eavesdropping exceedingly difficult [3]–[5]. In order to combine the advantages of millimeter-wave (mm-wave) RF communication (resilience to atmospheric and weather effects) and FSO communication (secure transmission at a high data rate), a parallel setup of FSO and millimeter-wave (mm-wave) RF communication systems have been developed as a more reliable candidate solution for backhaul networks as an integral part of 5G systems and in a variety of other applications [6]. Because of the enormous potential of parallel FSO/mm-wave systems in next-generation mobile networks [1], many research has been conducted, notably in the field of performance analysis of such systems [7]–[11]. As different links confront different atmospheric disturbances, performance analysis of parallel FSO/mm-wave RF systems has inspired a lot of interest in the literature. The Fisher-Snedecor $\mathcal{F}$-distribution was recently presented to characterize the atmospheric turbulence over FSO links [12]. The $\mathcal{F}$-distribution model provided a better fit to the experimental data for all turbulence conditions compared to other FSO models. Furthermore, the probability density function (PDF) of this model includes very basic elementary functions; hence, it is mathematically simpler than other known distributions, namely the log-normal, Gamma-Gamma (G-G), and Malaga-M distributions [13]. Moreover, the $\mathcal{F}$-distribution was developed by the authors of [14] as a composite model for analyzing the impacts of multipath and shadowing in RF communications. The authors established in [14] that in the case of RF communications, the $\mathcal{F}$-distribution gives a more exact match than the generalized K- and lognormal composite distributions due to the PDF of the generalized- K having the non-elementary function, i.e., the modified Bessel function. In addition, the $\mathcal{F}$-distribution is flexible since it can be reduced to some special cases when the fading parameters are fixed for some values, i.e., Nakagami-m distribution, Rayleigh distribution, and one-sided Gaussian distribution [15].

Physical layer security (PLS) techniques have recently been proposed as a viable option for preventing adversary eavesdropping in parallel FSO/mm-wave RF systems by taking advantage of the unpredictability of time-varying wireless channels. Because of the strong directionality of the laser beam,

Manuscript received January 28, 2022; accepted February 12, 2022. Date of publication February 16, 2022; date of current version March 7, 2022. *(Corresponding author: Wafaa Mohammed Ridha Shakir.)*

Wafaa Mohammed Ridha Shakir is with the Computer Systems Department, Al-Furat Al-Awsat Technical University, Babil 51015, Iraq (e-mail: inb.wfa@atu.edu.iq).

Mohamed-Slim Alouini is with the Department of Computer, Electrical and Mathematical Science and Engineering, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia (e-mail: slim.alouini@kaust.edu.sa).

Digital Object Identifier 10.1109/JPHOT.2022.3151675

FSO links are regarded as more secure against unauthorized access than mm-wave RF links. However, eavesdropping may occur in a few instances owing to optical beam divergence, atmospheric turbulence, pointing errors, and adverse weather. Existing research on the secrecy performance of such systems is mostly limited to either single FSO link-based systems [16]–[19] or mixed FSO–RF relaying systems [20]–[34], and the secrecy performance of parallel FSO/mm-wave systems has not yet been thoroughly explored, according to a comprehensive open literature review. The secrecy performance analysis of the parallel FSO/RF system is performed across Malaga-M/η-μ distributions in [35], Malaga-M/Nakagami-m distributions in [4], [36], and [37]. We suggest a novel system structure for a parallel FSO/mm-wave system under a unified $\mathcal{F}$-distribution model for both links. In contrast to prior works, it is assumed that the eavesdroppers can overhear the intended information of the legitimate FSO- and mm-wave-link separately and simultaneously. However, taking into account both links' $\mathcal{F}$-fading impairments provides a significant problem in developing unique closed-form formulations for secrecy metrics, which we have greatly improved in our work. To the author's knowledge, no research has examined the impact of unified $\mathcal{F}$-fading on the secrecy of parallel FSO/mm-wave systems. Furthermore, past research has focused on eavesdropping attacks on legitimate RF links in parallel FSO/mm-wave systems but has never looked at simultaneous eavesdropping attacks on both channels under the influence of unified distributions for optical and radio links.

B. Motivation and Contributions

Despite their considerable potential as excellent candidates for future network backhaul and a variety of other applications, the secrecy performance of parallel FSO/mm-wave RF systems has not been widely examined in the open literature using a unified distribution to describe both links. In contrast to earlier secrecy performance study efforts on comparable systems [4], [35]–[37], which evaluated the FSO and RF links using different fading distributions, we propose the $\mathcal{F}$-distributions to describe both radio and optical links. The proposed unification of channel models would make it easy to track how different system and channel parameters affect the considered system security performance. Moreover, we analyze the secrecy performance of the considered system based on the assumption of maximal ratio combining (MRC) at the legitimate and eavesdropper receivers of the mm-wave links, since the diversity technique is an effective method to compact the multipath fading and shadowing [38].

Taking these benefits into account, we will present a secure scenario for a parallel FSO/mm-wave system over a unified $\mathcal{F}$-distribution turbulence and fading channels. In specifically, we assume that in the first scenario, an eavesdropper can wiretap transmitted data using just the FSO link, in the second scenario, only the mm-wave link, and in the third scenario, eavesdropping across both links simultaneously. To summarize, the following are the paper's contributions:

1) We first evaluate the cumulative distribution function (CDF) of the parallel FSO/mm-wave system with selection combining (SC) receiver using the CDF of each link with the $\mathcal{F}$-distributions. The major impairments and features of the FSO and mm-wave links are taken into account to make the study more realistic (e.g., multipath fading, shadowing effects and the number of diversity branches for the mm-wave links, and atmospheric turbulence and pointing errors conditions for the FSO links).
2) The exact analytical expressions of the average secrecy capacity (ASC), secrecy outage probability (SOP), and strictly positive secrecy capacity (SPSC) for the parallel FSO/mm-wave system are obtained for these three separate scenarios.
3) An asymptotic secrecy analysis for the ASC, SOP, and SPSC metrics is performed for the considered three eavesdropping scenarios to give some insightful information into the security performance of the parallel system under investigation.
4) These expressions are used to generate numerical results with specified figures. In addition, Monte-Carlo simulations verify the accuracy of the analytical results.

The following is the outline for this paper: Section II presents models of the parallel system and channel in consideration, while Section III develops an analytical expression for the three eavesdropping scenarios for the ASC, SOP, and SPSC, as well as their asymptotic expressions. Section IV has several interesting numerical examples as well as instructive discussions. Finally, Section V brings the paper to a conclusion.

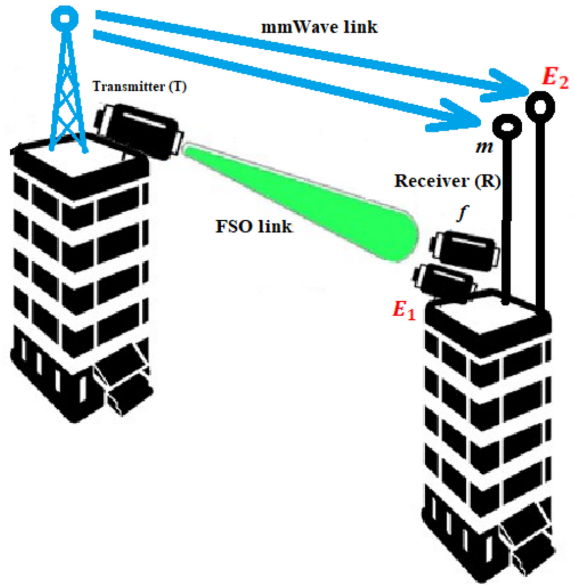

Fig. 1. Parallel FSO/mm-wave system model depicting the transmitter, receiver, and the eavesdropper E_1 and E_2.

II. System and Channel Models

A. System Model

We propose a parallel FSO/mm-wave system with parallel FSO and mm-wave legitimate transmission links, as shown in Fig. 1. During transmission, two unauthorized receivers (E_1 and E_2) attempt to intercept data at the FSO terminal of the legitimate receiver (which signifies f) and R's mm-wave terminal (which

denotes m) respectively. In this case, the considered system's transmitter (T) simultaneously sends a private message to the legal receiver R by both links. The selection combiner (SC) at the receiver R chooses the signal from the best link (i.e., the link with the highest signal-to-noise ratio (SNR)). Here, the parallel FSO/mm-wave link is considered the main channel, while the transmitter-to-eavesdropper links i.e., $T \to E_1$ and $T \to E_2$ are referred to as the wiretap channels. We consider the secure information transmission over the mm-wave link from a single antenna transmitter at T to L antenna legitimate receiver at m is wiretapped by L antenna eavesdropper. The receiver maximizes the probability of secure transmission by MRC, whereas the eavesdropper maximizes the probability of eavesdropping by adopting MRC.

B. Channel Model

The direct links between *T* and *R* are assumed to be severely faded. Due to the limitations of the eavesdropper location in the FSO systems and the practicality of its operating technique, it is assumed that the eavesdropper E_1 close to the optical terminal of the legitimate receiver f, since this is possibly the most probable case for eavesdropping in FSO communications [39] because the legitimate receiver serves as a reference for the eavesdropper to align its direction.

The $\mathcal{F}$-distribution describes the FSO link, and this model has very successfully approximated the link's atmospheric turbulence and pointing error impairments. Taking into account the heterodyne detection (HD) techniques for optical signal detection, the PDF, and CDF of instantaneous SNR; $\gamma_{Tk},\ (k \in \{f, E_1\})$ of the FSO links are described as follows [40], [41]

$$f_{\gamma_{Tk}}(\gamma) = \mathcal{A}_k\, \gamma_k^{\frac{a_k}{2}-1} G_{2,2}^{2,1}\left(\frac{\mathcal{B}_k\gamma}{\bar{\gamma}_{Tk}}\middle| \begin{matrix} 1-b_k, 1+\xi_k^2 \\ a_k, \xi_k^2, 0 \end{matrix}\right) \quad (1)$$

$$F_{\gamma_{Tk}}(\gamma) = \mathcal{A}_k\, \gamma_k^{\frac{a_k}{2}} G_{3,3}^{2,2}\left(\frac{\mathcal{B}_k\gamma}{\bar{\gamma}_{Tk}}\middle| \begin{matrix} 1-b_k,\ 1,\ 1+\xi_k^2 \\ a_k, \xi_k^2,\ 0 \end{matrix}\right). \quad (2)$$

In (1) and (2), $G_{p,q}^{m,n}(.)$ denotes the Meijer's G-function which is defined as the following [42, Eq. (9.301)]

$$G_{p,q}^{m,n}\left(\mathrm{z}\middle| \begin{matrix} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{matrix}\right) = \frac{1}{2\pi j} \int \frac{\prod_{i=1}^{m}\Gamma(b_i+s)\prod_{i=1}^{n}\Gamma(1-a_i-s)}{\prod_{i=m+1}^{q}\Gamma(1-b_i-s)\prod_{i=n+1}^{p}\Gamma(a_i+s)} z^s ds, \quad (3)$$

In which $0 \le m \le q$, $0 \le n \le p$, and $\Gamma(.)$ represented the Gamma function. $\mathcal{A}_k = \xi_k^2/\Gamma(a_k)\Gamma(b_k)$, $\mathcal{B}_k = a_k\ \ \xi_k^2/((b_k-1)(1+\xi_k^2))$, a and b are two key parameters that describe the atmospheric refractive index structure parameter, the propagation path length, and the inner and outer scale of turbulence, respectively [12]. The parameters, a, and b can be written as

$$a = \frac{1}{\exp(\sigma_{In\mathcal{S}}^2) - 1},\ and\ b = \frac{1}{\exp(\sigma_{In\mathcal{L}}^2) - 1} + 2, \quad (4)$$

where $\sigma_{In\mathcal{S}}^2$ and$\sigma_{In\mathcal{L}}^2$ correspond to the small- and large-scale log-irradiance variances, respectively. Assuming spherical wave propagation, the small-scale log-irradiance variance, $\sigma_{In\mathcal{S}}^2$, is given by [13]

$$\sigma_{In\mathcal{S}}^2 = \frac{0.51\ \delta_{SP}^2\left(1+0.69\delta_{SP}^{12/5}\right)^{-5/6}}{1+0.90d^2(\sigma_1/\delta_{SP})^{12/5}+0.62d^2\sigma_1^{12/5}}, \quad (5)$$

where δ_{SP}^2 represents the spherical wave scintillation index assuming weak irradiance fluctuations, which is given by [12]

$$\delta_{SP}^2 = 9.65\sigma_1^2\left\{0.4(1+9/Q_l^2)^{11/12}\left[\sin\left(\frac{11}{6}\arctan\frac{Q_l}{3}\right) + \frac{2.61}{(9+Q_l^2)^{1/4}}\sin\left(\frac{4}{3}\arctan\frac{Q_l}{3}\right) - \frac{0.52}{(9+Q_l^2)^{7/24}} \times \sin\left(\frac{5}{4}\arctan\frac{Q_l}{3}\right) - 3.5/Q_l^{5/6}\right\}, \quad (6)$$

where $Q_l = 10.89L/(\mathfrak{B}\ l_0^2)$ with L denoting the distance between the transmitter and the receiver and l_0 denoting the inner scale in mm. $d = \sqrt{\mathfrak{B}D^2/4L}$ denotes the equivalent aperture diameter, $\mathfrak{B}$ is the optical wave number, D is the receiving aperture diameter. Furthermore, $\sigma_1^2 = 0.5C_n^2\mathfrak{B}^{7/6}L^{11/6}$ is the Rytov variance, and C_n^2 is the atmospheric refractive index structure parameter, having units of $m^{-2/3}$. It is important to note that σ_1^2 defines the weak and moderate-to-strong irradiance fluctuations (i.e., $\sigma_1^2 < 1$ for weak and$\sigma_1^2 > 1$ for moderate to strong).

The large-scale log-irradiance variance $\sigma_{In\mathcal{L}}^2$ can be expressed as [13]

$$\sigma_{In\mathcal{L}}^2 = \sigma_{In\mathcal{L}}^2(l_0) - \sigma_{In\mathcal{L}}^2(L_0) \quad (7)$$

where $\sigma_{In\mathcal{L}}^2(l_0)$ and $\sigma_{In\mathcal{L}}^2(L_0)$ denote the large-scale log- irradiance variances that consider inner- and outer-scale effects, displacement standard deviation (jitter) at the receiver. The

PDF of the pointing error impairment is given by [43]

$$f(x) = \frac{\xi^2}{\mathbb{A}_0^{\xi^2}}\, x^{\xi^2-1},\ 0 \le x \le \mathbb{A}_0, \quad (8)$$

where $\mathbb{A}_0$ represents a constant term that defines the pointing loss. In addition, $\bar{\gamma}_{Tk}$ is the average SNR of the FSO links defined as $\bar{\gamma}_{Tk} \triangleq (\eta\mathbb{E}[I]/N_o)$, with η, I, $\mathbb{E}[.]$, N_o indicating the ratio of photoelectric, total channel gain, the expectation operator, and the variance of the additive white Gaussian noise (AWGN), respectively.

In this work, both legitimate (i.e., $T \to m$) and unauthorized (i.e., $T \to E_2$) mm-wave links are assumed to adopt the MRC consisting of L to combine the received signals across both $\mathcal{F}$-fading-affected links. The outputs from L receivers are co-phased, weighted, and then assumed to produce the corresponding SNR at the output of the combiner. The output SNR at the output of the L branch MRC combiner is determined by $\gamma_{Tj} \triangleq \sum_{l=1}^{L_j}\gamma_l$, where γ_l is the SNR at l branch. Thus, the PDF and CDF of the instantaneous SNR ($\gamma_{Tj};\ j \in \{m, E_2\}$)

of the mm-wave links is given by [44]

$$f_{\gamma_{Tj}}(\gamma) = \mathcal{C}_j\, \gamma_j^{m_j L_j - 1} G_{2,2}^{1,2}\left(\frac{\mathcal{D}_j \gamma}{\bar{\gamma}_{Tj}} \text{bigg}| \begin{matrix} 1-(m_j+s_j),\ 1-m_j L_j \\ 0, 1-m_j L_j \end{matrix}\right) \tag{9}$$

$$F_{\gamma_{Tj}}(\gamma) = \mathcal{C}_j\, \gamma_j^{m_j L_j} G_{2,2}^{1,2}\left(\frac{\mathcal{D}_j \gamma}{\bar{\gamma}_{Tj}} \middle| \begin{matrix} 1-(m_j+s_j),\ 1-m_j L_j \\ 0, -m_j L_j \end{matrix}\right), \tag{10}$$

in which $\mathcal{C}_j = \frac{1}{\Gamma(m_j L_j)\Gamma(m_j+s_j)}\left(\frac{m_j}{\bar{\gamma}_{Tj} s_j}\right)^{m_j L_j}\left[\frac{\Gamma(m_j+s_j)}{\Gamma(s_j)}\right]^{L_j}$, $\mathcal{D}_j = \frac{m_j}{s_j}$, and m_j, s_j, $\bar{\gamma}_{Tj}$ denote the multipath fading severity, shadowing characteristics of the mm-wave links, and the average SNR of the $T \to m$ or the $T \to E_2$ links, respectively.

C. Unified Statistic Characteristics of the Parallel FSO/mm-Wave System

When using an SC method at R, the CDF of the parallel system's equivalent SNR, i.e., $\gamma_{eq.R}$ is based on the SNRs of both legal links as shown in the following [4]

$$F_{\gamma_{eq.R}}(\gamma) = F_{\gamma_{Tf}}(\gamma)\, F_{\gamma_{Tm}}(\gamma). \tag{11}$$

The CDF of $\gamma_{eq.R}$ can be rewritten by replacing (2) and (10) into (11), as

$$\begin{aligned} F_{\gamma_{eq.R}}(\gamma) &= \mathcal{A}_f\, \mathcal{C}_m\, \gamma^{\frac{a_f}{2}+m_m L_m} G_{3,3}^{2,2}\left(\frac{\mathcal{B}_f\, \gamma}{\bar{\gamma}_{Tf}} \middle| \begin{matrix} 1-b_f, 1,\ 1+\xi_f^2 \\ a_f, \xi_f^2, 0 \end{matrix}\right) \\ &\times G_{2,2}^{1,2}\left(\frac{\mathcal{D}_m \gamma}{\bar{\gamma}_{Tm}} \middle| \begin{matrix} 1-(m_m+s_m), 1-m_m L_m \\ 0, -m_m L_m \end{matrix}\right). \end{aligned} \tag{12}$$

D. Asymptotic Analysis

To obtain insight into the influence of different system and channel characteristics on secrecy performance, this section develops accurate and straightforward asymptotic equations in the high optical SNR and mm-wave RF SNR, for the acquired secrecy metrics [14], [40]. As such, the FSO, mm-wave links, and main channel CDFs may all be approximated using

$$F_{\gamma_{Tk}}^{asy}(\gamma) \approx \frac{2\mathcal{A}_k}{a_k}\gamma^{\frac{a_k}{2}} \tag{13}$$

$$F_{\gamma_{Tj}}^{asy}(\gamma) \approx \frac{\mathcal{C}_j}{m_j L_j}\gamma^{m_j L_j} \tag{14}$$

Substituting (13) and (14) in (11), we get

$$F_{\gamma_{eq.R}}^{asy}(\gamma) \approx \frac{2\mathcal{A}_f \mathcal{C}_m}{a_f m_m L_m}\gamma^{\frac{a_f}{2}+m_m L_m} \tag{15}$$

The exact and asymptotic CDF expressions of the parallel system were verified via Monte-Carlo simulations as shown in Fig. 2.

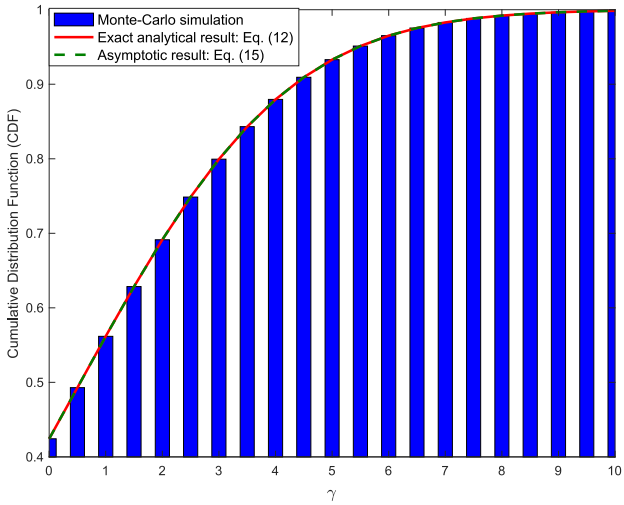

Fig. 2. CDF validation for the parallel FSO/mm-wave system.

III. Secrecy Performance Evaluation

In what follows, the secrecy capacity is defined as the highest rate of secure information transmission through a secure link between transmitter and receiver. On the other side, the eavesdropper is unable to intercept the link. As a result, the achievable secrecy capacity, C_s, can be defined mathematically as the difference of the main channel's capacity, $C_{eq.R}$, and the capacity of the wiretap channel, C_E [45] as

$$C_s = C_{eq.R} - C_E \tag{16}$$

where $E \in \{E_1, E_2\}$, $C_{eq.R} = \log_2(1+\gamma_{eq.R})$ and $C_E = log_2(1+\gamma_E)$ signify the legitimate and eavesdropper's link channel capacities, respectively, and γ_E signifies the SNR at E_1 (or E_2). In the next section, we perform an ASC analysis and obtain the SOP and SPSC expressions for the three eavesdropping scenarios.

A. Scenario 1: Eavesdropping Attack on FSO Link

In this scenario, the eavesdropper E_1 actively participates in information hacking through a legitimate FSO link. E_2 has no communication role in this scenario.

1) Average Secrecy Capacity (ASC) Evaluation: The average value of the secrecy capacity can be calculated using the formula [21]

$$ASC = \frac{1}{\ln(2)}\int_0^\infty \frac{F_{\gamma_E}(\gamma)}{1+\gamma}\left(1+F_{\gamma_{eq.R}}(\gamma)\right)d\gamma. \tag{17}$$

Following (17), the ASC for this case can be stated as

$$ASC_1 = \frac{1}{\ln(2)}\left(\mathcal{I}_1 + \mathcal{I}_2\right), \tag{18}$$

where

$$\mathcal{I}_1 = \int_0^\infty \frac{F_{\gamma_{TE_1}}(\gamma)}{1+\gamma}\, d\gamma,$$

and

$$\mathcal{I}_2 = \int_0^\infty \frac{F_{\gamma_{eq.R}}(\gamma) F_{\gamma_{TE_1}}(\gamma)}{1+\gamma}\, d\gamma.$$

On plugging (2) in $\mathcal{I}_1$ and (2) and (12) in $\mathcal{I}_2$ of (18), then by using (10) of [46], (9.31.5) of [42], and further involve [47, Eq. (07.34.21.0013.01)] to find $\mathcal{I}_1$ and using [47, Eq. (07.34.21.0081.01)] to find $\mathcal{I}_2$, the ASC for this scenario can be reduced to

$$ASC_1 = \frac{\mathcal{A}_{E_1}}{\ln(2)} \left[G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle| \begin{matrix} k_1 \\ k_2 \end{matrix}\right) + \mathcal{A}_f \mathcal{C}_m \, G_{1,1:3,3:2,2:3,3}^{1,1:2,2:1,2:2,2} \times \left[\begin{matrix} k_3 \\ k_3 \end{matrix} \middle| \begin{matrix} k_4 \\ k_5 \end{matrix} \middle| \begin{matrix} k_6 \\ k_7 \end{matrix} \middle| \begin{matrix} k_8 \\ k_9 \end{matrix} \middle| \frac{\mathcal{B}_f}{\bar{\gamma}_{Tf}}, \frac{\mathcal{D}_m}{\bar{\gamma}_{Tm}}, \frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}} \right] \right], \quad (19)$$

where $k_1 = 1 - b_{E_1},\ 1, -a_{E_1}/2,\ 1 + \xi_{E_1}^2$, $k_2 = a_{E_1}, \xi_{E_1}^2, -a_{E_1}/2,\ 0$, $k_3 = -(\frac{a_f}{2} + \frac{a_{E_1}}{2} + m_m L_m)$, $k_4 = 1 - b_f,\ 1, 1 + \xi_f^2$, $k_5 = a_f\ , \xi_f^2, 0$, $k_6 = 1 - (m_m + s_m), 1 - m_m L_m$, $k_7 = 0, -m_m L_m$, $k_8 = 1 - b_{E_1},\ 1,\ 1 + \xi_{E_1}^2$, $k_9 = a_{E_1}, \xi_{E_1}^2,\ 0$, and $G_{\cdot,\cdot}^{\cdot,\cdot}[.,.,.,|\begin{smallmatrix}\cdot\cdot\cdot\\ \cdot\cdot\cdot\end{smallmatrix}|\begin{smallmatrix}\cdot\cdot\cdot\\ \cdot\cdot\cdot\end{smallmatrix}|\begin{smallmatrix}\cdot\cdot\cdot\\ \cdot\cdot\cdot\end{smallmatrix}|\begin{smallmatrix}\cdot\cdot\cdot\\ \cdot\cdot\cdot\end{smallmatrix}]$ represents the integral of the multiplication of four Meijer G-functions with three different variables [48]. This integral is mathematically calculated using the Mathematica program.

For this case, the asymptotic ASC may be obtained by putting (2) and (15) into (17) and then utilizing [46, Eq. (10)], [42, Eq. (9.31.5)], as well as [47, Eq. (07.34.21.0013.01] to solve the resultant integrals, we have

$$ASC_1^{asy} \approx \frac{\mathcal{A}_{E_1}}{\ln(2)} G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle| \begin{matrix} k_1 \\ k_2 \end{matrix}\right) + \frac{4\mathcal{A}_f \mathcal{A}_{E_1} \mathcal{C}_m}{ln(2)\, a_f m_m L_m} G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle| \begin{matrix} k_{10} \\ k_{11} \end{matrix}\right), \quad (20)$$

where $k_{10} = 1 - b_{E_1},\ 1, -(\frac{a_f}{2} + \frac{a_{E_1}}{2} + m_m L_m),\ 1 + \xi_{E_1}^2$, and $k_{11} = a_{E_1}, \xi_{E_1}^2,\ -(\frac{a_f}{2} + \frac{a_{E_1}}{2} + m_m L_m),\ 0$.

2) Secure Outage Probability (SOP) Evaluation: A secrecy outage event occurs when the achievable secrecy capacity equals 0 or when C_s is less than the target secrecy rate, $\mathcal{R}_s$, i.e., $C_s < \mathcal{R}_s$ [4]. Returning to (16), the secrecy outage probability, SOP, is theoretically and mathematically can be expressed as

$$SOP = P_r\ [C_s(\gamma_{eq.R}, \gamma_E) \le \mathcal{R}_s] = \int_0^\infty f_{\gamma_{TE}}(\gamma_E)\, F_{eq.R}((1+\gamma_E)\ \emptyset - 1) d\gamma_E, \quad (21)$$

In (21), $\emptyset = exp(\mathcal{R}_s)$ [4]. Due to complexity in obtaining (21) into closed form, the lower bound of the SOP for $\gamma_E \gg 1$ is derived as follows [21]

$$SOP^L = \int_0^\infty f_{\gamma_{TE}}(\gamma_E)\, F_{eq.R}(\emptyset\gamma_E)\ d\gamma_E. \quad (22)$$

In this case, the lower bound of the SOP is found by inserting (1) and (12) into (22) and then using [47, Eq. (07.34.21.0081.01) as

$$SOP_1^L = \mathcal{A}_f \mathcal{C}_m \mathcal{C}_{E_1} \emptyset^{\frac{a_f}{2} + m_m L_m} \left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\right)^{-\Upsilon} \times G_{2,2:3,3:2,2}^{2,1:2,2:1,2} \left[\begin{matrix} k_{12} \\ k_{13} \end{matrix} \middle| \begin{matrix} k_4 \\ k_5 \end{matrix} \middle| \begin{matrix} k_6 \\ k_7 \end{matrix} \middle| \frac{\emptyset\mathcal{B}_f \bar{\gamma}_{TE_1}}{\mathcal{B}_{E_1}\bar{\gamma}_{Tf}}, \frac{\emptyset\mathcal{D}_m \bar{\gamma}_{TE_1}}{\mathcal{B}_{E_1}\bar{\gamma}_{Tm}} \right], \quad (23)$$

where $\Upsilon = (\frac{a_f}{2} + \frac{a_{E_1}}{2} + m_m L_m)$, $k_{12} = 1 - \Upsilon - k_2$, $1 - \Upsilon - \xi_{E_1}^2, 1 - \Upsilon$, and $k_{13} = 1 - \Upsilon + b_{E_1}, -\Upsilon, -\Upsilon - \xi_{E_1}^2$. $G_{\cdot,\cdot,\cdot,\cdot,\cdot,\cdot}^{\cdot,\cdot,\cdot,\cdot,\cdot,\cdot}[.]$ is the extended generalized bivariate Meijer G-function (EGBMGF) as defined by (8) of [49].

We can get the asymptotic lower bound of SOP at high SNR by substituting (1) and (15) into (22) and utilizing [47, Eq. (07.34.21.0003.01)] as

$$SOP_1^{L,asy} \approx \frac{2\mathcal{A}_f \mathcal{A}_{E_1} \mathcal{C}_m \emptyset^{\frac{a_f}{2} + m_m L_m}}{a_f m_m L_m} \times \gamma^\Upsilon G_{3,3}^{2,2}\left(\frac{\mathcal{B}_{E_1}\emptyset\gamma}{\bar{\gamma}_{TE_1}}\middle| \begin{matrix} 1-\mathcal{Y}, k_{14} \\ k_9, -\mathcal{Y} \end{matrix}\right), \quad (24)$$

where k_{14}= 1- $b_{E_1}, 1 + \xi_{E_1}^2$.

3) Strictly Positive Secrecy Capacity (SPSC) Evaluation: The strictly positive secrecy capacity (SPSC) is defined as the probability of attaining a positive secrecy rate (i.e., $C_s > 0$) and is represented as [4]

$$SPSC = P_r\ \{C_s(\gamma_{eq}, \gamma_E) > 0\} = P_r\ (\gamma_{eq.R} > \gamma_E). \quad (25)$$

In terms of SOP, (25) may be expressed as

$$SPSC = 1 - SOP_1^L(0),\ for\ \emptyset = 1. \quad (26)$$

For this scenario, the SPSC may be easily calculated substituting $\emptyset = 1$ into (23) as

$$SPSC_1 = 1 - \left[\mathcal{A}_f \mathcal{A}_{E_2} \mathcal{C}_m \left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\right)^{-\Upsilon} \times G_{2,2:3,3:2,2}^{2,1:2,2:1,2} \left[\begin{matrix} k_{12} \\ k_{13} \end{matrix} \middle| \begin{matrix} k_4 \\ k_5 \end{matrix} \middle| \begin{matrix} k_6 \\ k_7 \end{matrix} \middle| \frac{\mathcal{B}_f \bar{\gamma}_{E_1}}{\mathcal{B}_{E_1}\bar{\gamma}_{Tf}}, \frac{\mathcal{D}_m \bar{\gamma}_{TE_1}}{\mathcal{B}_{E_1}\bar{\gamma}_{Tm}} \right] \right] \quad (27)$$

The asymptotic SPSC may be produced similarly to (24) by inserting (24) into (26). As a result, the asymptotic SPSC simply can be expressed as

$$SPSC_1^{asy} \approx 1 - \left[\frac{2\mathcal{A}_f \mathcal{A}_{E_1} \mathcal{C}_m}{a_f m_m L_m} \gamma^\Upsilon G_{3,3}^{2,2}\left(\frac{\mathcal{B}_{E_1}\gamma}{\bar{\gamma}_{TE_1}}|_{k_9, -\Upsilon}^{1-\Upsilon, k_{14}}\right) \right] \quad (28)$$

B. Scenario 2: Eavesdropping Attack on Mm-Wave Link

The eavesdropper E_2 is actively engaging in information hacking through the legitimate mm-wave link in this scenario. The eavesdropper E_1, has no function to perform during communication in this case.

1) ASC: The ASC for this situation may be expressed as follows, using (17) as a guide

$$ASC_2 = \frac{1}{\ln(2)}\ (\mathcal{I}_3 + \mathcal{I}_4) \quad (29)$$

where $\mathcal{I}_3 = \int_0^\infty \frac{F_{\gamma_{TE_2}}(\gamma)}{1+\gamma}\, d\gamma$, and $\mathcal{I}_4 = \int_0^\infty \frac{F_{\gamma_{eq.R}}(\gamma) F_{\gamma_{TE2}}(\gamma)}{1+\gamma}$ $d\gamma$. Then, using the same approaches as $\mathcal{I}_1$ and $\mathcal{I}_2$,$\mathcal{I}_3$ and $\mathcal{I}_4$ can be found, yielding the solution of (29) as

$$ASC_2 = \frac{\mathcal{C}_{E_2}}{\ln(2)} \left[G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle| \begin{matrix} k_{15} \\ k_{16} \end{matrix}\right) + \mathcal{A}_f \mathcal{C}_m G_{1,1:3,3:2,2:1,2}^{1,1:2,2:1,2:1,2} \times \left[\begin{matrix} k_{17} \\ k_{17} \end{matrix} \middle| \begin{matrix} k_4 \\ k_5 \end{matrix} \middle| \begin{matrix} k_6 \\ k_7 \end{matrix} \middle| \begin{matrix} k_{18} \\ k_{19} \end{matrix} \middle| \frac{\mathcal{B}_f}{\bar{\gamma}_{Tf}}, \frac{\mathcal{D}_m}{\bar{\gamma}_{Tm}}, \frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}} \right] \right] \quad (30)$$

where $k_{15} = 1-(m_{E_2}+s_{E_2}), -m_{E_2}L_{E_2}, 1-m_{E_2}L_{E_2}$, $k_{16} = 0, -m_{E_2}L_{E_2}, -m_{E_2}L_{E_2}$, $k_{17} = -(\frac{a_f}{2}+m_mL_m+m_{E_2}L_{E_2})$, $k_{18} = 1-(m_{E_2}+s_{E_2}), 1-m_{E_2}L_{E_2}$, and $k_{19} = 0, -m_{E_2}L_{E_2}$.

The asymptotic ASC for this situation is found by inserting (10) and (15) into (17) and using the same processes to find ASC_1^{asy} as

$$ASC_2^{asy} \approx \frac{\mathcal{C}_{E_2}}{\ln(2)} G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle| \begin{matrix} k_{15} \\ k_{16} \end{matrix}\right) + \frac{4\mathcal{A}_f\mathcal{C}_m\mathcal{C}_{E_2}}{ln(2)\, a_f m_m L_m} G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle| \begin{matrix} k_{20} \\ k_{21} \end{matrix}\right), \quad (31)$$

where $k_{20} = 1-(m_{E_2}+s_{E_2}), -(\frac{a_f}{2}+m_{E_2}L_{E_2}+m_mL_m)$, $1-m_{E_2}L_{E_2}$, and $k_{21} = 0, -(\frac{a_f}{2}+m_{E_2}L_{E_2}+m_mL_m)$, $-m_{E_2}L_{E_2}$.

2) SOP: The lower bound of the SOP in this scenario is derived by putting (9) and (12) into (22) and applying [47, Eq. (07.34.21.0081.01)] as (32), shown at the bottom of the page, where $k_{22} = 0, (1-m_{E_2}L_{E_2})$.

The asymptotic of SOP at high SNR may therefore be obtained by plugging (9) and (15) into (22) and using [47, Eq. (07.34.21.0003.01)] as

$$SOP_2^{L,asy} \approx \frac{2\mathcal{A}_f\mathcal{C}_{E_2}\mathcal{C}_m\emptyset^{\frac{a_f}{2}+m_mL_m}}{a_f m_m L_m} \times \gamma^{k_{17}} G_{3,3}^{1,3}\left(\frac{\emptyset\mathcal{D}_m\gamma}{\bar{\gamma}_{Tm}}\middle| \begin{matrix} 1-k_{17}, k_{15} \\ k_{16}, -k_{17} \end{matrix}\right). \quad (33)$$

Remark 1: The SPSC and asymptotic SPSC for this scenario can be determined simply using the same procedure that was used to obtain (27) and (28).

C. Scenario 3: Eavesdropping Attack on Both FSO and Mm-Wave Links Simultaneously

In this scenario, it is assumed that both eavesdroppers E_1, and E_2 are active and attempting to intercept secure data across each authorized link of the communication.

1) *ASC:* The average secrecy capacity of a parallel FSO/mm-wave with SC receiver may be obtained as

$$ASC_3 = \frac{1}{\ln(2)} \left(\underbrace{\int_0^\infty \frac{\left(1+F_{\gamma_{Tf}}(\gamma)\right) F_{\gamma_{TE_1}}(\gamma)}{1+\gamma}\, d\gamma}_{\mathcal{I}_5}\right) \times \left(\underbrace{\int_0^\infty \frac{(1+F_{\gamma_{Tm}}(\gamma)) F_{\gamma_{TE_2}}(\gamma)}{1+\gamma}\, d\gamma}_{\mathcal{I}_6}\right) \quad (34)$$

Next, [47, Eq. (07.34.21.0011.01)] and [47, Eq. (07.34.21.0081.01)] can be combined to simplify $\mathcal{I}_5$ and $\mathcal{I}_6$ as

$$\mathcal{I}_5 = \mathcal{A}_{E_1} G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle| \begin{matrix} k_1 \\ k_2 \end{matrix}\right) + \mathcal{A}_f\mathcal{A}_{E_1} G_{1,1:3,3:3,3}^{1,1:2,2:2,2}\left[\begin{matrix} k_{23} \\ k_{23} \end{matrix}\middle| \begin{matrix} k_8 \\ k_9 \end{matrix}\middle| \begin{matrix} k_4 \\ k_5 \end{matrix}\middle| \frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}, \frac{\mathcal{B}_f}{\bar{\gamma}_{Tf}}\right] \quad (35)$$

$$\mathcal{I}_6 = \mathcal{C}_{E_2} G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle| \begin{matrix} k_{15} \\ k_{16} \end{matrix}\right) + \mathcal{C}_m\mathcal{C}_{E_2} G_{1,1:3,3:3,3}^{1,1:2,2:2,2}\left[\begin{matrix} k_{24} \\ k_{24} \end{matrix}\middle| \begin{matrix} k_{18} \\ k_{19} \end{matrix}\middle| \begin{matrix} k_6 \\ k_7 \end{matrix}\middle| \frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}, \frac{\mathcal{D}_m}{\bar{\gamma}_{Tm}}\right] \quad (36)$$

where $k_{23} = -(\frac{a_f}{2}+\frac{a_{E_1}}{2})$, $k_{24} = -(m_mL_m+m_{E_2}L_{E_2})$.

By inserting (2), (10), (13), and (14) in (34), the asymptotic ASC for this scenario can be derived, and the ASC_3^{asy} can be obtained as

$$ASC_3^{asy} \approx \frac{1}{\ln(2)} \left[\mathcal{A}_{E_1} G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle|_{k_2}^{k_1}\right) + \frac{2\mathcal{A}_f\mathcal{A}_{E_1}\mathcal{C}_m}{a_f m_m L_m} G_{4,4}^{3,3}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\middle|_{k_{26}}^{k_{25}}\right)\right] \times \left[\mathcal{C}_{E_2} G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle|_{k_{16}}^{k_{15}}\right) + \frac{2\mathcal{A}_f\mathcal{C}_m\mathcal{C}_{E_2}}{a_f m_m L_m} G_{3,3}^{2,3}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\middle|_{k_{28}}^{k_{27}}\right)\right] \quad (37)$$

where $k_{25} = 1-b_{E_1}, 1, -(\frac{a_f}{2}+\frac{a_{E_1}}{2}), 1+\xi_{E_1}^2, k_{26} = a_{E_1}, \xi_{E_1}^2, -(\frac{a_f}{2}+\frac{a_{E_1}}{2}), 0$, $k_{27} = 1-(m_{E_2}+s_{E_2}), -(m_{E_2}L_{E_2}+m_mL_m), 1-m_{E_2}L_{E_2}$, and $k_{28} = 0, -(m_{E_2}L_{E_2}+m_mL_m), -m_{E_2}L_{E_2}$.

2) *SOP*: Following (22), the SOP for a parallel system with an SC receiver can be written as

$$SOP_3^L = \left(\int_0^\infty f_{\gamma_{TE_1}}(\gamma_{E_1}) F_{\gamma_{Tf}}(\emptyset\gamma_{E_1})\, d\gamma_{E_1}\right) \times \left(\int_0^\infty f_{\gamma_{TE_2}}(\gamma_{E_2}) F_{\gamma_{Tf}}(\emptyset\gamma_{E_2})\, d\gamma_{E_2}\right). \quad (38)$$

The solution of (38) is derived by inserting (1), (2), (9), and (10) in (38) and using the integral identities from [47, Eq. (07.34.21.0011.01)] as

$$SOP_3^L = \left[\mathcal{A}_m\mathcal{A}_{E_1}\emptyset^{\frac{a_m}{2}}\left(\frac{\mathcal{B}_{E_1}}{\bar{\gamma}_{TE_1}}\right)^{-\Xi} G_{5,5}^{3,4}\left(\frac{\mathcal{B}_f\bar{\gamma}_{TE_1}}{\mathcal{B}_{E_1}\bar{\gamma}_{Tm}}\middle| \begin{matrix} k_{29} \\ k_{30} \end{matrix}\right)\right] \times \left[\mathcal{C}_m\mathcal{C}_{E_2}\emptyset^{m_mL_m-1}\left(\frac{\mathcal{D}_m}{\bar{\gamma}_{TE_2}}\right)^{-\nu} G_{4,4}^{3,3}\left(\frac{\mathcal{D}_m\bar{\gamma}_{TE_1}}{\mathcal{D}_{E_2}\bar{\gamma}_{TE_2}}\middle| \begin{matrix} k_{31} \\ k_{32} \end{matrix}\right)\right] \quad (39)$$

$$SOP_2^L = \mathcal{A}_f\mathcal{C}_m\mathcal{C}_{E_2}\emptyset^{\frac{a_f}{2}+m_mL_m}\left(\frac{\mathcal{D}_{E_2}}{\bar{\gamma}_{TE_2}}\right)^{k_{17}} G_{2,2:3,3:2,2}^{2,1:2,2:1,2}\left[\begin{matrix} 1-k_{17}-k_{22} \\ 1-k_{17}-k_{18} \end{matrix}\middle| \begin{matrix} k_4 \\ k_5 \end{matrix}\middle| \begin{matrix} k_6 \\ k_7 \end{matrix}\middle| \frac{\emptyset\mathcal{B}_f\bar{\gamma}_{TE_2}}{\mathcal{D}_{E_2}\bar{\gamma}_{Tf}}, \frac{\emptyset\mathcal{D}_m\bar{\gamma}_{TE_2}}{\mathcal{D}_{E_2}\bar{\gamma}_{Tm}}\right] \quad (32)$$

where $\Xi = (\frac{a_m}{2} + a_{E_1})$, $k_{29} = 1 - b_m, 1, 1 - \Xi + a_{E_1}, 1 - \Xi - \xi_{E_1}^2, 1 - \Xi, 1 + \xi_m^2$, $k_{30} = a_m, \xi_m^2, -\Xi + b_{E_1}, -\Xi, -\Xi - \xi_{E_1}^2, 0$. $\nu = m_m L_m + m_{E_2} L_{E_2}$, $k_{31} = 1 - (m_{E_2} + s_{E_2}), 1 - \nu, -\nu + m_{E_2} L_{E_2}, 1 + m_m L_m$, and $k_{32} = 0, -\nu + (m_{E_2} + s_{E_2}), -\nu + m_{E_2} L_{E_2}, m_m L_m$.

Now, we can obtain the asymptotic SOP at high SNR by substituting (1), (9), (13), and (14) into (38) and utilizing [47, Eq. (07.34.21.0002.01)] as

$$SOP_3^{L,asy} \approx \left[\frac{2\mathcal{A}_f \mathcal{A}_{E_2} \emptyset^{\frac{a_f}{2}} \gamma^{\chi_1}}{a_f} G_{3,3}^{2,2}\left(\frac{\mathcal{B}_{E_1}\gamma}{\bar{\gamma}_{Tm}} \middle| \begin{matrix} k_{33} \\ k_{34} \end{matrix}\right)\right] \times \left[\frac{\mathcal{C}_m \mathcal{C}_{E_2} \emptyset^{m_m L_m} \gamma^{\chi_2}}{m_m L_m} G_{3,3}^{1,3}\left(\frac{\mathcal{D}_{E_2}\gamma}{\bar{\gamma}_{TE_2}} \middle| \begin{matrix} k_{35} \\ k_{36} \end{matrix}\right)\right], \quad (40)$$

where $\chi_1 = \frac{a_f}{2} + \frac{a_{E_1}}{2}$, $\chi_2 = m_m L_m + m_{E_2} L_{E_2}$, $k_{33} = 1 - \chi_1, 1 - b_{E_1}, 1 + \xi_{E_1}^2$, $k_{34} = a_{E_1}, \xi_{E_1}^2, 0, -\chi_1$, $k_{35} = 1 - \chi_2, 1 - (m_{E_2} + s_{E_2}), 1 - m_{E_2} L_{E_2}$, and $k_{36} = 0, 1 - m_{E_2} L_{E_2}, -\chi_2$

The final expressions of ASC_1, ASC_2, ASC_3, SOP_1^L, SOP_2^L, SOP_3^L, and their correspondence asymptotic expressions of the investigated parallel system are new and never found before, to the best of the author's knowledge based on the open literature, and thus our derived expressions are novel.

IV. Numerical Results

Selected simulation results under unified $\mathcal{F}$-distribution with considered eavesdropping situations are provided and analyzed in this section, using the aforementioned obtained analytical expressions. In the theoretical analysis, a MATLAB code provided in [50] was used to evaluate the EGBMGF in Section III. We investigate the effects of FSO turbulence parameters and pointing errors, fading, and shadowing parameters, number of diversity branches for mm-wave links, and SNR values received by eavesdropping links on secrecy performance. For all the eavesdropping scenarios and for the sake of simplicity, it is assumed that $a_f = a_{E_1} = a$, $b_f = b_{E_1} = b$, $\varepsilon_f = \varepsilon_{E_1} = \varepsilon$, $m_m = m_{E_2} = m_j$ and $s_m = s_{E_2} = s_j$ unless it is stated otherwise. Moreover, the average SNRs for both the legitimate links are assumed to be equal ($\bar{\gamma}_{Tf} = \bar{\gamma}_{Tm} = 10$ dB). The parameters a and b are set using the values obtained in [13]: for weak turbulence: $a = 4.5916$, $b = 7.0941$; for moderate turbulence: $a = 2.337$, $b = 4.5323$; and for strong turbulence: $a = 1.4321$, $b = 3.4948$. Unless otherwise stated, the values of the FSO and mm-wave links parameters utilized in our work for all eavesdropping scenarios are set according to [13], [51], [52] and provided in Table I. All of the graphs were generated in MATLAB using both analytical equations and Monte-Carlo (M-C) simulation with, 10^8 channel realizations.

A. Scenario 1: Eavesdropping on FSO Link Only

To assess the impacts of optical link's turbulence and pointing errors on ASC, Fig. 3 plots the ASC as a function of the average SNR of the main channel with moderate fading and low shadowing parameters (i.e., $m_j = 3$, $s_j = 50$) for the mm-wave links. Increasing the average SNR of the main channel enhanced secrecy performance, as indicated in the figure. When atmospheric turbulence severity rises from weak to strong, the system's overall ASC performance diminishes, proving the accuracy of (19) stated in Section III. This means that stronger turbulence has a larger effect on the legitimate receiver's SNR, leading to a poorer FSO link than weaker turbulence. Furthermore, the results show the impact of both significant and negligible pointing errors. More secure communication is established between the transmitter and the receiver due to enhanced pointing precision with negligible pointing errors ($\xi = 6.7$). The improvement in secrecy is obtained because the SNR received at R with weak turbulence and negligible pointing errors is greater than the SNR received with severe turbulence and substantial pointing errors and higher than the SNR of the eavesdropper's link.

The influence of the average SNR of the first eavesdropper's link $T \to E_1$, γ_{E_1} on the ASC performance of the investigated system is depicted in Fig. 4. Increasing the value of γ_{E_1} led to a decline in ASC performance under moderate atmospheric turbulence and negligible pointing errors circumstances, as seen in this figure. This is because the channel quality of a legitimate link

TABLE I
The Values of System Parameters

Parameters	Values
Links length	3.5 km
Wavelength	1550 nm
D	10 mm
l_0	0.8 m
L_0	5.98 mm
$\mathbb{A}_0$	0.8
σ_1^2	0.6343, 1.0058, 4.0230 (for weak, moderate, and strong turbulence.
Secrecy rate	0.1 bit/s/Hz
Transmit power	10 mW
η	1
N_o	1
Carrier frequency	60 GHz
Transmit antenna gain	44 dBi
Transmit antenna gain	44 dBi

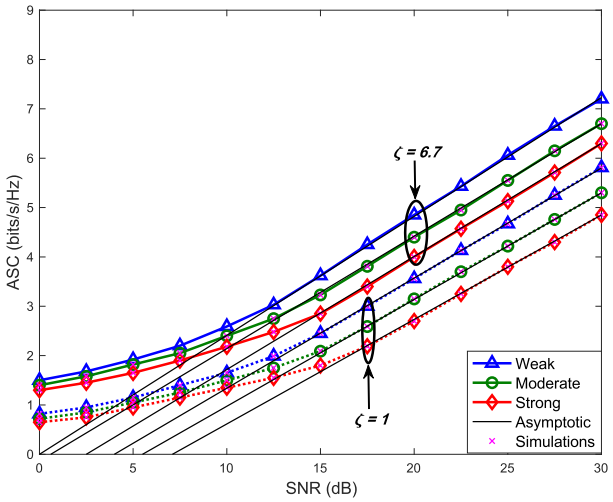

Fig. 3. ASC under different turbulence and pointing errors effects; where $\gamma_{E_1} = 5\ dB$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

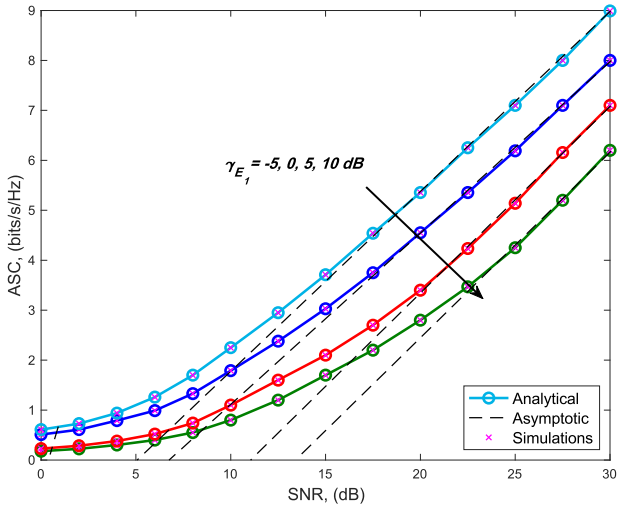

Fig. 4. ASC under the effects of selected values of γ_{E_1}; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

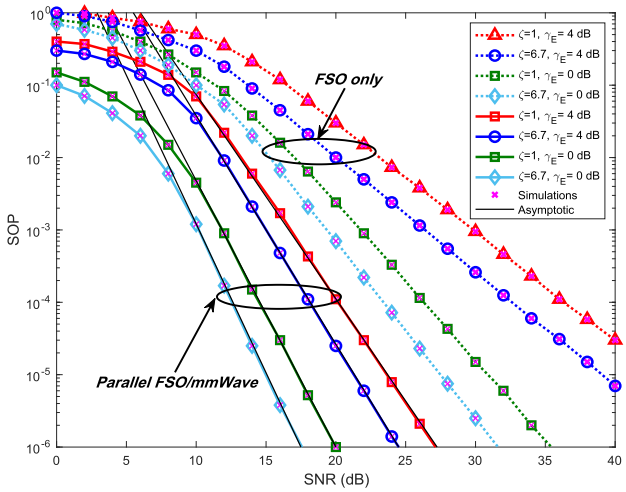

Fig. 6. SOP under selected values of γ_{E_1} and ε; where $a = 2.337$, $b = 4.5323$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

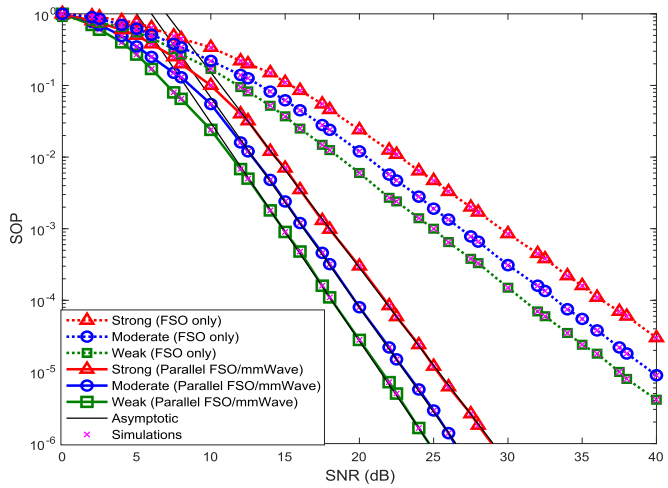

Fig. 5. SOP under different turbulence conditions; where $\varepsilon = 6.7$, $\gamma_{E_1} = 5\,dB$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

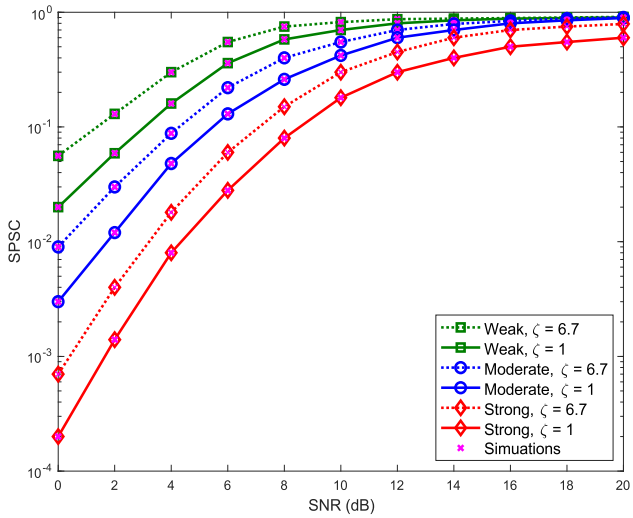

Fig. 7. SPSC under different turbulence and selected values of ε; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_{E_1} = 5\,dB$, $s_j = 20$, $m_j = 3$, and $L_j = 2$.

degrades faster than that eavesdropper link, which is connected to the eavesdropper link's high SNR with higher γ_{E_1}. In contrast, as γ_{E_1} grows, the eavesdropper E_1 becomes more effective, and the security of the system deteriorates. Furthermore, as can be observed in all of the preceding figures, the asymptotic curves in Fig. 3 and Fig. 4 closely match the exact ones, confirming the correctness of (20) that was derived in Section III in high SNR values (i.e., $\geq$15).

The effects of atmospheric turbulence on SOP are displayed in Fig. 5 under moderate atmospheric turbulence and negligible pointing errors conditions for FSO links with moderate fading and low shadowing parameters for the mm-wave links. The results in Fig. 5 show that the investigated parallel system has better secrecy than the FSO-only system. This is due to the parallel system's superior SOP performance when compared to the FSO only link-based system. Furthermore, it can be seen that the SOP for both systems is substantially poorer under strong turbulence for the same reason as in Fig. 3.

Fig. 6 shows the combined impact of receiver misalignment and the average SNR of the untheorized $T \rightarrow E_1$ link on SOP. Even when the optical communication link experiences substantial pointing errors and high SNR of eavesdropping link circumstances, the investigated parallel system has a considerably better SOP than the FSO only system. The parallel system is more resilient to the negative effects of FSO turbulence and pointing errors since the radio communication link is included.

In Fig. 7, the SPSC performance is demonstrated concerning SNR under different turbulence conditions and varying pointing error conditions for the FSO links with moderate fading and low shadowing parameters for the mm-wave links. It is possible to deduce that a greater value of ε and weak turbulence ensures secure transmission with a higher probability. Because

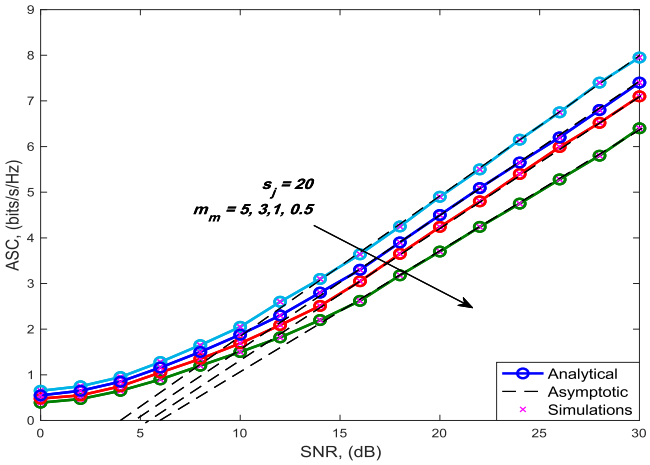

Fig. 8. ASC for selected values of m_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5\,dB$, $m_{E_2} = 3$, and $L_j = 2$.

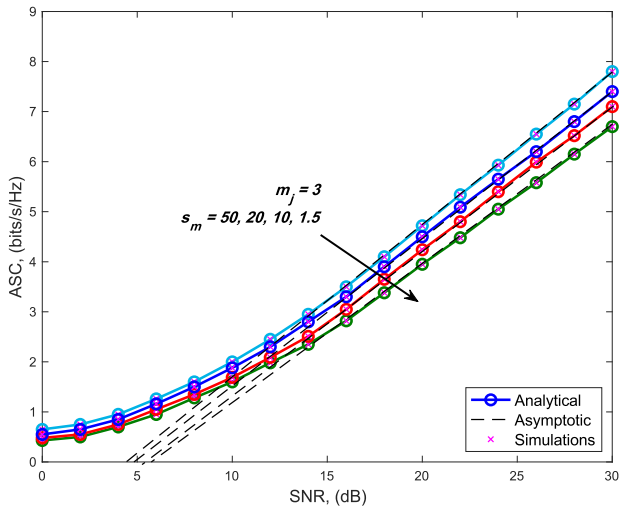

Fig. 9. ASC for selected values of s_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5\,dB$, $s_{E_2} = 20$, and $L_j = 2$.

the received SNR at R is dependent on and turbulence severity conditions as described in (27), the SPSC performance degrades as these parameters become more severe. However, it has been observed that when SNR rises, the associated SPSC performance improves noticeably.

B. Scenario 2: Eavesdropping on Mm-Wave Link Only

The impact of various fading conditions of the legitimate mm-wave, $T \to m$ link of the main channel on the ASC performance is illustrated in Fig. 8 for $m_m = 5$, 3,1, 0.5, $s_m = s_{E_2} = 20$, and $m_{E_2} = 3$ for mm-wave links with moderate turbulence and negligible pointing errors for FSO links. For this scenario, we set $\gamma_{E_2} = 5$ dB. It is obvious that the ASC improves as the severity of the fading conditions decreases, i.e., as the value of the main channel's fading parameter, m_m, increases. This is because as, m_m increases, so do the number of multipath clusters arrive at R, and therefore the received SNR. A larger value of m_m can be obtained to assure secure transmission with a higher probability.

In the same context, Fig. 9 depicts the influence that the shadowing parameter of the legitimate mm-wave link, $T \to m$, might have on the ASC for $m_m = m_{E_2} = 3$. The ASC performance increases significantly when, s_m is dropped from 1.5 (high shadowing) to 50 (light shadowing). This is because the legitimate mm-wave link obtains increasingly good reception as the level of shadowing decreases. To put it another way, more shadowing of the received signal strength is beneficial to improving system secrecy. This is because the physical layer security makes use of the unpredictability of wireless channels, i.e., fading, to increase secrecy.

The ASC versus the average SNR for selected values of L_m under moderate fading and light shadowing settings for mm-wave links is plotted in Fig. 10 to highlight the effect of the number of diversity branches L_m of the legitimate mm-wave link on the secrecy performance. The positive impact of MRC diversity on the parallel system's secrecy performance can be observed in this figure, where the ASC improves as L_m increases while m_j and s_j remain constant ($m_j = 3$, $s_j = 50$). The

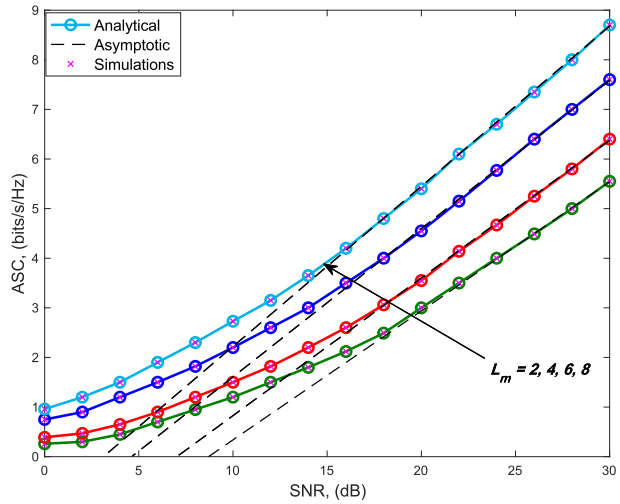

Fig. 10. ASC for selected values of L_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5\,dB$, $m_j = 3$, $s_j = 50$.

Monte-Carlo simulation results successfully support our analytical results, which are given by (30), in Section III. Furthermore, the following conclusion might be reached: (i) lower m_m results in a lower ASC; (ii) ASC can be improved by ensuring high s_m; (iii) The ASC performance curves converge very rapidly to one other under all channel conditions for low SNR values, i.e., $>$ 5 dB, as illustrated in Figs. 8-10; (iv) our asymptotic ASC_1^{asy} given by (20) begin to progressively approach the exact one only when SNR is larger than 15 dB for our given simulation configuration.

Fig. 11 depicts the SOP versus the average SNR of the investigated system for various values of the legitimate mm-wave link's fading severity parameter, m_m, and light shadowing. The system's SOP performance has greatly deteriorated when the main channel experiences significant fading (i.e., lower values of the fading severity parameter, m_m). However, the results in

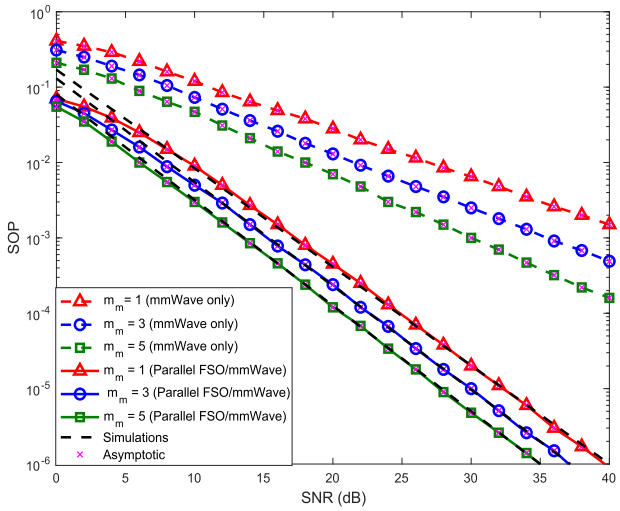

Fig. 11. SOP for selected values of m_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7, \gamma_{E_2} = 5\,dB$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

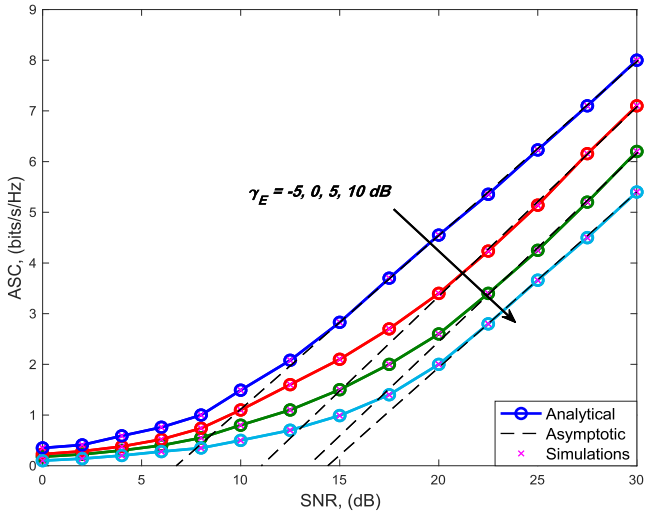

Fig. 13. ASC under the effects of selected values of γ_E; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

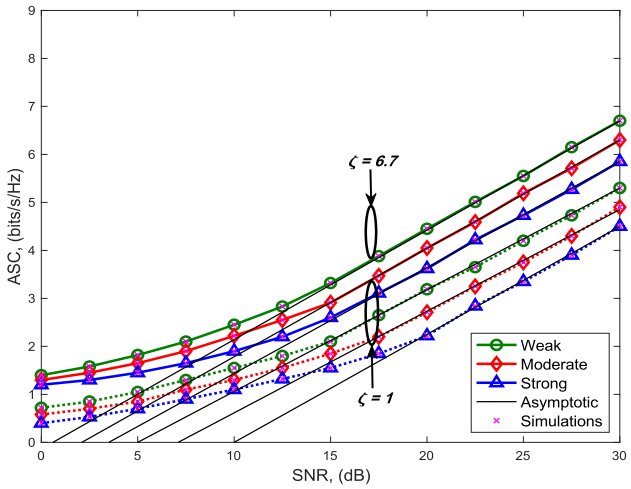

Fig. 12. ASC under different turbulence and pointing errors effects; where $\gamma_E = 5\,dB$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

Fig. 11 again demonstrate the improved secrecy of the investigated parallel system compared to the mm-wave only link system. Furthermore, the asymptotic curves ($SOP^{L.asy}$) match tightly the exact ones, 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.

C. Scenario 3: Simultaneous Eavesdropping on Both FSO and Mm-Wave Links

Fig. 12 displays the ASC_3 closed-form expression that was previously derived in Section III for varied pointing errors and atmospheric conditions when both eavesdroppers E_1 and E_2 are active. To show the influence of both eavesdroppers, we set γ_{E_1}=γ_{E_2} = 5 dB in this example. As predicted, the low pointing errors (i.e., $\varepsilon = 6.7$) effect produces a greater ASC than the higher effect of ε, (i.e., $\varepsilon = 1$). This is because smaller values of ε represent high pointing errors, which cause significant distortions in received optical signals. As a result of these distortions, the legitimate receiver's signal is weakened, and the capacity of the main channel is lowered. In addition, the ASC is greater in the presence of weak turbulence than in the presence of strong turbulence. The reason for the previous findings is the same as it was in Fig. 3. In this case, where both legal links are simultaneously overheard by the eavesdroppers, the ASC curves in Fig. 12 are smaller than their corresponding curves in Fig. 3.

Fig. 13 displays the ASC performance as a function of the main channel's SNR under the impact of different values of the average SNR of the wiretap channels, γ_E. In this scenario, we assume that the average SNRs for both eavesdropper links are equal (i.e., $\gamma_{E_1} = \gamma_{E_2} = \gamma_E$). The increased value of, γ_E obtained by $E_1$and E_2 resulted in a considerable drop in ASC performance, as seen in this figure. This is since as γ_E rises, the channel capacity of the eavesdropper's links improves, leading to a decline in the ASC of the main channel. As a result, the greater γ_E, the higher the quality of the eavesdropper's channels, and therefore the ASC performance would decline as projected. When comparing the results in Fig. 4 to this case, it can be seen that ASC decreases. This is because the FSO link is less susceptible to eavesdropping than the mm-wave link.

Figs. 14 and 15 show the ASC as a function of the main channel's average SNR under the impact of different values of fading severity and shadowing parameter of the main channel. The curves were plotted by assuming two eavesdroppers simultaneously attacking both legitimate links. All of these figures illustrate that a lower severity of fading and/or shadowing (i.e., higher values of m_m and/or s_m), generates a better result than a higher severity of fading and/or shadowing. It is concluded that greater values of m_j and s_j contribute to better performance in terms of fading and shadowing severity (i.e., higher ASC). The reason for this is that, over the legitimate mm-waver link, the SNR values received by the R increased as the intensity of fading and shadowing reduced, while all other channel characteristics

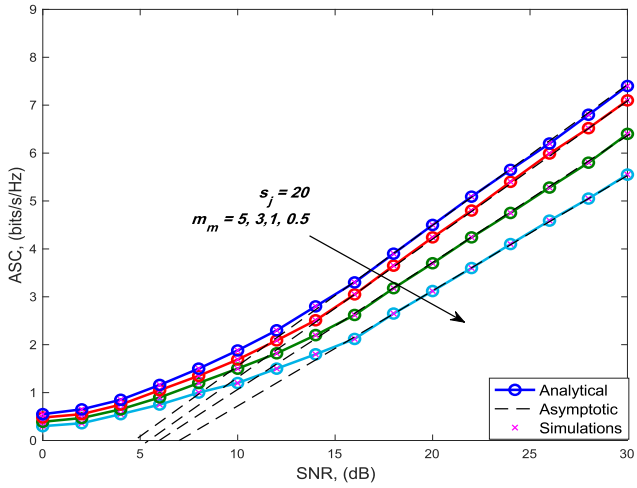

Fig. 14. ASC for selected values of m_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5\,dB$, $m_{E_2} = 3$, and $L_j = 2$.

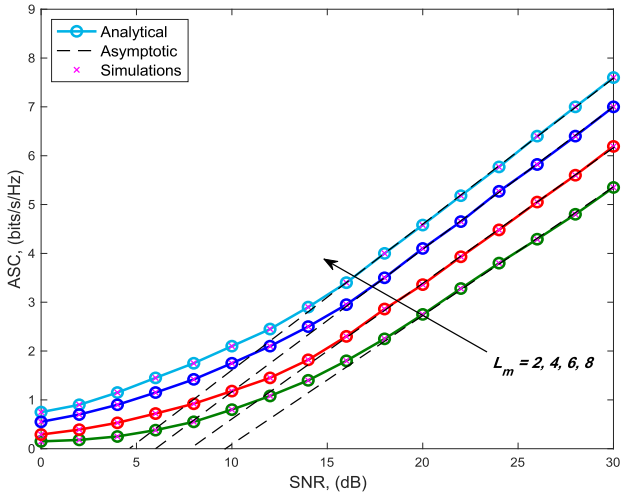

Fig. 16. ASC for selected values of L_m; where $L_{E_2} = 2$, $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5dB$, and $m_j = 3$, $s_j = 50$..

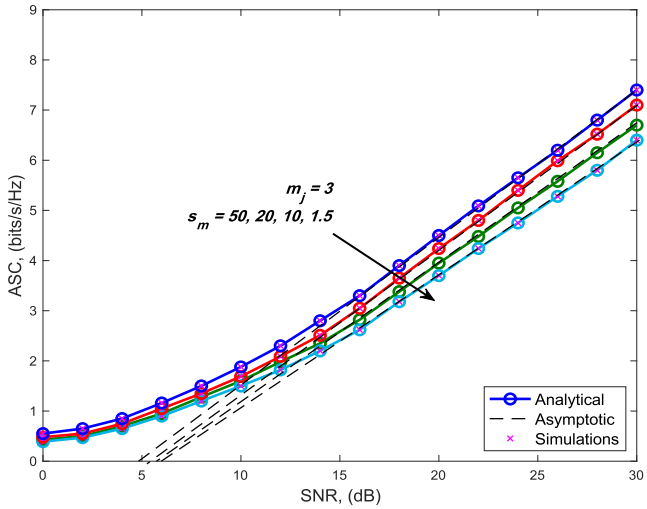

Fig. 15. ASC for selected values of s_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7$, $\gamma_E = 5\,dB$, $s_{E_2} = 50$, and $L_j = 2$.

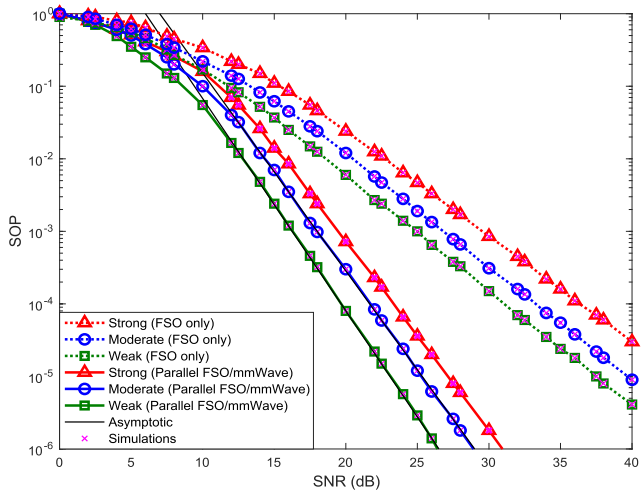

Fig. 17. SOP under different turbulence conditions; where $\varepsilon = 6.7$, $\gamma_{E_1} = 5\,dB$, $m_j = 3$, $s_j = 50$, and $L_j = 2$.

stayed constant, supporting the accuracy of ASC_3, previously obtained in Section III.

Fig. 16 depicts the ASC as a function of the average SNR of the main channel, as well as the effect of the legitimate mm-wave link's MRC diversity on the secrecy performance for scenario 3. For mm-wave links, moderate fading and low shadowing parameters were assumed, and moderate turbulence with negligible pointing errors was assumed for FSO links, while L_{E_2}= 2. As predicted, Fig. 16 indicates that as L_m increases so do the ASC. This is exemplified by the fact that raising the L_m resulted in an increase in MRC diversity gain at R. It is observed that ASC decreases when compared to the results of Fig. 10 in this case where the mm-wave link is more sensitive to eavesdropping than the FSO link.

Fig. 17 represents the SOP derived in (39) for different pointing errors and atmospheric conditions when both eavesdroppers $E1$ and $E2$ are active. As expected, the SOP with lower ε and stronger turbulence is greater than with the larger value of ε and weaker turbulence. The explanation is the same as it was for the prior findings in Fig. 5. Furthermore, when the SNR of the main channel increases, the parallel system outperforms the FSO-only system in terms of SOP performance.

The effect of fading effects encountered on the main link, m_m can have on the SOP is shown in Fig. 18 for $\gamma_E = 5\,dB$, and $s_j = 50$. The SOP improves as the intensity of the fading conditions decreases, i.e., as the fading parameter of the main link m_m increases. This is owing to the fact that as m_m grows, so does the number of multipath clusters arrive at R , and therefore the received SNR. It is possible to notice that the SOP is higher in this situation when compared to the results of Fig. 11. According to Figs. 11 and 18, fading has a negative influence on SOP performance, and it has a higher impact on SOP performance under low values of the SNR. However, due to the complementary features of FSO and mm-wave links, it can be shown from these findings that the fading parameter

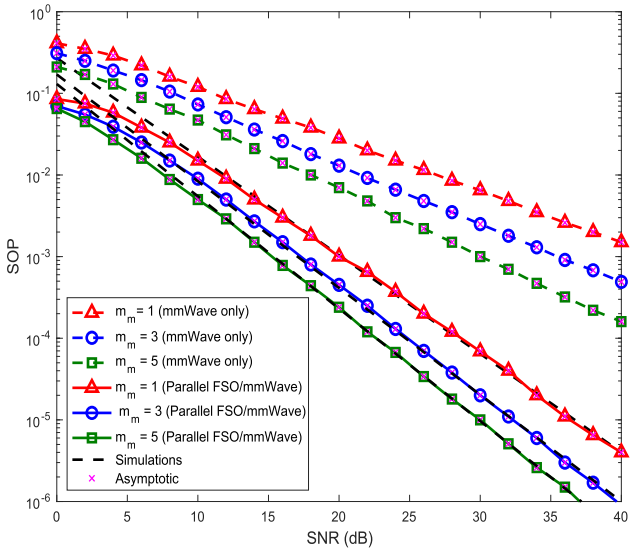

Fig. 18. SOP for selected values of m_m; where $a = 2.337$, $b = 4.5323$, $\varepsilon = 6.7, \gamma_E = 5\,dB$, $s_j = 20$, $m_{E_2} = 3$, and $L_j = 2$.

has less performance fluctuation on the SOP for the parallel FSO/mm-wave system compared to the mm-wave only system.

Three notable remarks should be made here. To begin, in scenario 3, when both E_1 and E_2 are active and attempting to hack information from both legitimate links at the same time, the secrecy performance of the investigated parallel system slightly degrades compared to the results of scenarios 1 and 2 when either E_1 or E_2 is active, thanks to inheriting complementary properties of the FSO and mm-wave links. Second, in all of the figures in this section, the analytical results nearly match the simulated ones, demonstrating that the model and analysis are valid. Finally, for all of the results shown in the preceding figures, the asymptotic results closely match the closed-form results.

V. Conclusion

In this paper, the secrecy performance of a parallel FSO/mm-wave system is analyzed using a unified $\mathcal{F}$-distribution. These analyses are provided for three different scenarios based on the number of eavesdroppers are activated during data transmission. For each of these scenarios, closed-form equations for ASC, SOP, and SPSC are produced and compared. Furthermore, it is concluded that the system is insecure due to increased turbulence and pointing errors strength of FSO links. In addition to this, when the SNR received by eavesdropper links grew, the system's secrecy performance decreased. The parameters m_m and s_m also influences the secrecy performance, the higher the values of m_m and s_m, the better the results for the investigated parallel system. Besides, a greater number of MRC branches for the legitimate mm-wave link can be employed to increase the parallel system's security performance. Also, the secrecy performance of the three eavesdropping scenarios is evaluated, and scenario 3 is shown to be somewhat poorer than the other two. Finally, it can be stated that the parallel FSO/mm-wave system outperforms the FSO- and mm-wave-only systems in terms of SOP performance.

References

[1] M. Alzenad, M. Z. Shakir, H. Yanikomeroglu, and M.-S. Alouini, "FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 218–224, Jan. 2018.

[2] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 57–96, Jan.–Mar. 2017.

[3] 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.

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

[5] Y. Ai, A. Mathur, M. Cheffena, M. Bhatnagar, and H. Lei, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photon. J.*, vol. 11, no. 1, Feb. 2019, Art. no. 7900814.

[6] W. M. R. Shakir, "Performance evaluation of a selection combining scheme for the hybrid FSO/RF system," *IEEE Photon. J.*, vol. 10, no. 1, Feb. 2018, Art. no. 7901110.

[7] N. Letzepis, K.D. Nguyen, A.G. i Fàbregas, and W.G. Cowley, "Outage analysis of the hybrid free-space optical and radio-frequency channel," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1709–1719, Dec. 2009.

[8] M. Usman, H.-C. Yang, and M.-S. Alouini, "Practical switching-based hybrid FSO/RF transmission and its performance analysis," *IEEE Photon. J.*, vol. 65, no. 5, Oct. 2014, Art. no. 7902713.

[9] T. Rakia, H.-C. Yang, M.-S. Alouini, and F. Gebali, "Outage analysis of practical FSO/RF hybrid system with adaptive combining," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1366–1369, Aug. 2015.

[10] V. Jamali, D.S. Michalopoulos, M. Uysal, and R. Schober, "Mixed RF and hybrid RF/FSO relaying," in *Proc. IEEE Glob. Commun. Conf. Workshop*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[11] A. Touati, A. Abdaoui, F. Touati, M. Uysal, and A. Bouallegue, "On the effects of combined atmospheric fading and misalignment on the hybrid FSO/RF transmission," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 8, no. 19, pp. 717–725, Oct. 2016.

[12] K. Peppas, G. Alexandropoulos, E. D. Xenos, and A. Maras, "The Fischer–Snedecor F-distribution model for turbulence-induced fading in free-space optical systems," *J. Lightw. Technol.*, vol. 38, no. 6, pp. 1286–1295, Mar. 2020.

[13] O. S. Badarneh, R. Derbas, F. S. Almehmadi, F. E. Bouanani, and S. Muhaidat, "Performance analysis of FSO communications over F turbulence channels with pointing errors," *IEEE Comm Lett.*, vol. 25, no. 3, pp. 926–930, Mar. 2021.

[14] S. K. Yoo, S. Cotton, P. Sofotasios, M. Matthaiou, M. Valkama, and G. Karagiannidis, "The Fisher–Snedecor F-distribution: A simple and accurate composite fading model," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1661–1664, Jul. 2017.

[15] L. Kong and G. Kaddoum, "On physical layer security over the fisher snedecor F wiretap fading channels," *IEEE Access*, vol. 6, pp. 39466–39472, 2018.

[16] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, Apr. 2015, Art. no. 7901014.

[17] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7901110.

[18] 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.

[19] 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.

[20] 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.

[21] H. Lei, Z. Dai, I. S. Ansari, K. H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photon. J.*, vol. 9, no. 4, Aug. 2017, Art. no. 7904814.

[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. Lightw. Technol.,* vol. 35, no. 9, pp. 1490–1505, May 2017.

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

[24] 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.

[25] 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.

[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 *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.

[28] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "Secrecy analysis for multi-relaying RF-FSO systems with a multi-aperture destination," *IEEE Photon. J.*, vol. 12, no. 2, Apr. 2020, Art. no. 7902011.

[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. J.*, vol. 477, 2020, Art. no. 126334.

[31] Z. Wang, W. Shi, W. Liu, Y. Zhao, and K. Kang, "Performance analysis of full duplex relay assisted mixed RF/FSO system," *Opt. Commun. J.*, vol. 474, 2020, Art. no. 126170.

[32] S. H. Islam *et al.*, "On secrecy performance of mixed generalized gamma and málaga RF-FSO variable gain relaying channel," *IEEE Access*, vol. 8, pp. 104127–104138, 2020.

[33] N. A. Sarker *et al.*, "Secrecy performance analysis of mixed hyper-Gamma and gamma-gamma cooperative relaying system," *IEEE Access*, vol. 8, pp. 131273–131285, 2020.

[34] 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, Aug. 2021, Art. no. 7300517.

[35] 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, 2019.

[36] 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. J.*, vol. 475, 2020, Art. no. 126193.

[37] H. Liang, Y. Li, M. Miao, C. Gao, and X. Li, "Analysis of selection combining hybrid FSO/RF systems considering physical layer security and interference," *Opt. Commun.*, vol. 497, 2021, Art. no. 127146.

[38] H. Shankar and A. Kansal, "Performance analysis of MRC receiver over fisher snedecor (F) composite fading channels," *Wireless Pers. Commun.*, vol. 117, pp. 1337–1359, 2021.

[39] Y. Ai, A. Mathur, G. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, 2020, Art. no. 7906617.

[40] O. S. Badarneh and R. Mesleh, "Diversity analysis of simultaneous mm-Wave and free-space-optical transmission over F-distribution channel models," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 12, no. 11, pp. 324–334, Nov. 2020.

[41] L. Han, W. Yawei, L. Xuemei, and L. Boyu, "Secrecy performance of FSO using HD and IM/DD detection technique over F-distribution turbulence channel with pointing error," *IEEE Wireless Commun. Lett.*, vol. 10, no. 10, pp. 2245–2248, Oct. 2021.

[42] I.S. Gradshteyn and I.M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Burlington, MA, USA: Academic, 2007.

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

[44] R. Singh and M. Rawat, "Physical layer security of MRC in fisher–snedecor f fading channels," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst.*, Goa, India, Dec. 2019, pp. 1–5.

[45] 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.

[46] 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. Computation*, Tokyo, Japan, Jul. 1990, pp. 212–224.

[47] The Wolfram Functions Site, Accessed: Oct. 1, 2021. [Online]. Available: http://functions.wolfram.com/

[48] Y. F. Al-Eryani, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Two-way multiuser mixed RF/FSO relaying: Performance analysis and power allocation," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 396–408, Apr. 2018.

[49] S. C. Gupta, "Integrals involving products of G-function," in *Proc. Nat. Acad. Sci.*, India, 1969, vol. 39(A), no. 2, pp. 193–200.

[50] H. Chergui, M. Benjillali, and S. Saoudi, "Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and Rayleigh dual-hop channel," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 610–613, Mar. 2016.

[51] W. M. R. Shakir, "Performance analysis of the hybrid MMW RF/FSO transmission system," *Wireless Pers. Commun.*, vol. 109, pp. 2199–2211, 2019.

[52] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. M. Rabie, and N. Aldhahir, "Achievable physical-layer security over composite fading channels," *IEEE Access*, vol. 8, pp. 195772–195787, 2020.