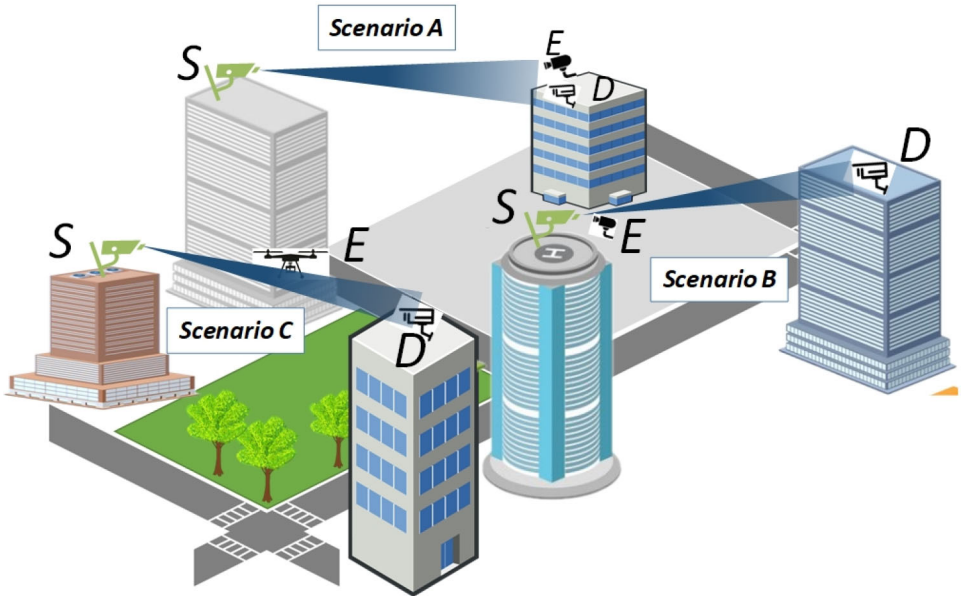
IEEE Photonics Journal
An IEEE Photonics Society Publication

Comprehensive Physical Layer Security Analysis of FSO Communications Over Málaga Channels

Volume 12, Number 6, December 2020

Yun Ai
Aashish Mathur
Gyan Deep Verma
Long Kong
Michael Cheffena



DOI: 10.1109/JPHOT.2020.3036244

Comprehensive Physical Layer Security Analysis of FSO Communications Over Málaga Channels

Yun Ai,[1] **Aashish Mathur**,[2] **Gyan Deep Verma**,[2] **Long Kong**,[3] **and Michael Cheffena**[1]

[1]Faculty of Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2]Department of Electrical Engineering, Indian Institute of Technology Jodhpur, Jodhpur 342037, India
[3]Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, L-1855 Luxembourg, Luxembourg

DOI:10.1109/JPHOT.2020.3036244

Manuscript received August 12, 2020; revised October 18, 2020; accepted November 3, 2020. Date of publication November 6, 2020; date of current version December 4, 2020. Corresponding author: Yun Ai (e-mail: yun.ai@ntnu.no).

Abstract: In this article, we study the physical layer security of free-space optical (FSO) communications under different eavesdropping scenarios. More specifically, the secrecy performance of FSO communication employing intensity modulation/direct detection detection is analyzed for the well-established Málaga channels. Three different realistic scenarios of eavesdropping are considered by assuming different placement locations for the eavesdropper in the paper. Novel expressions for the average secrecy capacity (ASC) and secrecy outage probability (SOP) are derived for the considered scenarios, and useful insights are also provided through asymptotic analysis. The results show: (1) When the eavesdropper is placed near the transmitter, atmospheric condition imposes a less significant impact on secrecy performance; (2) Certain level of correlation can potentially enhance the secrecy performance for FSO communications; (3) The correlation imposes opposite impacts on the ASC and SOP of FSO communications; and the secrecy performance metrics exhibit a non-monotonic impact with the increase of correlation; (5) When the correlation of the FSO links is too small or too large (i.e., the correlation parameter around 0 or 1), the correlation plays a more significant impact on secrecy performance; and (6) The asymptotic slope of the SOP is 0.5 for all eavesdropping scenarios under practical FSO channels.

Index Terms: Average secrecy capacity, free-space optical (FSO) communications, Málaga ($\mathcal{M}$)-distribution, physical layer security, secrecy outage probability.

1. Introduction

Physical layer security (PLS) has recently been considered as a complementary technique to the conventional encryption schemes to improve the communication secrecy [1]–[3]. It is demonstrated that communication nodes can exploit the variations in the communication channels to increase the communication security against eavesdropping [3]. This observation has attracted an increasing amount of interest in the research community to investigate the physical layer secrecy performance of communication systems under different setups [4]–[10].

The secrecy outage probability (SOP) and the Probability of the Non-zero Secrecy Capacity (PNZSC) performances were studied for the correlated composite Nakagami-*m*/Gamma fading channels in [4], where the small-scale Nakagami fading is assumed to be independent and shadowing is correlated. The impact of spatial correlation on the average secrecy capacity (ASC) was investigated in [5] by assuming that the transmitter has full knowledge on the channel state information (CSI) of both the legitimate receiver and eavesdropper. The effect of correlation on the PLS performance over the widely used α-μ fading channels was investigated in [6]. In [7], the ASC performance over double-Rayleigh fading channel under the vehicular communication scenario was studied. To facilitate the PLS analysis of mmWave propagation channels in the incoming 5 G, the secrecy performance over the newly proposed α-η-κ-μ fading channel was studied in [8]. The ASC and SOP performance over correlated log-normal fading channels were investigated in [9].

Compared to the radio-frequency (RF) transmission, free-space optical (FSO) communications is considered to be inherently more secure [11]–[15]. Owing to the good directivity of optical beams, it becomes a much harder, yet not impossible task for the eavesdropper to intercept the FSO signals (considering a very narrow beam with the small divergence angle 0.001 radian, the divergence region of the laser beam will be 1 m for the 1 km distance between the two legitimate peers). However despite the nonignorable possibility of being eavesdropped for FSO communications, the research investigating the PLS of optical communications is quite limited for both visible light [16] and FSO communications [11]–[14]. In [11], the PNZSC performance was studied for the FSO communications by ignoring the large-scale induced turbulence and assuming Gamma random variables (RVs) for the small-scale fluctuation. The secrecy performance of a line-of-sight (LoS) FSO link using orbital angular momentum (OAM) multiplexing was investigated in [12]. The performance of secure FSO communication was studied in [13] by assuming both the main and wiretap links following independent Málaga distributions. In [14], the secrecy throughput of the coherent FSO communication in the presence of a multi-input multi-output (MIMO) multi-apertures eavesdropper was studied for the Gamma-Gamma fading channel conditions.

Motivated by the latest advances in the PLS analysis on FSO communication and aiming at investigating the PLS performance of FSO communications under more realistic conditions, we study in this paper the secrecy performance of FSO communications under the Wyner's wiretap model over Málaga fading channels under different realistic scenarios. The choice of Málaga distribution as the investigated statistical model is justified by its applicability to all atmospheric turbulence regimes and its generality, which encompasses some of the most widely used distributions such as log-normal, exponential, and Gamma-Gamma, etc. [17]. The main contributions of this article are as follows:

- We comprehensively analyze the secrecy performance of FSO communication under different realistic scenarios based on the positions of the eavesdropper (i.e., the eavesdropper is close to the receiver, the eavesdropper is close to the transmitter, and the eavesdropper is close to neither the transmitter nor the receiver).
- Novel expressions are obtained for the average secrecy capacity and secrecy outage probability for different eavesdropping scenarios.
- The impact of correlation on the secrecy performance metrics such as ASC and SOP for FSO communication is evaluated.

The remaining parts of the paper are structured as follows. The three different scenarios (i.e., *Scenarios A, B,* and *C* in the paper) for the eavesdropping of FSO communications as well as the FSO channel model are elaborated in Section II. The secrecy performance for the three different scenarios of eavesdropping are conducted in Sections III and IV, respectively. The analytical results verified with simulations are presented and discussed in Section V. Section VI briefly summarizes this work.

Notations: $[x]^+ = \max(x, 0)$, $\mathrm{E}\{\cdot\}$ denotes the expectation operator, $\Gamma(\cdot)$ represents the Gamma function [18, Eq. (8.310)], $u(\cdot)$ is the unit step function [18, p. xliv]. $G_{p,q}^{m,n}(\cdot)$ is the Meijer G-function [18, Eq. (9.343)], $H_{p,q:u,v:e,f}^{m,n:s,t:i,j}(\cdot)$ denotes the extended generalized bivariate Fox H-function (EGBFHF) [19,

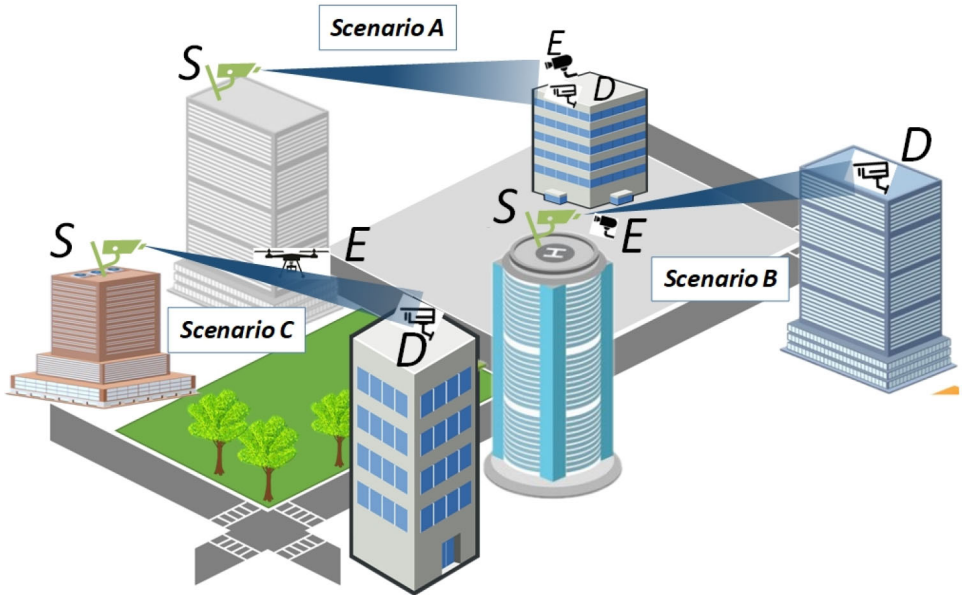


Fig. 1. Investigated PLS scenarios for FSO communications. *Scenario A:* Eavesdropper close to the legitimate receiver; *Scenario B:* Eavesdropper close to the legitimate transmitter; and *Scenario C:* Eavesdropper not close to the legitimate transmitter nor the receiver.

Eq. (2.56)], which can be readily evaluated with Mathematica [20, Table I], $U(\cdot, \cdot, \cdot)$ is the Kummer hypergeometric function [18, Eq. (9.210)].

2. FSO Channel and System Models

In this article, we consider an intensity modulation/direct detection (IM/DD) based FSO system. The fading behaviors of the FSO links are characterized by the generalized Málaga model, which takes into account three components: the LoS component, the component that is coupled to the LoS component and quasi-forward scattered by the eddies on the propagation axis, and the component resulting from the energy that is scattered by off-axis eddies [21].

The investigated security scenarios for the FSO communication are illustrated in Fig. 1. The legitimate source *S* sends confidential information to the legitimate destination node *D* over the main channel. The eavesdropper *E* attempts to intercept the information by decoding its received signal from the eavesdropper channel. For FSO communications, the PLS analysis can be classified into the following three scenarios depending on the position of the eavesdropper:

1) *Scenario A. Eavesdropper close to the legitimate receiver:* This is arguably the most probable case for eavesdropping in FSO communications since the legitimate receiver serves as a reference for the eavesdropper to align its direction. In this scenario, the main and wiretap fading channels will be correlated due to their spatial proximity or similarity of the scatterers surrounding them.
2) *Scenario B. Eavesdropper close to the legitimate transmitter:* In this case, in order to intercept the beam without partially blocking the LoS between the legitimate peers, a sufficiently sophisticated device is required. Also, it is also reasonable to assume that the SNR received by the eavesdropper is a constant since the turbulence and attenuation can be ignored due to its short distance to the transmitter.
3) *Scenario C. Eavesdropper not close to the legitimate transmitter and receiver:* When the eavesdropper is neither close to the transmitter nor the receiver, it is practically very difficult, though still possible (e.g., with the help of drone), to correctly align its position such that it can receive the irradiance from the laser beam towards the legitimate receiver.

In the following sections, we will analyze the secrecy performance of FSO communications under the above three scenarios, respectively.

The regenerated electrical signals at the FSO receiver nodes D and E, respectively, can be expressed as

$$y_D = \eta I_D s + w = \eta Y_D X_D s + w, \tag{1}$$

$$y_E = \eta I_E s + w = \eta Y_E X_E s + w, \tag{2}$$

where s is the transmitted symbol with unit energy, the random variables (RVs) I_D and I_E represent the received signal irradiance that is affected by the atmospheric turbulence at the corresponding receiver aperture, w represents the additive white Gaussian noise (AWGN) with power spectral density $\frac{N_0}{2}$, which, without loss of generality, is assumed to be the same for both channel links. In (1) and (2), Y_x and X_x, $x \in \{D, E\}$, represent the small-scale and large-scale fluctuations, respectively [22]. As in [4], we consider the realistic scenario that the turbulent flow of the large-scale eddies induce the correlation while the small-scale fluctuation is assumed to be independent between D and E. The instantaneous signal-to-noise ratio (SNR) between S and x, $x \in \{D, E\}$, can be written as $\gamma_{Sx} = \frac{\eta^2 Y_x^2 X_x^2}{N_0}$. In the following, let us denote the instantaneous SNRs for the S-D and S-E links γ_1 and γ_2, respectively, for simplicity.

When the eavesdropper is located close to the legitimate receiver (i.e., *Scenario A*), the main and wiretap channel links are assumed to be arbitrarily correlated due to either close proximity of the nodes D and E or similarity of the scatterers surrounding them. The joint probability density function (PDF) $f_{\gamma_1,\gamma_2}(\gamma_1, \gamma_2)$ of the SNRs γ_1 and γ_2 over the considered arbitrarily correlated Málaga fading channel can be obtained from [21, Eq. (7)], after some algebra, as follows:

$$f_{\gamma_1,\gamma_2}(\gamma_1, \gamma_2) = \sum_{t=0}^{\infty} \mathcal{F}_t \frac{(-1)^{k-1}}{(k-1)!} \cdot \prod_{p=1}^{2} \Bigg[\frac{1}{2\sqrt{\gamma_p \mu_p}} \sum_{k=1}^{\beta} \cdot \binom{\beta-1}{k-1} \cdot \left(\frac{\beta\Omega(1-\rho^2)\sqrt{\gamma_p}}{(\xi\beta+\Omega_1)\sqrt{\mu_p}} \right)^{\frac{\alpha+t-k}{2}}$$
$$\cdot \left(-\frac{\Omega_1\sqrt{\gamma_p}}{(\xi\beta+\Omega_1)\xi\sqrt{\mu_p}} \right)^{k-1} \cdot G_{0,2}^{2,0}\left(\frac{\beta}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)} \sqrt{\frac{\gamma_p}{\mu_p}} \middle| \begin{matrix} - \\ \frac{\alpha+t-k}{2}, -\frac{\alpha+t-k}{2} \end{matrix} \right) \Bigg], \tag{3}$$

where

$$\mathcal{F}_t = \xi^{2(\beta-1)} \cdot \left(\frac{\beta}{\xi\beta+\Omega_1} \right)^{2\beta} \cdot \frac{(1-\rho^2)^{-\alpha-2t} \cdot \rho^{2t}}{\Gamma(\alpha)\Gamma(t)\Gamma(\alpha+t) \cdot \Omega^{2\alpha+2}}, \tag{4}$$

and $\rho \in [0, 1)$ represents the correlation factor between the Málaga fading channels, $\mu_p = \mathrm{E}\{\gamma_p\}$ denotes the average SNR of the corresponding FSO link, the parameter α describes the fading severity due to the atmospheric turbulence, β is a natural number related to the effective number of small-scale cells, $\xi = 2b_0(1-\delta)$ is the average power of the scattering component with $2b_0$ being the average power of the total scatter components and δ $(0 < \delta < 1)$ being the amount of scattered power coupled to LoS component, Ω is the average power of the large-scale fluctuation, $\Omega_1 = \Omega' + 2b_0\delta + 2\sqrt{2b_0\delta\Omega'}\cos(\phi_A - \phi_B)$, where Ω' is the average power of the LoS component, ϕ_A and ϕ_B are the deterministic phases of the LoS component and the scatterers coupled to the LoS component, respectively [21], [23], [24].

When the eavesdropper E is located close to the legitimate transmitter (i.e., *Scenario B*), the effect of the turbulence and attenuation on the eavesdropper's received SNR can be ignored [11]. Therefore, the electrical SNR γ_2 can be considered as a constant of large value under *Scenario B*. However, the link between the transmitter S and legitimate receiver D is still subject to the random fluctuations described by the Málaga model. Then, the PDF $f_{\gamma_1}(\gamma)$ and the cumulative distribution function (CDF) $F_{\gamma_1}(\gamma)$ of the SNR γ_1 can be expressed as follows [25], [26]:

$$f_{\gamma_1}(\gamma) = \mathcal{P} \cdot \sum_{k=1}^{\beta} \mathcal{Q}_k \cdot \left(\frac{1}{\mu_1} \right)^{\frac{\alpha+k}{4}} \cdot \gamma^{\frac{\alpha+k}{4}-1} \cdot G_{0,2}^{2,0}\left(\frac{\alpha\beta}{(\xi\beta+\Omega_1)} \sqrt{\frac{\gamma}{\mu_1}} \middle| \begin{matrix} - \\ \frac{\alpha-k}{2}, -\frac{\alpha-k}{2} \end{matrix} \right), \tag{5}$$

$$F_{\gamma_1}(\gamma) = 2\mathcal{P} \cdot \sum_{k=1}^{\beta} \mathcal{Q}_k \cdot \left(\frac{1}{\mu_1}\right)^{\frac{\alpha+k}{4}} \cdot \gamma^{\frac{\alpha+k}{4}} \cdot G_{1,3}^{2,1}\left(\frac{\alpha\beta}{(\xi\beta+\Omega_1)}\sqrt{\frac{\gamma}{\mu_1}}\,\middle|\, \begin{matrix} 1-\frac{\alpha+k}{2} \\ \frac{\alpha-k}{2}, -\frac{\alpha-k}{2}, -\frac{\alpha+k}{2} \end{matrix}\right), \tag{6}$$

where

$$\mathcal{P} = \frac{\alpha^{\frac{\alpha}{2}}}{2\xi^{\frac{\alpha}{2}+1}\cdot\Gamma(\alpha)} \cdot \left(\frac{\xi\beta}{\xi\beta+\Omega_1}\right)^{\frac{\alpha}{2}+\beta}, \tag{7}$$

$$\mathcal{Q}_k = \binom{\beta-1}{k-1} \cdot \frac{(\xi\beta+\Omega_1)^{1-\frac{k}{2}}}{\Gamma(k)} \cdot \left(\frac{\Omega_1}{\xi}\right)^{k-1} \cdot \left(\frac{\alpha}{\beta}\right)^{\frac{k}{2}}. \tag{8}$$

3. Secrecy Analysis for *Scenarios A and C*

3.1 *ASC Analysis for* Scenarios A *and* C

The instantaneous secrecy capacity of the considered wiretap model is defined as [27]

$$C_s(\gamma_1, \gamma_2) = [\ln(1+\gamma_1) - \ln(1+\gamma_2), 0]^+, \tag{9}$$

where $\ln(1+\gamma_1)$ and $\ln(1+\gamma_2)$ are the instantaneous channel capacity of the main and wiretap channels, respectively.

Under the active eavesdropping scenario, the node S has full CSI of both the main and wiretap channels, based on which S can adapt the achievable secrecy rate accordingly [28]. In this case, the ergodic or average secrecy capacity is a useful secrecy performance metric. The ASC $\overline{C}_s$ of the investigated FSO system over arbitrarily correlated Málaga channels can be formulated as [9]

$$\begin{aligned}\overline{C}_s &= \mathrm{E}\left\{C_s(\gamma_1,\gamma_2)\right\} = \int_0^\infty \int_0^\infty C_s(\gamma_1,\gamma_2)\cdot f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)\,d\gamma_1 d\gamma_2 \\ &= \int_0^\infty \ln(1+\gamma_1)\cdot\int_0^{\gamma_1} f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)d\gamma_2 d\gamma_1 - \int_0^\infty \ln(1+\gamma_2)\cdot\int_{\gamma_2}^\infty f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)d\gamma_1 d\gamma_2 \\ &= C_1 - C_2,\end{aligned} \tag{10}$$

where

$$C_1 = \int_0^\infty \ln(1+\gamma_1)\cdot\int_0^{\gamma_1} f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)d\gamma_2 d\gamma_1, \tag{11}$$

$$C_2 = \int_0^\infty \ln(1+\gamma_2)\cdot\int_{\gamma_2}^\infty f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)d\gamma_1 d\gamma_2. \tag{12}$$

We first solve the integral C_1. Substituting the joint PDF $f_{\gamma_1,\gamma_2}(\gamma_1,\gamma_2)$ into the expression of C_1, the following double integral $\mathcal{I}_1$ is deduced:

$$\mathcal{I}_1 = \int_0^\infty \ln(1+\gamma_1)\cdot\gamma_1^{\frac{\alpha+t+k-4}{4}}\cdot G_{0,2}^{2,0}\left(\frac{\beta\sqrt{\gamma_1}}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}}\,\middle|\, \begin{matrix} - \\ \mathcal{K}_1 \end{matrix}\right)\cdot\mathcal{I}_{1a}\,d\gamma_1, \tag{13}$$

where $\mathcal{I}_{1a} = \int_0^{\gamma_1}\gamma_2^{\frac{\alpha+t+k-4}{4}}\cdot G_{0,2}^{2,0}\left(\frac{\beta(1-\rho^2)^{-1}\sqrt{\gamma_2}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_2}}\,\middle|\, \begin{matrix} - \\ \mathcal{K}_1 \end{matrix}\right)d\gamma_2$ and $\mathcal{K}_1 = (\frac{\alpha+t-k}{2}, -\frac{\alpha+t-k}{2})$.

Utilizing the property [29, Eq. (2.24.2.2)] for $\mathcal{I}_{1a}$, the following results:

$$\mathcal{I}_{1a} = \frac{1}{2\pi}\cdot\gamma_1^{\frac{\alpha+t+k}{4}}\cdot G_{1,5}^{4,1}\left(\left[\frac{\beta}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_2}}\right]^2\cdot\gamma_1\,\middle|\, -\frac{\alpha+t+k-4}{4}\mathcal{K}_2\right), \tag{14}$$

where $\mathcal{K}_2 = (\frac{\alpha+t-k}{4}, \frac{\alpha+t-k+2}{4}, -\frac{\alpha+t-k}{4}, -\frac{\alpha+t-k-2}{4}, -\frac{\alpha+t+k}{4})$.

Substituting (14) into (13) and making the change of RVs: $\sqrt{\gamma_1} = y$, $\mathcal{I}_1$ can be rewritten as

$$\mathcal{I}_1 = \frac{1}{\pi} \cdot \int_0^{\infty} y^{\alpha+t+k-1} \cdot G_{0,2}^{2,0}\Big(\frac{\beta}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}} y \,\Big|_{\mathcal{K}_1'}^{-}\Big) \cdot G_{1,5}^{4,1}\Big(\Big[\frac{\beta}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_2}}\Big]^2 \cdot y^2 \,\Big|_{\mathcal{K}_2'}^{-\frac{\alpha+t+k-4}{4}}\Big) \cdot G_{2,2}^{1,2}\Big(y^2 \,\Big|_{1,0}^{1,1}\Big)\, dy, \tag{15}$$

where the terms $\mathcal{K}_1' = (\frac{\alpha+t-k}{2}, -\frac{\alpha+t-k}{2})$ and $\mathcal{K}_2' = (\frac{\alpha+t-k}{4}, \frac{\alpha+t-k+2}{4}, -\frac{\alpha+t-k}{4}, -\frac{\alpha+t-k-2}{4}, -\frac{\alpha+t+k}{4})$.

The integral $\mathcal{I}_1$ in (15) can be solved with the aid of [30, Eq. (18)] in terms of the EGBFHF as follows:

$$\mathcal{I}_1 = \mathcal{A} \cdot H_{2,0:2,2:1,5}^{0,2:1,2:4,1}\Bigg(\Big[\frac{\Omega(\xi\beta+\Omega_1\sqrt{\mu_1})}{\beta(1-\rho^2)^{-1}}\Big]^2, \frac{\mu_1}{16\mu_2} \,\Bigg|\, \begin{matrix}(\frac{2-3\alpha-3t-k}{2}; 2, 2), (\frac{2-\alpha-t-3k}{2}; 2, 2) \\ - \end{matrix} \,\Bigg|\, \begin{matrix}(1,1),(1,1) \\ (1,1),(0,1)\end{matrix} \,\Bigg|\, \begin{matrix}(-\frac{\alpha+t+k-4}{4}, 1) \\ \mathcal{K}_2'\end{matrix}\Bigg), \tag{16}$$

where $\mathcal{A} = \frac{1}{\pi} \cdot [\frac{\beta(1-\rho^2)^{-1}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_1}}]^{-(\alpha+t+k)}$.

Next, we solve the integral C_2. On substituting the joint PDF (3) into the expression of C_2, the following integral $\mathcal{I}_2$ occurs:

$$\mathcal{I}_2 = \int_0^{\infty} \ln(1+\gamma_2) \cdot \gamma_2^{\frac{\alpha+t+k-4}{4}} \cdot G_{0,2}^{2,0}\left(\frac{\beta\sqrt{\gamma_2}}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_2}} \,\middle|\, \begin{matrix}- \\ \mathcal{K}_1\end{matrix}\right) \cdot \mathcal{I}_{2a}\, d\gamma_2, \tag{17}$$

where $\mathcal{I}_{2a} = \int_{\gamma_2}^{\infty} \gamma_1^{\frac{\alpha+t+k-4}{4}} G_{0,2}^{2,0}\left(\frac{\beta(1-\rho^2)^{-1}\sqrt{\gamma_1}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_1}} \,|\, \begin{matrix}- \\ \mathcal{K}_1\end{matrix}\right) d\gamma_1$.

Utilizing [29, Eq. (2.24.2.3)], $\mathcal{I}_{2a}$ can be solved as

$$\mathcal{I}_{2a} = \frac{1}{2\pi} \cdot \gamma_2^{\frac{\alpha+t+k}{4}} \cdot G^{5,0}1,5\left(\Big[\frac{\beta}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}}\Big]^2 \cdot \gamma_2 \,\middle|\, \begin{matrix}-\frac{\alpha+t+k-4}{4} \\ \mathcal{K}_3\end{matrix}\right), \tag{18}$$

where $\mathcal{K}_3 = (-\frac{\alpha+t+k}{4}, \frac{\alpha+t-k}{4}, \frac{\alpha+t-k+2}{4}, -\frac{\alpha+t-k}{4}, -\frac{\alpha+t-k-2}{4})$.

Substituting (18) into (17) and making the following change of RVs: $\sqrt{\gamma_2} = z$, $\mathcal{I}_2$ can be rewritten as

$$\mathcal{I}_2 = \frac{1}{\pi} \cdot \int_0^{\infty} z^{\alpha+t+k-1} \cdot G_{0,2}^{2,0}\Big(\frac{\beta}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_2}} z \,\Big|_{\mathcal{K}_1'}^{-}\Big) \cdot G_{1,5}^{5,0}\Big(\Big[\frac{\beta}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}}\Big]^2 z^2 \,\Big|_{\mathcal{K}_3'}^{-\frac{\alpha+t+k-4}{4}}\Big) \cdot G_{2,2}^{1,2}\Big(z^2 \,\Big|_{1,0}^{1,1}\Big) dz, \tag{19}$$

where $\mathcal{K}_3'$ consists of the following five terms: $\mathcal{K}_3' = (-\frac{\alpha+t+k}{4}, \frac{\alpha+t-k}{4}, \frac{\alpha+t-k+2}{4}, -\frac{\alpha+t-k}{4}, -\frac{\alpha+t-k-2}{4})$.

The integral $\mathcal{I}_2$ in (19) can be solved again with the help of [30, Eq. (18)] in terms of the EGBFHF as

$$\mathcal{I}_2 = \mathcal{B} \cdot H_{2,0:2,2:1,5}^{0,2:1,2:5,0}\Bigg(\Big[\frac{\Omega(\xi\beta+\Omega_1\sqrt{\mu_2})}{\beta(1-\rho^2)^{-1}}\Big]^2, \frac{\mu_2}{16\mu_1} \,\Bigg|\, \begin{matrix}(\frac{2-3\alpha-3t-k}{2}; 2, 2), (\frac{2-\alpha-t-3k}{2}; 2, 2) \\ - \end{matrix} \,\Bigg|\, \begin{matrix}(1,1),(1,1) \\ (1,1),(0,1)\end{matrix} \,\Bigg|\, \begin{matrix}(-\frac{\alpha+t+k-4}{4}, 1) \\ \mathcal{K}_3'\end{matrix}\Bigg), \tag{20}$$

where $\mathcal{B} = \frac{1}{\pi} \cdot [\frac{\beta(1-\rho^2)^{-1}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_2}}]^{-(\alpha+t+k)}$.

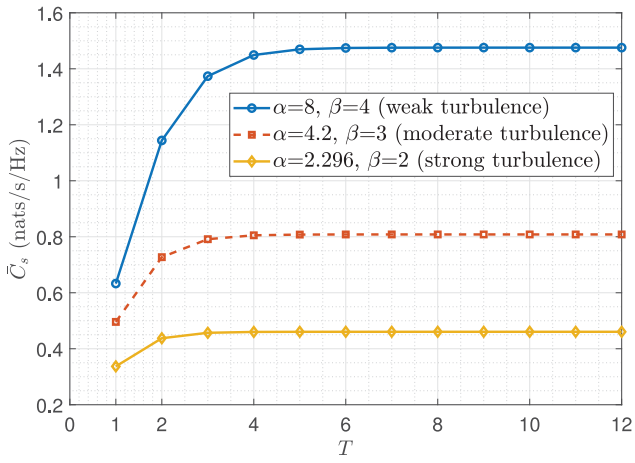


Fig. 2. The computed analytical ASC using different number of summation terms under different atmospheric conditions.

Finally, the exact expression for the ASC of FSO system over arbitrarily correlated Málaga ($\mathcal{M}$) turbulence channels can be obtained, after some algebra, as follows:

$$\bar{C}_s = \sum_{t=0}^{\infty} \mathcal{F}_t \cdot \prod_{p=1}^{2} \left[\frac{1}{2\sqrt{\mu_p}} \sum_{k=1}^{\beta} \frac{(-1)^{k-1}}{(k-1)!} \cdot \left(\frac{\beta\Omega(1-\rho^2)}{(\xi\beta+\Omega_1)\sqrt{\mu_p}} \right)^{\frac{\alpha+t-k}{2}} \right.$$
$$\left. \cdot \binom{\beta-1}{k-1} \cdot \left(-\frac{\Omega_1}{(\xi\beta+\Omega_1)\xi\sqrt{\mu_p}} \right)^{k-1} \right] \cdot (\mathcal{I}_1 - \mathcal{I}_2), \tag{21}$$

where the closed-form expressions of $\mathcal{I}_1$ and $\mathcal{I}_2$ are given in (16) and (20), respectively.

Remark 1: Although the expression for ASC in (21) is expressed in terms of an infinite series, it converges for finitely small values of $t = T$ up to 5 decimal places. For instance, the plots for ASC values for $\mu_1 = 10$ dB and $\mu_2 = 3$ dB for different turbulence conditions are shown in Fig. 2. It is evident that the curves converge to a fixed ASC value with only around $T = 6$ terms for all atmospheric fading conditions. In this paper, we have used $T = 11$ terms for the analytical curves of all figures.

Remark 2: When the eavesdropper is far from both the legitimate receiver and transmitter (i.e., *Scenario C*), it is more likely that the main and wiretap channels will experience independent fading. This scenario is actually a special case of *Scenario A* with the correlation factor ρ equalling 0. Hence, the secrecy performance results derived for *Scenario A* are actually also valid for *Scenario C* simply by setting $\rho = 0$.

3.2 SOP Analysis for Scenarios A and C

The concept of outage capacity is invoked when the channel varies slowly and the instantaneous SNR can be considered as constant for the whole transmission session [31]. The outage probability is then associated with the outage capacity, which is the probability that the system cannot successfully decode the information [32]. In the context of PLS, the secrecy outage probability is a widely used secrecy performance metric in the scenario where the node *S* does not have *E*'s CSI [33]. The SOP is mathematically expressed as [34]

$$P_o = \Pr[C_s(\gamma_1, \gamma_2) \leq R_s] = \Pr[\gamma_1 \leq \Theta\gamma_2 + \Theta - 1]$$
$$= \int_0^{\infty} \int_0^{(1+\gamma_2)\Theta-1} f_{\gamma_1,\gamma_2}(\gamma_1, \gamma_2)\, d\gamma_1 d\gamma_2, \tag{22}$$

where R_s is a predefined secrecy rate and $\Theta = \exp(R_s) \geq 1$.

Assuming $\gamma_2 \to \infty$, a lower bound of the SOP, P_o^L, can be derived as

$$P_o^L \triangleq \Pr[\gamma_1 < \Theta\gamma_2] \leq \Pr[\gamma_1 \leq \Theta\gamma_2 + \Theta - 1] = P_o. \tag{23}$$

Then, P_o^L can be expressed in terms of the joint PDF of the SNRs γ_1 and γ_2 as

$$P_o^L = \int_0^\infty \int_0^{\Theta\gamma_2} f_{\gamma_1,\gamma_2}(\gamma_1, \gamma_2)\, d\gamma_1 d\gamma_2. \tag{24}$$

Substituting (3) into (24), the lower bound of the SOP, P_o^L, can be rewritten as

$$P_o^L = \sum_{t=0}^{\infty} \mathcal{F}_t \cdot \prod_{p=1}^{2} \Bigg[\frac{1}{2\sqrt{\mu_p}} \sum_{k=1}^{\beta} \binom{\beta-1}{k-1} \cdot \frac{(-1)^{k-1}}{(k-1)!} \cdot \left(\frac{\beta\Omega(1-\rho^2)}{(\xi\beta+\Omega_1)\sqrt{\mu_p}} \right)^{\frac{\alpha+t-k}{2}} \cdot \left(-\frac{\Omega_1}{(\xi\beta+\Omega_1)\xi\sqrt{\mu_p}} \right)^{k-1} \Bigg] \cdot \mathcal{I}_3, \tag{25}$$

where $\mathcal{I}_3$ is the double integral expressed as

$$\mathcal{I}_3 = \int_0^\infty \gamma_2^{\frac{\alpha+t+k-4}{4}} G_{0,2}^{2,0}\left(\frac{\beta(1-\rho^2)^{-1}\sqrt{\gamma_2}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_2}} \middle| \begin{matrix} - \\ \mathcal{K}_1 \end{matrix} \right) \cdot \underbrace{\int_0^{\Theta\gamma_2} \gamma_1^{\frac{\alpha+t+k-4}{4}} G_{0,2}^{2,0}\left(\frac{\beta(1-\rho^2)^{-1}\sqrt{\gamma_1}}{\Omega(\xi\beta+\Omega_1)\sqrt{\mu_1}} \middle| \begin{matrix} - \\ \mathcal{K}_1 \end{matrix} \right) d\gamma_1}_{\mathcal{I}_{3a}} \, d\gamma_2. \tag{26}$$

We first consider the single integral $\mathcal{I}_{3a}$ in (26), which can be solved with the assistance of property [29, Eq. 2.24.2.2] as follows:

$$\mathcal{I}_{3a} = \frac{(\Theta\gamma_2)^{\frac{\alpha+t+k}{4}}}{2\pi} \cdot G_{1,5}^{4,1}\left(\frac{\Theta}{16} \cdot \left[\frac{\beta}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}} \right]^2 \cdot \gamma_2 \middle| \begin{matrix} 1-\frac{\alpha+t+k}{4} \\ \mathcal{K}_2 \end{matrix} \right). \tag{27}$$

Substituting (27) into (26) and utilizing the equality [29, Eq. 2.24.1.1] leads to the following solution in terms of Meijer G-function for the double integral $\mathcal{I}_3$:

$$\begin{aligned} \mathcal{I}_3 &= \frac{1}{2\pi} \cdot \Theta^{\frac{\alpha+t+k}{4}} \cdot \int_0^\infty \gamma_2^{\frac{\alpha+t+k-2}{2}} \cdot G_{0,2}^{2,0}\left(\frac{\beta\sqrt{\gamma_2}}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_2}} \middle| \begin{matrix} - \\ \mathcal{K}_1 \end{matrix} \right) \\ &\quad \cdot G_{1,5}^{4,1}\left(\frac{\Theta}{16} \cdot \left[\frac{\beta}{\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}} \right]^2 \cdot \gamma_2 \middle| \begin{matrix} 1-\frac{\alpha+t+k}{4} \\ \mathcal{K}_2 \end{matrix} \right) d\gamma_2 \\ &= \frac{1}{4\pi^2} \cdot \Theta^{\frac{\alpha+t+k}{4}} \cdot \left[\frac{\beta\sqrt{\Theta}}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}} \right]^{-(\alpha+t+k)} \cdot G_{5,5}^{5,4}\left(\frac{\mu_1}{\Theta\mu_2} \middle| \begin{matrix} 1-\frac{\alpha+t+k}{2}-\mathcal{K}_2 \\ \mathcal{K}_2 \end{matrix} \right). \end{aligned} \tag{28}$$

Finally, substituting (28) into (25), the lower bound of the SOP P_o^L can be expressed as

$$P_o^L = \frac{1}{4\pi^2} \cdot \sum_{t=0}^{\infty} \mathcal{F}_t \cdot \Theta^{\frac{\alpha+t+k}{4}} \cdot \prod_{p=1}^{2} \Bigg[\frac{1}{2\sqrt{\mu_p}} \sum_{k=1}^{\beta} \frac{(-1)^{k-1}}{(k-1)!} \cdot \binom{\beta-1}{k-1} \cdot \left(\frac{\beta\Omega(1-\rho^2)}{(\xi\beta+\Omega_1)\sqrt{\mu_p}} \right)^{\frac{\alpha+t-k}{2}} \cdot \left(-\frac{\Omega_1}{(\xi\beta+\Omega_1)\xi\sqrt{\mu_p}} \right)^{k-1} \Bigg] \cdot \left[\frac{\beta\sqrt{\Theta}}{4\Omega(1-\rho^2)(\xi\beta+\Omega_1)\sqrt{\mu_1}} \right]^{-(\alpha+t+k)} \cdot G_{5,5}^{5,4}\left(\frac{\mu_1}{\Theta\mu_2} \middle| \begin{matrix} 1-\frac{\alpha+t+k}{2}-\mathcal{K}_2 \\ \mathcal{K}_2 \end{matrix} \right), \tag{29}$$

where $\mathcal{K}_2 = (\frac{\alpha+t-k}{4}, \frac{\alpha+t-k+2}{4}, -\frac{\alpha+t-k}{4}, -\frac{\alpha+t-k-2}{4}, -\frac{\alpha+t+k}{4})$.

3.3 Asymptotic SOP Analysis for Scenarios A and C

In order to thoroughly investigate the impact of the link correlation and the Málaga fading channel on the SOP performance, we evaluate the secrecy diversity of the considered system for high values of the average SNR, μ_1.

Under this assumption, employing the Slater's theorem to rewrite the Meijer G-function in terms of the generalized hypergeometric function and utilizing the property $\lim_{z\to 0} {}_pF_q(a_p; b_q; \pm z) \to 1$, the following asymptotic relation is obtained:

$$G_{5,5}^{5,4}\left(\frac{\mu_1}{\Theta\mu_2}\middle|\begin{matrix}\mathbf{a_p}\\ \mathbf{b_q}\end{matrix}\right) \approx \sum_{h=1}^{4}\left(\frac{\mu_1}{\Theta\mu_2}\right)^{a_h-1}\cdot\frac{\prod_{j=1}^{4}\Gamma(a_h-a_j)^*\prod_{j=1}^{5}\Gamma(1-a_h+b_j)}{\Gamma(1-a_h+a_5)}, \tag{30}$$

where $\mathbf{a_p} = [a_1, a_2, \cdot, \cdot, \cdot, a_5] = [1-\frac{3\alpha+3t+k}{4}, 1-\frac{3\alpha+3t+k+2}{4}, 1-\frac{\alpha+t+3k}{4}, 1-\frac{\alpha+t+3k+2}{4}, 1-\frac{\alpha+t+k}{4}]$, $\mathbf{b_q} = \mathcal{K}_2$, and $(\cdot)^*$ indicates to ignore the terms with the subscript $j = h$.

Now, substituting the asymptotic relation given by (30) into (29), the asymptotic expression for the lower bound of SOP is approximated as

$$\begin{aligned}P_o^L \approx \frac{1}{16\pi^2\sqrt{\mu_2}}\sum_{t=0}^{\infty}\mathcal{F}_t\Bigg[&\sum_{k=1}^{\beta}\frac{(-1)^k\Theta^{\frac{\alpha+t+k}{4}}\binom{\beta-1}{k-1}}{(k-1)!}\cdot\left(\frac{\beta\Omega(1-\rho^2)}{(\zeta\beta+\Omega_1)}\right)^{\frac{\alpha+t-k}{2}}\cdot\left(-\frac{\Omega_1}{(\zeta\beta+\Omega_1)\zeta}\right)^{k-1}\Bigg]\\ &\cdot\sum_{k=1}^{\beta}\frac{(-1)^k\binom{\beta-1}{k-1}}{(k-1)!}\cdot\left(\frac{\beta\Omega(1-\rho^2)}{(\zeta\beta+\Omega_1)\sqrt{\mu_2}}\right)^{\frac{\alpha+t-k}{2}}\cdot\left(-\frac{\Omega_1}{(\zeta\beta+\Omega_1)\zeta\sqrt{\mu_2}}\right)^{k-1}\\ &\cdot\left(\frac{\beta\sqrt{\Theta}}{4\Omega(1-\rho^2)(\zeta\beta+\Omega_1)}\right)^{-(\alpha+t+k)}\\ &\cdot\sum_{h=1}^{4}\frac{\Pi_{j=1}^{4}\Gamma(a_h-a_j)^*\Pi_{j=1}^{5}\Gamma(1-a_h+b_j)}{\Gamma(1-a_h+a_5)(\Theta\mu_2)^{a_h-1}}\cdot\mu_1^{\frac{\alpha+t+k}{4}+a_h-1}.\end{aligned} \tag{31}$$

It is evident from (31) that the asymptotic performance will be dominated by the smallest power of μ_1 which corresponds to $t = 0$. Thus, on substituting the values of a_h, $h \in [1, 4]$ in (31), it is concluded that the asymptotic slope of the lower bound of SOP curve is $\min\{\frac{\alpha}{2}, \frac{1}{2}\}$. In practical channels, the value of α is generally larger than 1. This implies that the slope of the asymptotic curve is $\frac{1}{2}$ for practical channels.

Remark 3: Through the asymptotic analysis, it is revealed that the asymptotic slope of P_o^L, that is, the secrecy diversity order is independent of the correlation coefficient, ρ. However, the coding gain significantly depends on the value of ρ as indicated by (31).

4. Secrecy Analysis for *Scenario B*

4.1 ASC Analysis for Scenario B

When the eavesdropper is quite close to the transmitter (i.e., *Scenario B*), the atmospheric turbulence plays an insignificant role on its performance. Therefore, the SNR $\gamma_2 = \mu_2$ of the eavesdropper's link can be viewed as a constant while the SNR γ_1 of the long-distance legitimate transmission is still subject to atmospheric turbulence with fading distribution functions given in (5)–(8). Then, the ASC under *Scenario B* can be expressed as

$$\begin{aligned}\overline{C}_s &= \mathrm{E}\left\{[\ln(1+\gamma_1) - \ln(1+\gamma_2), 0]^+\right\}\\ &= \int_0^{\infty}\ln(1+\gamma_1)\cdot u(\gamma_1-\mu_2)\cdot f_{\gamma_1}(\gamma_1)\,d\gamma_1.\end{aligned} \tag{32}$$

Substituting (6) into (32) and utilizing the following transformations related to the Meijer G-functions: $\ln(1+x) = G_{2,2}^{1,2}\left(x\middle|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right)$, $u(x-1) = G_{1,1}^{0,1}\left(x\middle|\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ [35], we can obtain the ASC under *Scenario B* expressed by the following integral:

$$\overline{C}_s = \mathcal{P}\cdot\sum_{k=1}^{\beta}\mathcal{Q}_k\cdot\left(\frac{1}{\mu_1}\right)^{\frac{\alpha+k}{4}}\cdot\int_0^{\infty}\gamma^{\frac{\alpha+k}{4}-1}\cdot G_{2,2}^{1,2}\left(\gamma\middle|\begin{smallmatrix}1,1\\1,0\end{smallmatrix}\right)$$
$$\cdot\, G_{1,1}^{0,1}\left(\frac{\gamma}{\mu_2}\middle|\begin{smallmatrix}1\\0\end{smallmatrix}\right)\cdot G_{0,2}^{2,0}\left(\frac{\alpha\beta}{(\xi\beta+\Omega_1)}\cdot\sqrt{\frac{\gamma}{\mu_1}}\middle|\begin{smallmatrix}-\\\frac{\alpha-k}{2},-\frac{\alpha-k}{2}\end{smallmatrix}\right)d\gamma. \tag{33}$$

Finally, making the change of RVs: $\sqrt{\frac{\gamma}{\mu_1}} = t$ in (33) and utilizing the equality [30, Eq. (18)] for the resulting integral, we can obtain the exact expression for ASC under *Scenario B* in (34) as

$$\overline{C}_s = 2\mathcal{P}\cdot\sum_{k=1}^{\beta}\mathcal{Q}_k\cdot\left(\frac{1}{\mu_1}\right)^{\frac{\alpha+k}{2}}\cdot\left[\frac{\alpha\beta}{(\xi\beta+\Omega_1)}\right]^{-\left(\frac{\alpha+k}{2}-1\right)}$$
$$\cdot\, H_{2,0:2,2:1,1}^{0,2:1,2:0,1}\left(\frac{\mu_1(\xi\beta+\Omega_1)^2}{(\alpha\beta)^2},\frac{\mu_1(\xi\beta+\Omega_1)^2}{\mu_2(\alpha\beta)^2}\middle|\begin{matrix}(2-\alpha;2,2),(2-k;2,2)\\-\end{matrix}\middle|\begin{matrix}(1,1),(1,1)\\(1,1),(0,1)\end{matrix}\middle|\begin{matrix}(1,1)\\(0,1)\end{matrix}\right), \tag{34}$$

where $\mathcal{P}$ and $\mathcal{Q}_k$ are given in (7) and (8), respectively.

4.2 SOP Analysis for Scenario B

Under *Scenario B*, it is justified that only the channel for legitimate transmission is subject to fading caused by turbulence due to the close distance for the eavesdropping transmission. Then, the exact expression for the secrecy outage probability with target secrecy rate $R_s = \ln(\Theta)$ can be expressed as follows:

$$\begin{aligned}P_o &= \Pr\left[C_s(\gamma_1,\gamma_2)\le R_s\right]\\ &= \Pr\left[\gamma_1\le\Theta\mu_2+\Theta-1\right] = F_{\gamma_1}(\Theta\mu_2+\Theta-1)\\ &= 2\mathcal{P}\cdot\sum_{k=1}^{\beta}\mathcal{Q}_k\cdot\left(\frac{1}{\mu_1}\right)^{\frac{\alpha+k}{4}}\cdot(\Theta\mu_2+\Theta-1)^{\frac{\alpha+k}{4}}\cdot G_{1,3}^{2,1}\left(\frac{\alpha\beta\sqrt{\Theta\mu_2+\Theta-1}}{(\xi\beta+\Omega_1)\sqrt{\mu_1}}\middle|\begin{matrix}1-\frac{\alpha+k}{2}\\\frac{\alpha-k}{2},-\frac{\alpha-k}{2},-\frac{\alpha+k}{2}\end{matrix}\right),\end{aligned} \tag{35}$$

where $\mathcal{P}$ and $\mathcal{Q}_k$ are given in (7) and (8), respectively.

Remark 4: It is obvious from (35) that the SOP under *Scenario B* is fully characterized by the CDF of the electrical SNR at the legitimate receiver. Also, based on the property of CDF, it can be seen that the SOP approaches 1 when the SNR $\mu_2\to\infty$.

Remark 5: The exact expression for the PNZSC can be obtained from the expression of SOP by setting $\Theta = 1$ in (35). The PNZSC under *Scenario B* can be expressed as

$$PNZSC = 1 - 2\mathcal{P}\cdot\sum_{k=1}^{\beta}\mathcal{Q}_k\cdot\left(\frac{\mu_2}{\mu_1}\right)^{\frac{\alpha+k}{4}}\cdot G_{1,3}^{2,1}\left(\frac{\alpha\beta}{(\xi\beta+\Omega_1)}\cdot\sqrt{\frac{\mu_2}{\mu_1}}\middle|\begin{matrix}1-\frac{\alpha+k}{2}\\\frac{\alpha-k}{2},-\frac{\alpha-k}{2},-\frac{\alpha+k}{2}\end{matrix}\right). \tag{36}$$

It is observed from (36) that the PNZSC is only dependent on the ratio of the average SNRs of the eavesdropper and legitimate receiver, i.e., $\frac{\mu_2}{\mu_1}$, under the same optical channel condition.

4.3 Asymptotic SOP Analysis for Scenario B

To gain more insights on the impact of the Málaga fading channel on the secrecy performance for *Scenario B*, we conduct the secrecy diversity analysis for SOP by considering high values of the average SNR, μ_1, at the legitimate receiver.

Let us observe (35) for very high values of μ_1. Rewriting the Meijer G-function in (35) in terms of the generalized hypergeometric function using Slater's theorem and applying the relation

$\lim_{z\to 0}\, {}_pF_q(a_p; b_q; \pm z) \to 1$, the following asymptotic relation is deduced:

$$G_{1,3}^{2,1}\left(z\middle|\begin{matrix}1-\frac{\alpha+k}{2}\\ \frac{\alpha-k}{2}, -\frac{\alpha-k}{2}, -\frac{\alpha+k}{2}\end{matrix}\right) \approx \frac{\Gamma(-(\alpha-k))\Gamma(\alpha)}{\Gamma(1+\alpha)} z^{\frac{\alpha-k}{2}} + \frac{\Gamma(\alpha-k)\Gamma(k)}{\Gamma(1+k)} z^{-\frac{\alpha-k}{2}}, \tag{37}$$

where $z = \frac{\alpha\beta\sqrt{\Theta\mu_2+\Theta-1}}{(\zeta\beta+\Omega_1)\sqrt{\mu_1}}$.

Then, utilizing the asymptotic relation in (37) and substituting in (32), the asymptotic SOP is expressed as

$$P_o \approx 2\mathcal{P}\cdot\sum_{k=1}^{\beta}\mathcal{Q}_k\cdot\left[\frac{\Gamma(-(\alpha-k))\Gamma(\alpha)}{\Gamma(1+\alpha)\mu_1^{\frac{\alpha}{2}}}\cdot\left(\frac{\alpha\beta\sqrt{\Theta\mu_2+\Theta-1}}{(\zeta\beta+\Omega_1)}\right)^{\frac{\alpha-k}{2}}\right.$$
$$\left.+\frac{\Gamma(\alpha-k)\Gamma(k)}{\Gamma(1+k)\mu_1^{\frac{k}{2}}}\cdot\left(\frac{\alpha\beta\sqrt{\Theta\mu_2+\Theta-1}}{(\zeta\beta+\Omega_1)}\right)^{-\frac{\alpha-k}{2}}\right]. \tag{38}$$

From (38), we observe that the dominant term in the asymptotic expression for SOP corresponds to the lowest power of μ_1. Thus, it can be concluded that the asymptotic slope of the SOP curve is $\min\{\frac{\alpha}{2}, \frac{k}{2}\}$, where the smallest value of k corresponds to $k = 1$. Therefore, the results on the asymptotic slope of the SOP curve is the same for all scenarios of *A*, *B*, and *C*. Recall that the value of α is generally larger than 1 in practical channels. We can conclude that the slope of the asymptotic curve is always $\frac{1}{2}$ for eavesdropping of FSO communications, which is independent of the eavesdropping scenario and turbulence condition.

5. Numerical Results and Discussions

In this section, we evaluate the PLS performance of the FSO communications under different scenarios. For the SOP analysis, we set the secrecy rate threshold as 0.5 nats per second per unit bandwidth. The secrecy performance are evaluated under varying turbulence levels, i.e., weak turbulence ($\alpha = 8$, $\beta = 4$), moderate turbulence ($\alpha = 4.2$, $\beta = 3$), and strong turbulence ($\alpha = 2.296$, $\beta = 2$).

5.1 Numerical Results for Scenarios A and C

In Fig. 3, the ASC under the *Scenario A* is plotted as a function of SNR μ_1 of legitimate transmission for varying values of eavesdropper's SNR μ_2 under different turbulence conditions. The ASC performance improves as SNR μ_1 increases. It is also observed that as the value of μ_2 increases from 3 dB to 6 dB, the ASC performance deteriorates for a given turbulence regime. Further, the ASC performance becomes better as we move from strong to weak turbulence conditions.

Figures 4 and 5 show the SOP against the SNR μ_1 of legitimate transmission under varying correlation condition over strong and weak atmospheric conditions, respectively. The asymptotic curves also verify the theoretical analysis conducted in Subsection IV-C, where the slope of the asymptotic curve is $\frac{1}{2}$ for all cases.

The impact of correlation on the ASC under different turbulence conditions is demonstrated in Figs. 6 and 7. In Fig. 6, the ASC under different turbulence conditions is plotted as a function of the correlation coefficient ρ. In Fig. 7, the ASC penalty caused by correlation is plotted against the correlation parameter ρ, where the ASC penalty is defined as the difference between the ergodic capacity of legitimate transmission (i.e., the upper bound of ASC) and the ASC under the corresponding correlation level. It is seen that for a given turbulence scenario, as the value of ρ increases, the ASC becomes better, i.e., ASC value increases indicating that correlation helps in improving the ASC. However, this behavior is observed only up to a critical value of ρ beyond which the ASC starts to decrease on further increase of ρ. It is worthy mentioning that this non-monotonic impact of correlation on secrecy performance is not necessarily present in other fading channels,

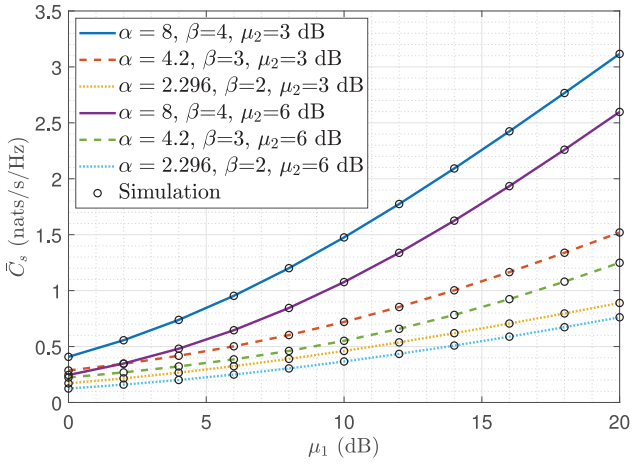


Fig. 3. ASC versus SNR μ_1 of legitimate transmission under different atmospheric conditions and varying values of μ_2, $\rho = 0.3$.

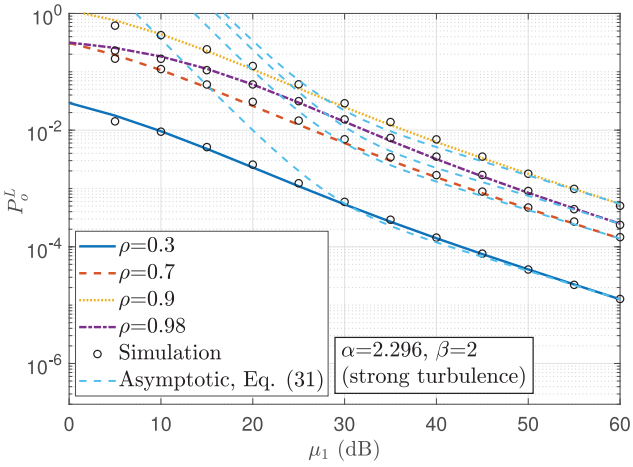


Fig. 4. SOP versus SNR μ_1 of legitimate transmission under strong atmospheric condition and varying correlation condition, $\mu_2 = 5$ dB.

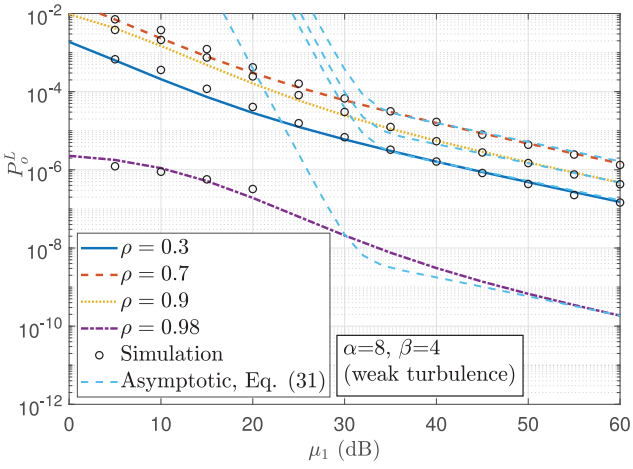


Fig. 5. SOP versus SNR μ_1 of legitimate transmission under weak atmospheric condition and varying correlation condition, $\mu_2 = 5$ dB.

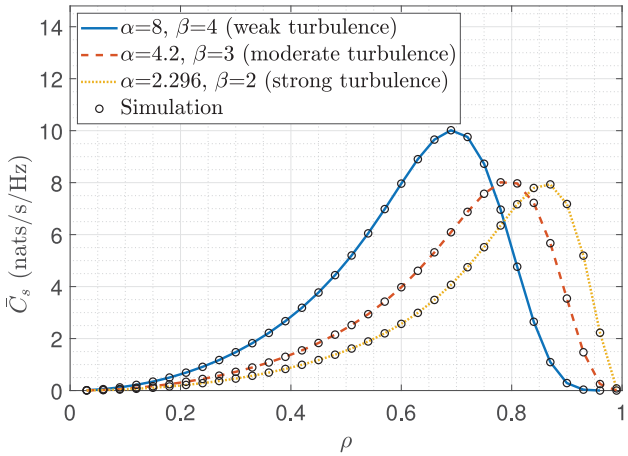


Fig. 6. ASC versus the correlation parameter ρ under different atmospheric conditions, $\mu_1 = 10$ dB and $\mu_2 = 3$ dB.

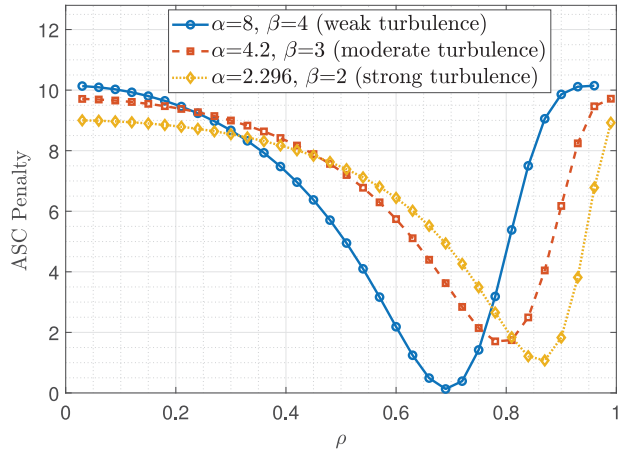


Fig. 7. ASC penalty versus the correlation parameter ρ under different atmospheric conditions, $\mu_1 = 10$ dB and $\mu_2 = 3$ dB.

e.g., α-μ channels[6, Fig. 2]. We also note that the ASC performance for weak turbulence scenario is better compared to the moderate and strong turbulence scenarios up to a certain value of ρ. An interesting feature is observed for high values of ρ where the opposite observation is made, i.e., ASC for strong turbulence is better than weak turbulence. This indicates that the deteriorating effect of the high correlation coefficient on secrecy capacity is more pronounced for weak turbulence compared to strong turbulence.

In Fig. 8, the SOP is plotted as a function of the correlation parameter ρ under different turbulence conditions. It is found that the analytical lower bound of SOP derived in (29) is very tight and matches the simulation well. It is interesting that the impact of correlation on the SOP in Fig. 8 is opposite compared to that on ASC as shown in 6. Overall, it can be concluded from Figs. 6 and 8 that the correlation between the legitimate and eavesdropper links of FSO communications exhibits opposites trends on the ASC and SOP of the FSO communication. More specifically, the channel correlation can possibly enhance the ASC performance while deteriorating the SOP performance at the same time, and vice versa. This opposite impact of channel correlation on ASC and SOP was also observed in [9]. Additionally, it can also be found from Figs. 6, 7 and 8 that the value of the critical ρ, i.e., the value beyond which the secrecy performance starts improving or deteriorating upon further increase of ρ, decreases as the system undergoes from strong turbulence to weak

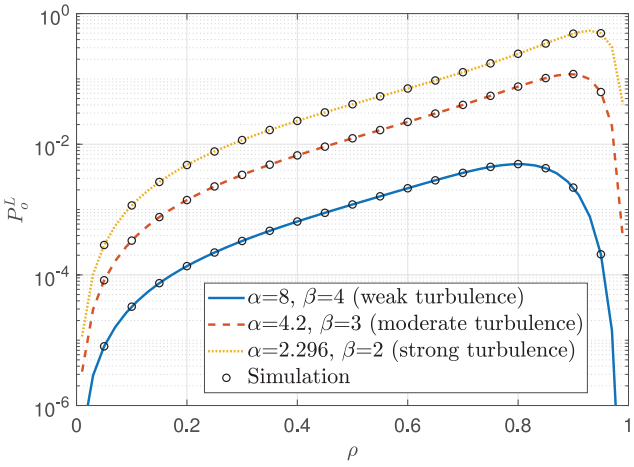


Fig. 8. SOP versus the correlation parameter ρ under different atmospheric conditions, $\mu_1 = 10$ dB and $\mu_2 = 5$ dB.

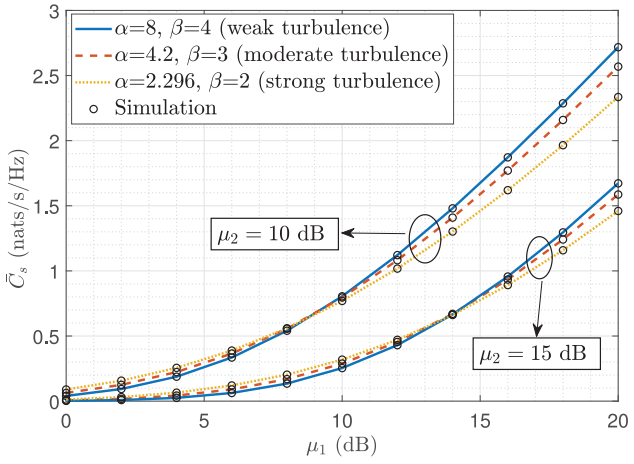


Fig. 9. ASC versus SNR μ_1 of legitimate transmission under different atmospheric conditions, $\mu_2 = 1$ dB.

turbulence. By observing Figs. 6 and 8 (note that the y axis is in log scale in Fig. 8), it can be observed that changing the correlation around the correlation values of 0 and 1 lead to less sharp changes in terms of secrecy performance. While the performance variation is more significant when the correlation factor changes around of aforementioned critical value. In other words, the correlation impacts the secrecy performance less significantly when the correlation is too small or too large.

5.2 Numerical Results for Scenario B

In Fig. 9, we compare the ASC performance under different turbulence conditions as a function of the SNR μ_1. The ASC increases as the SNR of the legitimate link improves. We observe that for a given atmospheric turbulence, the ASC deteriorates as the value of SNR μ_2 increases, which is also verified in Fig. 10. A unique feature about these curves is that for a given value of μ_2, the ASC improves as we move from strong to weak turbulence scenario only beyond a particular threshold μ_1 before which the converse is true (i.e., the ASC under strong turbulence is slightly better than under the weak turbulence). This reveals that under *Scenario B* when the SNR μ_1 of legitimate transmission is low, stronger turbulence plays a less deteriorating role compared to the weaker

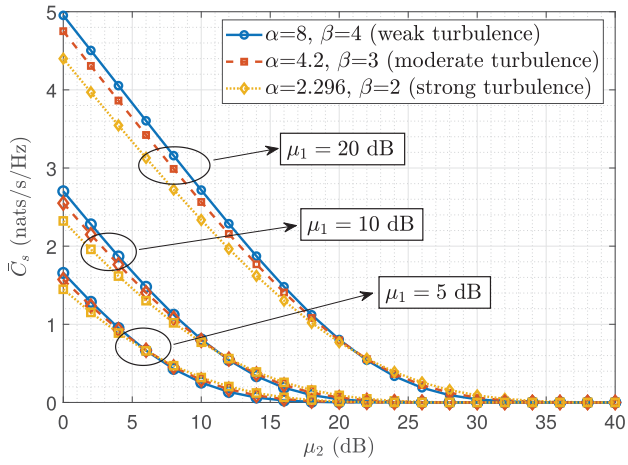


Fig. 10. ASC versus SNR μ_2 of legitimate transmission under different atmospheric conditions and μ_1.

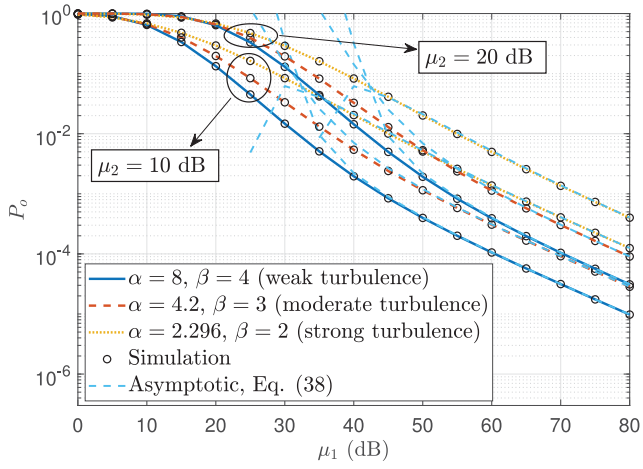


Fig. 11. SOP versus SNR μ_1 of legitimate transmission under different atmospheric conditions and varying values of μ_2.

turbulence due to higher instantaneous capacity. The similar intersection has also been observed in other research related to FSO communications, eg., [30, Fig. 7] and [36, Fig. 3].

In Fig. 11, the SOP under *Scenario B* is plotted as a function of SNR μ_1 for different turbulence scenarios. It is seen that the analytical results closely match with the simulation results, thereby establishing the validity of our analysis. It is observed that as we move from strong ($\alpha = 2.296$, $\beta = 2$) to weak ($\alpha = 8$, $\beta = 4$) atmospheric turbulence regime, the SOP performance improves. We also note that for a given turbulence scenario, the SOP performance becomes poor as the eavesdropper's SNR increases from 10 dB to 20 dB. This indicates that the closeness of the eavesdropper to the transmitter can significantly deteriorate the secrecy of the FSO system. The asymptotic SOP curves are also plotted under *Scenario B*. As a check, the SOP is 9.173×10^{-5} at 70 dB SNR and 2.838×10^{-5} at 80 dB SNR for the moderate turbulence condition ($\alpha = 4.2$ and $\beta = 3$) at 10 dB eavesdropper SNR. Therefore, the asymptotic slope for this case is $\log_{10}(9.173 \times 10^{-5}) - \log_{10}(2.838 \times 10^{-5}) = 0.5082 \approx 0.5$, which again verifies our conclusion that the slope for the asymptotic curve is always 0.5 regardless of the eavesdropping scenario. By comparing the results of *Scenario B* with those of *Scenario A*, it can be seen that when the eavesdropper is located close to the transmitter, the atmospheric turbulence condition imposes a less significant impact on the secrecy performance

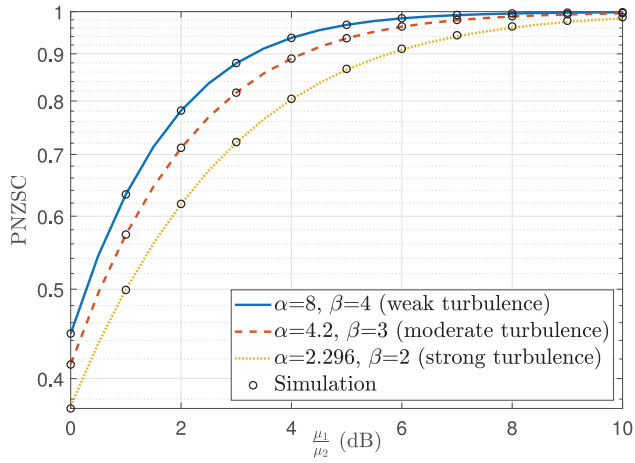


Fig. 12. PNZSC versus the ratio of the SNRs $\frac{\mu_2}{\mu_1}$ under different atmospheric conditions.

The PNZSC curves are plotted in Fig. 12 as a function of the ratio of legitimate and eavesdropping SNRs for different turbulence conditions. It is seen that the simulation results closely match with the analytical results. We can also observe that as the ratio of $\frac{\mu_1}{\mu_2}$ increases, the PNZSC performance improves because the link condition of the legitimate transmission gets better.

6. Conclusion

In this paper, we conducted a comprehensive study on the PLS for the FSO communications under three different scenarios. More specifically, the PLS was conducted for scenarios depending on the relative position of the eavesdropper, which leads to the different relationships between the main and wiretap links. Novel expressions for ASC and SOP were obtained, and asymptotic analysis on the SOP was also conducted. The results provide useful insights on FSO communication security under all scenarios of eavesdropping. The major findings of this are following: (1) The atmospheric turbulence condition demonstrates a less significant impact on the secrecy performance when the eavesdropper is located close to the transmitter than when it is close to the receiver; (2) The secrecy performance metrics demonstrates a non-monotonic behavior with the increase of correlation. This implies that the correlation can be potentially utilized to improve the secrecy performance for FSO communications; (3) The correlation exhibits opposite impacts on the ASC and SOP; (4) The critical value of correlation parameter (i.e., the value beyond which further increasing correlation reverses secrecy performance) increases as the atmospheric condition changes from weak to strong scenarios; (5) When the channel correlation parameter is around the critical value, the correlation plays a more significant impact on the secrecy performance; and (6) The asymptotic slope of the SOP is $\frac{1}{2}$ for all eavesdropping scenarios under practical FSO channels.

References

[1] 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.

[2] L. Kong, Y. Ai, L. Lei, G. Kaddoum, S. Chatzinotas, and B. Ottersten, "An overview of generic tools for information-theoretic secrecy performance analysis over wiretap fading channels," 2020. [Online]. Available: https://arXiv.org/abs/2009.05976

[3] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, USA, Jul. 2006, pp. 356–360.

[4] G. C. Alexandropoulos and K. P. Peppas, "Secrecy outage analysis over correlated composite Nakagami-*m*/Gamma fading channels," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 77–80, Jan. 2018.

[5] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[6] A. Mathur, Y. Ai, M. Cheffena, and G. Kaddoum, "Secrecy performance of correlated α-μ fading channels," *IEEE Commun. Lett.*, vol. 23, no. 8, pp. 1323–1327, Aug. 2019.

[7] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

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

[9] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over non-small-scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

[10] Y. Ai, M. Cheffena, T. Ohtsuki, and H. Zhuang, "Secrecy performance analysis of wireless sensor networks," *IEEE Sensors Lett.*, vol. 3, no. 5, pp. 1–4, May 2019.

[11] 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.

[12] 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.

[13] 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.

[14] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum secrecy throughput of MIMOME FSO communications with outage constraints," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3487–3497, May 2018.

[15] 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.

[16] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2017.

[17] 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.

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

[19] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. New York, NY, USA: Springer, 2009.

[20] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over α-μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[21] R. Priyadarshani, M. R. Bhatnagar, Z. Ghassemlooy, and S. Zvanovec, "Outage analysis of a SIMO FSO system over an arbitrarily correlated $\mathcal{M}$-distributed channel," *IEEE Photon. Technol. Lett.*, vol. 30, no. 2, pp. 141–144, Jan. 2018.

[22] A. Jurado-Navas, J. Garrido-Balsells, J. Paris, M. Castillo-Vazquez, and A. Puerta-Notario, "Further insights on Málaga distribution for atmospheric optical communications," in *Proc. IEEE Int. Workshop Opt. Wireless Commun.*, Pisa, Nov. 2012, pp. 1–3.

[23] A. Jurado-Navas, J. M. Garrido-Balsells, J. F. Paris, and A. Puerta-Notario, "A unifying statistical model for atmospheric optical scintillation," *Numer. Simulations Phys. Eng. Process.*, Rijeka, Croatia: InTech, Sep. 2011, pp. 181–206.

[24] N. D. Milosevic, M. I. Petkovic, and G. T. Djordjevic, "Average BER of SIM-DPSK FSO system with multiple receivers over $\mathcal{M}$-distributed atmospheric channel with pointing errors," *IEEE Photon. J.*, vol. 9, no. 4, Aug. 2017, Art. no. 6601210.

[25] H. Samimi and M. Uysal, "End-to-end performance of mixed RF/FSO transmission systems," *IEEE J. Opt. Commun. Netw.*, vol. 5, no. 11, pp. 1139–1144, Nov. 2013.

[26] J.-Y. Wang, C. Liu, J.-B. Wang, J. Dai, M. Lin, and M. Chen, "Secrecy outage probability analysis over Málaga-Málaga fading channels," in *Proc. IEEE Int. Conf. Commun.*, Kansas City, MO, USA, May 2018, pp. 1–6.

[27] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed Rician channels," *Electron. Lett.*, vol. 55, no. 13, pp. 765–767, Jun. 2019.

[28] L. Kong, Y. Ai, J. He, N. Rajatheva, and G. Kaddoum, "Intercept probability analysis over the cascaded Fisher-Snedecor $\mathcal{F}$ fading wiretap channels," in *Proc. IEEE Int. Symp. Wireless Commun. Syst.*, Oulu, Finland, Aug. 2019, pp. 672–676.

[29] A. Prudnikov, Y. Brychkov, and O. Marichev, *Integrals and Series. Volume 3: More Special Functions*. New York, NY, USA: Gordon and Breach Science Publishers, 1986.

[30] 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, p. 126193, Nov. 2020.

[31] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

[32] S. Choudhury and J. D. Gibson, "Information transmission over fading channels," in *Proc. IEEE Global Telecommun. Conf.*, Washington DC, USA, Dec. 2007, pp. 3316–3321.

[33] 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, Feb. 2019, Art. no. 7900814.

[34] D. S. Karas, A.-A. A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, "Physical layer security in the presence of interference," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.

[35] 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 and Algebraic Comput.*, Tokyo, Japan, Aug. 1990, pp. 212–224.

[36] H. Liang, C. Gao, Y. Li, M. Miao, and X. Li, "Analysis of selection combining scheme for hybrid FSO/RF transmission considering misalignment," *Opt. Commun.*, vol. 435, pp. 399–404, Nov. 2019.