Research Article | Vol. 27, No. 23 / 11 November 2019 / Optics Express 34211

Optics EXPRESS

Secure communication for FSO links in the presence of eavesdropper with generic location and orientation

RUBÉN BOLUDA-RUIZ,[1,*] ANTONIO GARCÍA-ZAMBRANA,[2] BEATRIZ CASTILLO-VÁZQUEZ,[2] AND KHALID QARAQE[1]

[1] *Dept. of Electrical and Computer Engineering, Texas A&M University at Qatar, Doha, Qatar*
[2] *Dept. of Communications Engineering, University of Málaga, Málaga, Spain*
[*] *ruben.boluda_ruiz@qatar.tamu.edu*

Abstract: When the beam waist at the receiver is significantly larger than the receiver size, free-space optical (FSO) links may be vulnerable to some optical tapping risks at the physical layer. In this paper, we conduct a new framework for the analysis of the secrecy performance in terms of the secrecy outage probability (SOP) of FSO systems affected by gamma-gamma (GG) turbulence-induced fading channels with pointing errors. As a key feature, we evaluate the SOP in the presence of an external eavesdropper with generic location and orientation. For that reason, a new misalignment error model is proposed to consider a non-orthogonal optical beam with respect to the photodetector plane at the eavesdropper's receiver, where the effective area is determined by a rotated ellipse. New approximate and asymptotic solutions at high signal-to-noise-ratio (SNR) for the secrecy performance are obtained in closed-form, which are verified by exact Monte Carlo simulations. By using the developed expressions, we analyze in greater detail some effects such as the SNR of the eavesdropper's channel, the normalized beamwidth at the receiver-side, and the location and orientation of the eavesdropper on the secrecy performance for different turbulence conditions.

1. Introduction

Currently, the global data traffic in wireless communication networks continue growing exponentially, mainly due to the increase in mobile broadband. In this way, security issues of wireless communication systems have attracted considerable attention in the last decade. Furthermore, it is expected that this great interest in physical layer security issues continues growing in the coming years with the emerging implementation of 5G networks and beyond [1]. A secure transmission in the presence of an external eavesdropper is a vital research problem in communication and information theory. In this scenario, the transmitter wants to send classified messages to the receiver and also wants to keep a hearer as ignorant of these messages as possible.

According to recent research on optical communications, it has been shown that optical networks are vulnerable to some types of attacks at the physical layer [2]. Even when fiber-optic transmission systems are able to offer large capacities over long distances, optical wired links can suffer from some simple eavesdropping attacks at the physical layer [3]. In relation to optical transmission in unguided media such as free-space optical (FSO) communication [4], and visible light communication (VLC) [5–7], they are not interception-free. It is generally accepted that FSO communication systems have attracted widespread interest for a number of years due to the remarkable variety of applications that they can offer by using a large capacity [8]. For this reason, there is growing interest in privacy and security issues of FSO communication systems in the presence of an external eavesdropper that can extract information from the legitimate transmission. Furthermore, FSO is a line-of-sight (LOS) technology in nature, providing not only immunity to RF interference, but also robustness to eavesdropping. However, some authors have

#375122 https://doi.org/10.1364/OE.27.034211
Journal © 2019 Received 13 Aug 2019; revised 13 Oct 2019; accepted 23 Oct 2019; published 7 Nov 2019

Optics EXPRESS

demonstrated that eavesdropping in the context of FSO systems may occur when a wiretapper is hidden in the top of the same building as the main receiver. This is mainly due to the fact that the beam waist at the receiver is significantly larger than the receiver size as a consequence of the spreading of the laser beam through atmosphere [9]. Thus, one potential eavesdropping will take place when the eavesdropper is located in the divergence region of the received optical beam. For long FSO distances, the eavesdropper also has a greater opportunity for eavesdropping by capturing radiated power. For all these motives, physical layer security in FSO systems is presently considered as an open, challenging area by the research community. Unlike the traditional encryption technologies in upper layer, no secret key is required in physical layer security, exploiting the characteristics of fading channels to guarantee perfect secrecy [10,11].

Traditionally, physical layer security has been considered as a problem of radio-frequency (RF) systems. A great deal of research has been reported over the last decade [12–16] (and references therein). In [12], security issues are studied over α-μ fading channels. The use of multiple-inputs/single-output (MISO) systems was considered in [13], and the use of single-input/multiple-output (SIMO) systems in [14]. Moreover, a comprehensive analysis of physical layer security was reported in [15] for multiple-inputs/multiple-outputs (MIMO) systems, and in [16] for cooperative systems.

Due to the fact that FSO technology is inherently much safer than RF technology, the state-of-the-art of physical layer security for FSO communication is still under developed [17–23]. In relation to passive eavesdropping, the secrecy outage probability (SOP) for FSO links in the presence of an external eavesdropper was analyzed over Málaga atmospheric turbulence channels without considering pointing error effects in [17,21]. In [20], the effect of channel imperfections on security issues for mixed RF/FSO relay networks is analyzed in detail. In [22], the SOP is evaluated for a mixed RF/FSO communication system based on decode-and-forward (DF) relaying. Regarding active eavesdropping scenarios, the average secrecy capacity (ASC) was studied for mixed RF/FSO relay networks in [18,19], where eavesdropping is only produced in the RF link. In [23], the ASC was considered over Málaga turbulence with zero boresight misalignment errors, not taking into consideration the eavesdropper's location on the pointing error model. In contrast to the aforementioned literature, the zero boresight pointing errors model previously assumed in the FSO wiretap channel proved to be insufficient due to the very highly directive nature of laser-based communication systems. It is crucial to consider a nonzero boresight pointing error model for the FSO wiretap channel to include the eavesdropper's location since it is logic to think that the eavesdropper is not in the LOS of the legitimate transmitter. Mathematically speaking, this translates into a nonzero boresight pointing error due to the fact that the eavesdropper is able to capture radiated power. To the best of our knowledge, the study of the secrecy performance of terrestrial FSO links assuming an external eavesdropper with generic location and orientation is still an open research problem.

In this paper, we conduct a careful investigation of the secrecy performance of terrestrial FSO links over gamma-gamma (GG) fading channels with misalignment errors, assuming an external eavesdropper with generic location and orientation to fill the gap in the current literature. We derive new approximate closed-form expressions for the SOP and the probability of strictly positive secrecy capacity (SPSC), which are verified by exact Monte Carlo simulations for moderate-to-strong turbulence conditions. We also develop new asymptotic solutions at high signal-to-noise-ratio (SNR) for the SOP and the probability of SPSC to get more remarks about the impact of some important system parameters such as the SNR of the eavesdropper's channel, the normalized beamwidth at the receiver-side, and the location and orientation of the eavesdropper on the secrecy performance. Due to the fact that the eavesdropper presents a generic position and orientation in this analysis, we also propose a new misalignment error model to take into consideration a non-orthogonal optical beam with respect to the photodetector plane at the eavesdropper's receiver, where the effective area is determined by a rotated ellipse. Thus, we

Optics EXPRESS

refine not only the current pointing error model, but also the well-established channel model over GG atmospheric turbulence to consider a much more real FSO scenario by including the aforementioned new key aspects, where some attacks at the physical layer can take place. Unlike the current literature [17,22,23], the importance of this study lies in the fact that considering an external eavesdropper with generic location and orientation as well as assuming two different pointing error distributions for the desired and wiretap FSO links due to the very highly directive nature of laser-based communication systems. In line with this, one of the most interesting conclusions is that the eavesdropper's location and its orientation plays quite an important role in secrecy performance.

The remainder of this paper is arranged as follows. In Sections 2 and 3, the problem definition and the FSO wiretap channel model are examined, respectively. The new misalignment error model that takes into consideration a non-orthogonal optical beam with respect to the photodetector plane at the eavesdropper's receiver is included in Appendix A. The SOP and the probability of SPSC are carefully analyzed in Section 4, and some numerical results and discussion are provided in Section 5. Finally, the paper is concluded in Section 6.

2. Problem definition

We assume a classic Wyner's wiretap channel [24], where two legitimate peers want to communicate (Alice and Bob) with each other in the presence of an external eavesdropper (Eve) with generic location and orientation, as shown in Fig. 1. When eavesdropping takes place, Eve is able to capture a portion of the power emitted by Alice since both Bob and Eve are located in the top of the same building, and the beamwidth at the receiver is large enough. We also consider that the legitimate peers and the eavesdropper are fixed devices, as usually assumed in the deployment of FSO links [25]. Hereinafter, the subscript m is used as follows: $m = B$ for Bob, and $m = E$ for Eve. For the sake of simplicity, let us assume that $d_B \simeq d_E$ (with d_m denoting the FSO link distance between Alice and the receiver m) due to the fact that the effective areas associated with each of the photodetectors are located in the same transverse plane of the incident wave, i.e., xy-plane. This assumption can be perfectly applied to this analysis since d_m is much bigger than the distance between Bob and Eve.

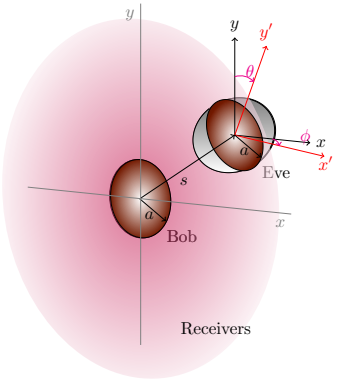


Fig. 1. Illustration of the geographical location of Bob and Eve, where the boresight displacement $s^2 = \mu_x^2 + \mu_y^2$ represents the eavesdropper's location in the xy-plane, and the angles θ and ϕ represent the orientation of the eavesdropper's receiver in x-axis and y-axis, respectively.

The major aspect of this study is twofold: a) we assume different fading distributions for the misalignment error at the receivers; b) we also assume that the optical beam is non-orthogonal with respect to the photodetector plane at Eve, i.e., the eavesdropper may present another

Optics EXPRESS

orientation that leads to a rotation in x-axis by an angle θ and/or in y-axis by an angle ϕ. In other words, the fraction of the power collected at Eve is not determined by the area of a circular receiver aperture, but also by the effective area that, in this case, is determined by the area of a rotated ellipse in xy-plane, as also shown in Fig. 1.

At the legitimate receiver Bob, we consider a zero boresight pointing error model, in which the legitimate transmitter is perfectly aligned with the main receiver and the optical beam is orthogonal with the photodetector plane, leading to a Rayleigh distributed pointing error. On the other hand, a nonzero boresight pointing error model is considered at Eve to include the eavesdropper's location, where the optical beam is non-orthogonal with respect to the photodetector plane. A useful way to include the eavesdropper's location is to assume a different fading distribution for the pointing error at Eve. The eavesdropper's location can be interpreted as an inherent boresight displacement, as defined in [26], since Alice is aligned with Bob. This leads to a lognormal-Rice distributed pointing error [27] at Eve. Moreover, we assume that the spacing s is larger than the atmospheric coherence length to consider uncorrelated FSO channels [28]. Since the atmospheric coherence length is on the order of centimeters, both receivers will be enough separated to consider uncorrelated fading.

3. System and channel models

Let us assume a generic intensity-modulation and direct-detection (IM/DD) FSO link using on-off keying (OOK) modulation, where the received electrical signal for the considered link is given by

$$y_m = h_m R x + z_m, \quad x \in \{0, 2P_t\}, \tag{1}$$

where R (A/W) is the detector responsivity, assumed hereinafter set to be the unity, x is the transmitted signal and the symbols are taken with the same probability from an OOK constellation such that $x \in \{0, 2P_t\}$ with P_t the average optical power, h_m denotes the unified fading channel coefficient, and z_m is additive white Gaussian noise (AWGN) with zero mean and variance $\sigma_n^2 = N_0/2$. In this case, the received electrical SNR for the considered FSO link is defined as in [29,30] as follows

$$\mathrm{SNR}(h_m) = \frac{2P_t^2 T_b}{\sigma_n^2} h_m^2 = 4\gamma_m h_m^2, \tag{2}$$

where T_b is the bit period, and γ_m is the transmit SNR in absence of fading, and $h_m = L_m \cdot h_a \cdot h_p$ with L_m being the atmospheric attenuation [31], h_a the atmospheric turbulence following the GG model [32], and h_p the pointing error [27,30,33]. Next, we examine the different pointing error models assumed here.

3.1. Pointing error modeling of Bob

At the legitimate receiver Bob, where the fraction of the collected power is determined by the detector area, i.e., by the area of a circle of radius a, the attenuation due to geometric spread and pointing errors can be directly approximated, as in [30, Eq. (9)], as follows

$$h_p^{\mathrm{Bob}}(r_B; z) \approx A_B \exp\left(\frac{-2r_B^2}{\omega_{z_{eqB}}^2}\right), \tag{3}$$

where r_B is the radial displacement at Bob, $A_B = [\mathrm{erf}(v_B)]^2$ is the fraction of the collected power at $r_B = 0$, $v_B = \sqrt{\pi}a/\sqrt{2}\omega_z$, and $\omega_{z_{eqB}}^2$ is the equivalent beamwidth. In this model, r_B is a Rayleigh distributed pointing error, where the same jitter variances ($\sigma_x = \sigma_y = \sigma_s$) and zero boresight displacement ($\mu_x = \mu_y = 0$) are considered. Note that x and y represent the horizontal

Optics EXPRESS

displacement and the elevation, respectively. Therefore, the probability density function (PDF) of the pointing error at Bob is expressed as in [30] as

$$f_{h_p}^{\text{Bob}}(h) = \frac{\varphi_B^2}{A_B^{\varphi_B^2}} h^{\varphi_B^2 - 1}, \quad 0 \leq h \leq A_B, \tag{4}$$

where $\varphi_B = \omega_{z_{eqB}}/2\sigma_s$.

3.2. Pointing error modeling of Eve

Unlike the previous pointing error model, where the optical beam is assumed to be orthogonal with respect to the photodetector plane and the fraction of the collected power is determined by the detector area, this assumption may not hold at the eavesdropper's receiver since Eve could be aligned with another transmitter and, hence, this one may present another position and orientation. Thus, the fraction of the power collected at Eve is determined by the area of a rotated ellipse, where one of the axis is a (the radius of the circular receiver aperture at Eve), and the other one is defined as $\rho = a \cos\phi \cdot \cos\theta$. Recently, a new statistical modeling for FSO fronthaul channels was proposed in [34], where the transceiver presents both random position and random orientation. Contrary to [34], the eavesdropper's position is considered to be fixed in this statistical model and, hence, the proposed statistical model for pointing errors reuses known expressions for the geometric losses that are modified when the fraction of the power collected at Eve is determined by the area of a rotated ellipse in the transverse plane of the incident wave. In Appendix A, the parameter ρ is derived in greater detail. Hereinafter, the parameter ρ is called rotation parameter and represents the eavesdropper's orientation. As also demonstrated in Appendix A, the attenuation due to geometric spread and pointing errors at the eavesdropper's receiver Eve can be approximated as follows

$$h_p^{\text{Eve}}(r_E; z) \approx A_0 \exp\left(\frac{-2r_E^2}{\omega_{z_{eqE}}^2}\right), \tag{5}$$

where r_E is the radial displacement at Eve, $A_0 = [\text{erf}(v_E)]^2$ is the fraction of the collected power at $r_E = 0$, $v_E = \sqrt{\pi}\sqrt{a^2 \cos\theta \cos\phi}/\sqrt{2}\omega_z$, and $\omega_{z_{eqE}}^2$ is the equivalent beamwidth. Notice that the area reduction by considering a rotated ellipse as an effective area instead of a circle is determined by the normalized rotation parameter as $1 - \rho/a$. Interestingly, from a physical layer security point of view, the worst case study is when $\rho/a = 1$ since both Bob and Eve present the same orientation and the optical beam is orthogonal with respect to the receiver plane in both photodetectors. However, when $\rho/a = 0$, Eve will not be able to capture radiated power at all. Another potential scenario would be when the eavesdropper is really close to Bob or is able to block the received optical beam in order to collect a larger amount of radiated power. This case would be represented when $s = 0$, as shown in Fig. 1. This scenario is considered as blocking case instead of eavesdropping one since the main receiver could notice that the received power is notably reduced and stop receiving.

It must be noted that the radiated power captured by Eve is determined by the effective area, which depends mainly on how apart the rotated ellipse is from the beamwidth center. For that reason, r_E follows the lognormal-Rice distribution [27], where the same jitter variances ($\sigma_x = \sigma_y = \sigma_s$) and a nonzero boresight displacement ($s^2 = \mu_x^2 + \mu_y^2$) are considered. This assumption has not been considered in any early paper. The PDF of the radial displacement r_E was obtained in [27, Eq. (4)], which appears quite cumbersome to use. Hence, we approximate accurately the lognormal-rice distribution by a modified Rayleigh distribution as presented in

Optics EXPRESS

[33, Eq. (11)] as follows

$$f_{r_E}(r) = \frac{r}{\sigma_s^2}\exp\left(-\frac{r^2+s^2}{2\sigma_s^2}\right) I_0\left(\frac{rs}{\sigma_s^2}\right) \simeq \frac{r}{\sigma_E^2}\exp\left(-\frac{r^2}{2\sigma_E^2}\right), \tag{6}$$

where $\sigma_E^2 = \left((3/2)\sigma_s^4 s^2 + \sigma_s^6\right)^{1/3}$ [33, Eq. (9)]. It is noteworthy to mention that this approximation is currently being used for the optics community to analyze the impact of nonzero boresight pointing errors on the performance of FSO communication systems [35,36]. This approximation allows us to derive an approximate closed-form solution for the unified fading channel. Thus, the PDF of the pointing error at Eve is given by

$$f_{h_p}^{\text{Eve}}(h) \simeq \frac{\varphi_E^2}{A_E^{\varphi_E^2}} h^{\varphi_E^2 - 1}, \quad 0 \le h \le A_E, \tag{7}$$

where $\varphi_E = \omega_{z_{eqE}}/2\sigma_E$, and A_E was also obtained in [33, Eq. (15)] as

$$A_E = A_0 e^{\left(4\sigma_s\left(\sqrt{s^2+\sigma_s^2}-\sigma_s\right)-2\sigma_s^2\right)/\omega_{z_{eqE}}^2}. \tag{8}$$

As can be observed from the expression of σ_E, this parameter considers a nonzero boresight displacement in addition to the random jitter variances in the wiretap FSO link. Finally, we summarize the generic pointing error parameters for Bob and Eve in Table 1, and the specific pointing error parameters in Table 2.

Table 1. Generic pointing error parameters for Bob and Eve.

Parameter	Symbol
Aperture receiver size	a
Normalized beamwidth	ω_z/a
Normalized jitter variance	σ_s/a
Normalized nonzero boresight error (Eavesdropper's location)	$(\mu_x/a, \mu_y/a)$
Normalized rotation parameter (Eavesdropper's orientation)	$\rho/a = \cos\theta\cos\phi$

Table 2. Specific pointing error parameters for Bob and Eve.

Parameter	Legitimate receiver Bob	Eavesdropper's receiver Eve
v_m	$v_B = \sqrt{\pi}a/\sqrt{2}\omega_z$	$v_E = \sqrt{\pi}\sqrt{a^2\cos\theta\cos\phi}/\sqrt{2}\omega_z$
$\omega_{z_{eqm}}^2$	$\omega_{z_{eqB}}^2 = \frac{\omega_z^2\sqrt{\pi}\,\text{erf}(v_B)}{2v_B\exp(-v_B^2)}$	$\omega_{z_{eqE}}^2 = \frac{\omega_z^2\sqrt{\pi}\,\text{erf}(v_E)}{2v_E\exp(-v_E^2)}$
σ_m^2	$\sigma_B^2 = \sigma_s^2$	$\sigma_E^2 = \left((3/2)\sigma_s^4 s^2 + \sigma_s^6\right)^{1/3}$
A_m	$A_B = [\text{erf}(v_B)]^2$	$A_E \approx [\text{erf}(v_E)]^2 \exp\left(\frac{4\sigma_s\left(\sqrt{s^2+\sigma_s^2}-\sigma_s\right)-2\sigma_s^2}{\omega_{z_{eqE}}^2}\right)$
φ_m	$\varphi_B = \omega_{z_{eqB}}/2\sigma_B$	$\varphi_E = \omega_{z_{eqE}}/2\sigma_E$

3.3. *Unified fading channel*

The PDF of the FSO communication link when GG turbulence of parameters α_m and β_m is considered [32] in the presence of pointing errors modeled by Rayleigh distributions is expressed

Optics EXPRESS

as in [33] as follows

$$f_{h_m}(h) = \frac{\varphi_m^2 h^{-1}}{\Gamma(\alpha_m)\Gamma(\beta_m)} G_{1,3}^{3,0}\left[\frac{\alpha_m\beta_m}{A_m L_m}h \,\middle|\, \begin{matrix} \varphi_m^2+1 \\ \varphi_m^2, \alpha_m, \beta_m \end{matrix}\right], \quad h \geq 0, \tag{9}$$

where $G_{p,q}^{m,n}[\cdot]$ is the Meijer's G-function [37, Eq. (8.2.1)]. The cumulative distribution function (CDF) is readily derived by using [37, Eq. (1.16.2.1)] as follows

$$F_{h_m}(h) = \frac{\varphi_m^2}{\Gamma(\alpha_m)\Gamma(\beta_m)} G_{2,4}^{3,1}\left[\frac{\alpha_m\beta_m}{A_m L_m}h \,\middle|\, \begin{matrix} 1, \varphi_m^2+1 \\ \varphi_m^2, \alpha_m, \beta_m, 0 \end{matrix}\right], \quad h \geq 0. \tag{10}$$

When plane wave propagation is considered, α_m and β_m are obtained as in [38]. Note that both the PDF in Eq. (9) and the CDF in Eq. (10) for the desired link represent exact solutions for the unified fading channel, whereas for the wiretap link represent approximate solutions, allowing us to study security issues in FSO communication systems.

4. Secrecy outage probability (SOP) analysis

In this section, the SOP and the probability of SPSC of FSO systems in the presence of an external eavesdropper with generic location and orientation are analyzed. It should be noted that both the SOP and the probability of SPSC are performance metrics to study physical layer security of passive eavesdropping FSO scenarios since the channel state information (CSI) of the eavesdropper's channel is not known at the transmitter-side. Hence, perfect secrecy cannot be achieved. We only assume the knowledge of the CSI at the receiver-side. In this situation, the SOP becomes important and significant as it gives a probabilistic measure of how the instantaneous secrecy capacity is below a given expected secrecy rate. The secrecy capacity C_s is defined as the maximum achievable secrecy rate, and is computed as in [10] as follows

$$C_s = [C_B - C_E]^+, \tag{11}$$

where $[x]^+ = \max(x, 0)$, C_B is the instantaneous capacity of the legitimate transmission (Alice-Bob), and C_E is the instantaneous capacity of the wiretap channel (Alice-Eve). In general, C_m is defined as $C_m = B\log_2(1 + 4\gamma_m h_m^2)$, where B is the channel bandwidth. Note that the capacity for terrestrial FSO links based on IM/DD systems is a lower bound [39]. Due to the fact that both scintillation and dynamic misalignment lead to a slow fading, the SOP of FSO links is adopted as a more suitable performance metric than the average secrecy capacity. Thus, the SOP is defined as the outage probability of the secrecy capacity that is given by

$$P_{\text{out}}(R_s) := \Pr\left[C_s < R_s\right], \tag{12}$$

where R_s is defined as the expected secrecy rate and, hence, if $R_s > C_s$, information theoretic security may be compromised. As the transmitter has no info about the CSI at Eve, this one will transmit information at a constant rate of R_s. From Eq. (11), we can compute the SOP as follows

$$P_{\text{out}}(R_s) := \Pr\left[\log_2\left(\frac{1+4\gamma_B h_B^2}{1+4\gamma_E h_E^2}\right) < R_s\right] = \int_0^\infty F_{h_B}\left(\sqrt{\frac{2^{R_s}(1+4\gamma_E h^2)-1}{4\gamma_B}}\right) f_{h_E}(h)dh. \tag{13}$$

The probability of SPSC is defined as

$$\Pr\left[C_s > 0\right] = 1 - \Pr\left[C_s < R_s\right]|_{R_s=0}. \tag{14}$$

To the best of our knowledge, the integral in Eq. (13) cannot be expressed in closed-form and, hence, we have to invoke another kind of approximation. To deal with this, both a lower bound

Optics EXPRESS

(LB) and an asymptotic solution at high SNR are derived, which will be validated by exact Monte Carlo simulations in the next section. Thus, a lower bound for the SOP can be derived as

$$P_{\text{out}}^{\text{LB}}(R_s) \simeq \int_0^{\infty} F_{h_B}\left(2^{R_s/2}\left(\frac{\gamma_E}{\gamma_B}\right)^{1/2} h\right) f_{h_E}(h)dh. \tag{15}$$

Substituting Eqs. (9) and (10) into Eq. (15), we can express the above integral in terms of the Meijer's G-function with the help of [37, Eq. (2.24.1.1)]. Therefore, a lower bound for the SOP can be expressed as follows

$$\begin{aligned} P_{\text{out}}^{\text{LB}}(R_s) \simeq & \frac{\varphi_B^2\varphi_E^2}{\Gamma(\alpha_B)\Gamma(\beta_B)\Gamma(\alpha_E)\Gamma(\beta_E)} \\ & \times G_{5,5}^{4,3}\left[\frac{\alpha_E\beta_E A_B L_B}{\alpha_B\beta_B A_E L_E} 2^{-\frac{R_s}{2}}\left(\frac{\gamma_B}{\gamma_E}\right)^{\frac{1}{2}} \middle| \begin{matrix} 1-\varphi_B^2, 1-\alpha_B, 1-\beta_B, 1, 1+\varphi_E^2 \\ \varphi_E^2, \alpha_E, \beta_E, 0, -\varphi_B^2 \end{matrix}\right]. \end{aligned} \tag{16}$$

At the same time, a lower bound for the probability of SPSC can be easily computed as

$$\Pr^{\text{LB}}[C_s{>}0] \simeq 1 - P_{\text{out}}^{\text{LB}}(R_s)\big|_{R_s=0}. \tag{17}$$

4.1. Asymptotic secrecy outage probability analysis

In order to get more remarks, an asymptotic solution for the SOP can be easily obtained at high SNR. To do that, the CDF of h_B is approximated by a single polynomial term as $F_{h_B}(h) \doteq \frac{a_B}{b_B}h^{b_B}$. In this way, different expressions for $F_{h_B}(h)$ are derived depending on the relation between φ_B^2 and $\min(\alpha_B, \beta_B)$. When plane wave propagation is assumed, the minimum value between α_B and β_B is equal to β_B [40]. Therefore, the CDF of h_B is approximated as in [33, Eq. (18)] as follows

$$F_{h_B}(h) \doteq \hat{F}_{h_B}(h) = \frac{a_B}{b_B}h^{b_B} = \begin{cases} \frac{\varphi_B^2(\alpha_B\beta_B)^{\beta_B}\Gamma(\alpha_B-\beta_B)h^{\beta_B}}{\beta_B(A_B L_B)^{\beta_B}\Gamma(\alpha_B)\Gamma(\beta_B)(\varphi_B^2-\beta_B)}, & \varphi_B^2{>}\beta_B \\ \frac{\varphi_B^2\Gamma(\alpha_B-\varphi_B^2)\Gamma(\beta_B-\varphi_B^2)h^{\varphi_B^2}}{\varphi_B^2(\alpha_B\beta_B)^{-\varphi_B^2}(A_0 L_B)^{\varphi_B^2}\Gamma(\alpha_B)\Gamma(\beta_B)}, & \varphi_B^2{<}\beta_B \end{cases} \tag{18}$$

Now, substituting Eq. (18) into Eq. (13) and applying some easy algebraic manipulations, we obtain the following integral for the asymptotic solution of the SOP as follows

$$P_{\text{out}}(R_s) \doteq \frac{a_B 2^{\frac{R_s b_B}{2}}}{b_B}\left(\frac{\gamma_B}{\gamma_E}\right)^{-\frac{b_B}{2}} \int_0^{\infty}\left(h^2 + \frac{1-2^{-R_s}}{4\gamma_E}\right)^{\frac{b_B}{2}} f_{h_E}(h)dh. \tag{19}$$

The above integral can be solved by making the change of variable of $t = h^2$ and, then, we can use [37, Eq. (2.24.2.4)] in order to express the above integral in terms of the Meijer's G-function, yielding

$$\begin{aligned} P_{\text{out}}(R_s) \doteq & \left(\frac{2^{-b_B-3}a_B(2^{R_s}-1)^{b_B/2}}{\pi b_B\Gamma(-b_B/2)}\right) \times \left(\frac{2^{\alpha_E+\beta_E}\varphi_E^2}{\Gamma(\alpha_E)\Gamma(\beta_E)}\right) \\ & \times G_{3,7}^{7,1}\left[\left(\frac{\alpha_E\beta_E}{A_E L_E}\right)^2 \frac{(1-2^{-R_s})}{64\gamma_E} \middle| \begin{matrix} 1, \frac{1+\varphi_E^2}{2}, \frac{2+\varphi_E^2}{2} \\ -\frac{b_B}{2}, \frac{\varphi_E^2}{2}, \frac{1+\varphi_E^2}{2}, \frac{\alpha_E}{2}, \frac{1+\alpha_E}{2}, \frac{\beta_E}{2}, \frac{1+\beta_E}{2} \end{matrix}\right] \times \gamma_B^{-b_B/2}. \end{aligned} \tag{20}$$

It can be deduced from Eq. (20) that the asymptotic closed-form solution of the SOP at high SNR behaves asymptotically as $P_{\text{out}}(R_s) \doteq (S_c \cdot \gamma_B)^{-S_d}$, where S_d and S_c denote the secrecy diversity

Optics EXPRESS

order and the secrecy gain, respectively. On the one hand, S_d determines the slope of the SOP versus SNR curve, at high SNR, in a log-log scale. On the other hand, S_c determines the shift of the curve in SNR in decibels, as defined for bit error rate (BER) performance in [41]. As can be also observed, the secrecy diversity order depends completely on the main channel, i.e., the secrecy diversity order is determined by $S_d = \min(\beta_B, \varphi_B^2)$. On the contrary, the secrecy gain depends not only on the main channel, but also on the eavesdropper's channel.

At this point, it would be interesting to compare and contrast the asymptotic solution of the SOP obtained here with the asymptotic solution of the outage capacity with no eavesdropper in order to analyze the influence of some important system parameters such as the SNR of the eavesdropper's channel, the normalized beamwidth at the receiver-side, and the location and orientation of the eavesdropper on the secrecy gain. The asymptotic expression for the outage capacity with no eavesdropper was derived in [42, Eq. (7)] as

$$P_{\text{out}}^{\text{no Eve}}(R_s) \doteq (O_c \cdot \gamma_B)^{-O_d} = \left[\left(\frac{a_B (2^{R_s} - 1)^{b_B/2}}{b_B 2^{b_B}} \right)^{-2/b_B} \cdot \gamma_B \right]^{-b_B/2}, \tag{21}$$

where O_c and O_d denote the coding gain and the outage diversity, respectively. The parameters a_B and b_B were obtained in Eq. (18).

5. Numerical results and discussion

Some numerical results are presented in this Section for the secrecy outage performance under clear visibility conditions when a value of the expected secrecy rate of $R_s = 0.5$ bit/channel use is considered. The FSO system setup considered here, which is used in most practical terrestrial FSO links [25], is summarized in Table 3. In addition, both the SOP and the probability of SPSC are evaluated for different severity of pointing errors. Note that while the SOP gives information of how the instantaneous secrecy capacity is below a given expected secrecy rate, the probability of SPSC gives information of the probability of existence of a safe communication.

Table 3. FSO system parameters.

Parameter	Symbol	Value
FSO link distance	d_m	3 km
Wavelength	λ	1550 nm
Clear visibility	V	16 km
Refractive index structure parameter	C_n^2	$\{2, 8\} \times 10^{-14}\ m^{-2/3}$
Rytov variance	σ_R^2	3
Receiver aperture diameter	D_m	10 cm
Normalized beamwidth	ω_z/a	{8,10}
Normalized standard deviation	σ_s/a	{2,4,6}
Eavesdropper's location	$(\mu_x/a, \mu_y/a)$	{(1,1),(4,1),(6,3)}
Eavesdropper's orientation	ρ/a	{0.4,0.6,0.7,0.8,1}
Expected secrecy rate	R_s	0.5 bits/channel use

In Fig. 2, the approximate SOP derived in Eq. (16) and the corresponding asymptotic solution derived in Eq. (20) are plotted as a function of γ_B, i.e. the SNR of the main channel, for different eavesdropper's locations of $(\mu_x/a, \mu_y/a) = \{(1, 1), (4, 1), (6, 3)\}$ and different eavesdropper's orientation of $\rho/a = \{0.4, 0.7, 1\}$ in order to see how these parameters impact on the SOP. As can be observed, the approximation based on a lower-bound presents a good agreement for the considered FSO scenarios in relation to the exact Monte Carlo simulation results. At the same

Optics EXPRESS

time, the asymptotic results also presents an excellent agreement at high SNR. As a benchmark, the results corresponding to the outage capacity performance with no eavesdropper are also included. It should be highlighted that the secrecy diversity order is fully dependent on the main channel, i.e., $S_d = b_B = \min(\beta_B, \varphi_B^2)$. In other words, all curves present the same slope, i.e. b_B, but different shifts or SNR gap because of the normalized rotation parameter ρ/a. The impact of the eavesdropper's channel on secure transmission for FSO systems is only reflected on the secrecy gain. As expected, the SOP is strongly dependent on the normalized rotation parameter. Interestingly, the maximum SOP is achieved when the normalized rotation parameter is set to $\rho/a = 1$, as commented in Section 3. Additionally, as ρ/a approaches zero, the SOP decreases, obtaining a performance very close to the outage capacity with no eavesdropper. In other words, the capacity of capturing radiated power by Eve decreases considerably. It is also observed that the secrecy outage is less likely at high SNR when $\gamma_B > \gamma_E$. In this SNR range, the secure communication is mainly dominated by the main channel. It is also confirmed that when the eavesdropper is nearby the legitimate receiver, the secrecy outage is more likely to happen regardless of the severity of pointing errors.

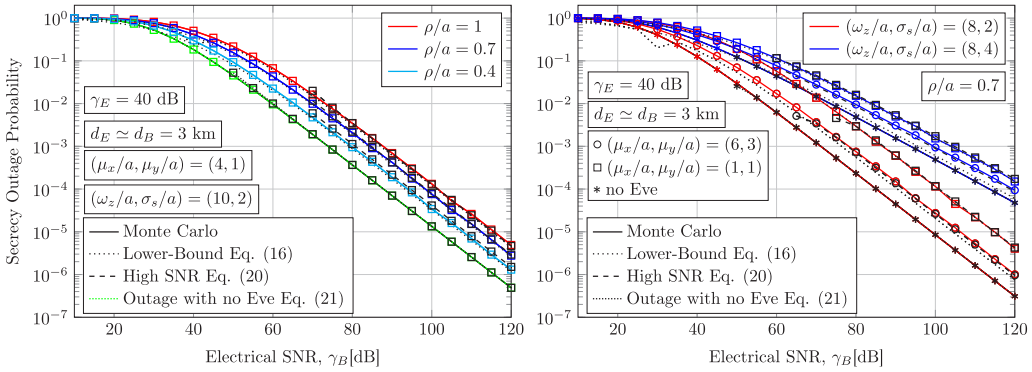


Fig. 2. Secrecy outage probability, $P_{\text{out}}(R_s)$, as a function of γ_B for different severity of pointing errors and different values of γ_E when an expected secrecy rate of $R_s = 0.5$ bits/channel use and a value of $C_n^2 = 2 \times 10^{-14}\ m^{-2/3}$ are considered.

In Fig. 3, the probability of SPSC obtained in Eq. (14) is plotted for the same set of parameters considered in Fig. 2. The same conclusions can be drawn from these results with regard to the eavesdropper's channel. At this point, we have to highlight that the lower bound derived

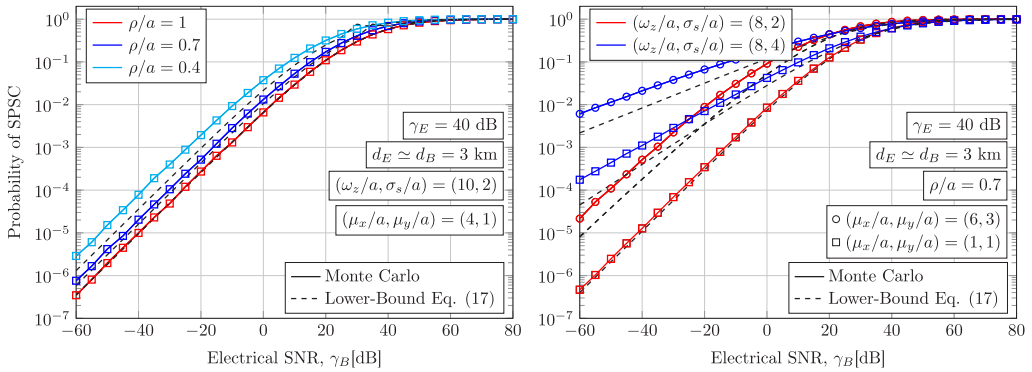


Fig. 3. Probability of SPSC, $\Pr[C_s > 0]$, as a function of γ_B for different severity of pointing errors and different values of γ_E when a value of $C_n^2 = 2 \times 10^{-14}\ m^{-2/3}$ is considered.

Optics EXPRESS

in this section represents a very accurate approximation in the analysis of secrecy issues of FSO communication systems. What we observe in this figure is the probability of existence of a safe communication, i.e., the probability of $C_s>0$. Obviously, as the SNR of the main channel increases, the probability of SPSC gets close to 1, indicating that the probability of a safe communication is every time more likely. Contrary to Fig. 2, as ρ/a approaches zero, the probability of SPSC increases and, hence, improving the probability of a safe communication.

5.1. Miscellaneous

For a better understanding of the impact of the eavesdropper's channel conditions on the SOP from moderate to strong turbulence conditions, we can quantify the SNR gap or loss between the outage capacity with no eavesdropper and the SOP with eavesdropper as follows

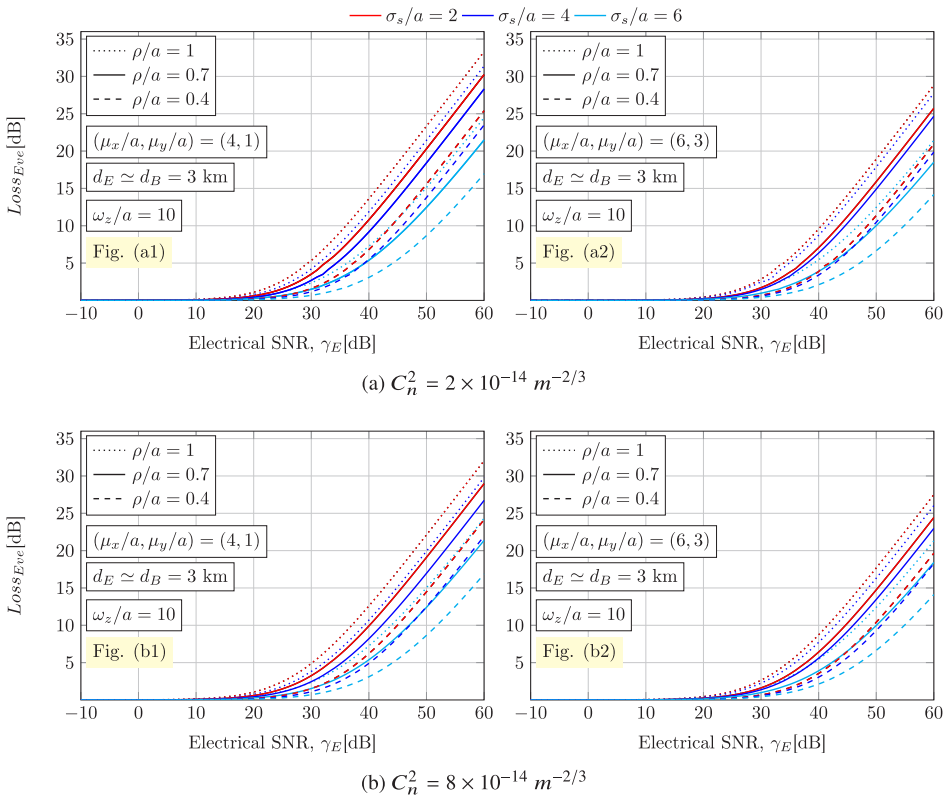
$$\begin{aligned} Loss_{\text{Eve}}[dB] &\triangleq 10\log_{10}\left[\frac{O_c}{S_c}\right] = \frac{20}{b_B} \\ &\times\log_{10}\left[\frac{2^{\alpha_E+\beta_E}\varphi_E^2}{8\pi\Gamma(\alpha_E)\Gamma(\beta_E)}G_{3,7}^{7,1}\left[\left(\frac{\alpha_E\beta_E}{A_E L_E}\right)^2\frac{(1-2^{-R_s})}{64\gamma_E}\,\middle|\,\begin{matrix}1, \frac{1+\varphi_E^2}{2}, \frac{2+\varphi_E^2}{2} \\ -\frac{b_B}{2}, \frac{\varphi_E^2}{2}, \frac{1+\varphi_E^2}{2}, \frac{\alpha_E}{2}, \frac{1+\alpha_E}{2}, \frac{\beta_E}{2}, \frac{1+\beta_E}{2}\end{matrix}\right]\right]. \end{aligned} \tag{22}$$

In Fig. 4, $Loss_{\text{Eve}}$[dB] is depicted as a function of γ_E for different eavesdropper's location of $(\mu_x/a, \mu_y/a) = \{(4,1),(6,3)\}$ and different eavesdropper's orientation of $\rho/a = \{0.4, 0.7, 1\}$. A normalized beamwidth value of $\omega_z/a = 10$ is assumed when different normalized jitter variances of $\sigma_s/a = \{2,4,6\}$ are considered. It can be observed that this loss increases with increasing γ_E. On the one hand, this growth presents an interesting behavior since for small values of γ_E we can confirm that the secure communication is not compromised at all since the performance is very close to the outage capacity with no eavesdropper regardless of the channel conditions. On the other hand, when γ_E takes larger values than 30 dB approximately, the SNR gap or loss notably increases with increasing γ_E. More importantly, we can see that for larger amounts of misalignment, i.e. for a normalized jitter variance of $\sigma_s/a = 6$, the SNR gap or loss is reduced, not allowing the eavesdropper to capture more power. Note that this loss is mitigated even more when the eavesdropper is located a little bit further away from the center of the beamwidth, as observed in Figs. 4(a2) and 4(b2).

In Fig. 5, $Loss_{\text{Eve}}$[dB] is depicted as a function of the normalized beamwidth ω_z/a for the same set of parameters assumed in the previous figure. As can be observed, the impact of eavesdropper's location and its orientation is really relevant, mainly when a larger value of γ_E is used, i.e., $\gamma_E = 40$ dB. Additionally, we can see that there is a maximum value of $Loss_{\text{Eve}}$[dB], in which the secure transmission between Alice and Bob can be truly compromised. As a general point of view, we can say that for small values of γ_E, the secure transmission between Alice and Bob is not compromised. This loss may be reduced when the normalized beamwidth is wider since it is possible to reduce the power incident on a fixed-size receiver increasing the beamwidth. Additionally, we can also see in this figure that the normalized beamwidth value that gets the maximum value of $Loss_{\text{Eve}}$[dB] depends on neither the rotation parameter ρ/a nor the value of γ_E. This is an interesting point since this maximum value represents the maximum loss from the secrecy performance point of view.

In Fig. 6, $Loss_{\text{Eve}}$[dB] is depicted as a function of the normalized horizontal displacement of the eavesdropper μ_x/a when the normalized vertical displacement is set to $\mu_y/a = 2$. In Figs. 6(a1) and 6(b1), $Loss_{\text{Eve}}$[dB] is plotted for different eavesdropper's orientation of $\rho/a = \{0.4, 0.6, 0.8\}$ when $\gamma_E = 60$ dB. In Figs. 6(a2) and 6(b2), $Loss_{\text{Eve}}$[dB] is plotted for different values of γ_E. Finally, in Figs. 6(a3) and 6(b3), $Loss_{\text{Eve}}$[dB] is plotted for different severity of pointing errors of $\sigma_s/a = \{2,4,6\}$. As we can observe from Fig. 6, both the location and the orientation of the eavesdropper play a fundamental role in the SOP performance of FSO communication systems. On the one hand, it is evident that in Figs. 6(a1), 6(b1), 6(a2) and 6(b2) the larger normalized

Optics EXPRESS



(a) $C_n^2 = 2 \times 10^{-14}\ m^{-2/3}$

(b) $C_n^2 = 8 \times 10^{-14}\ m^{-2/3}$

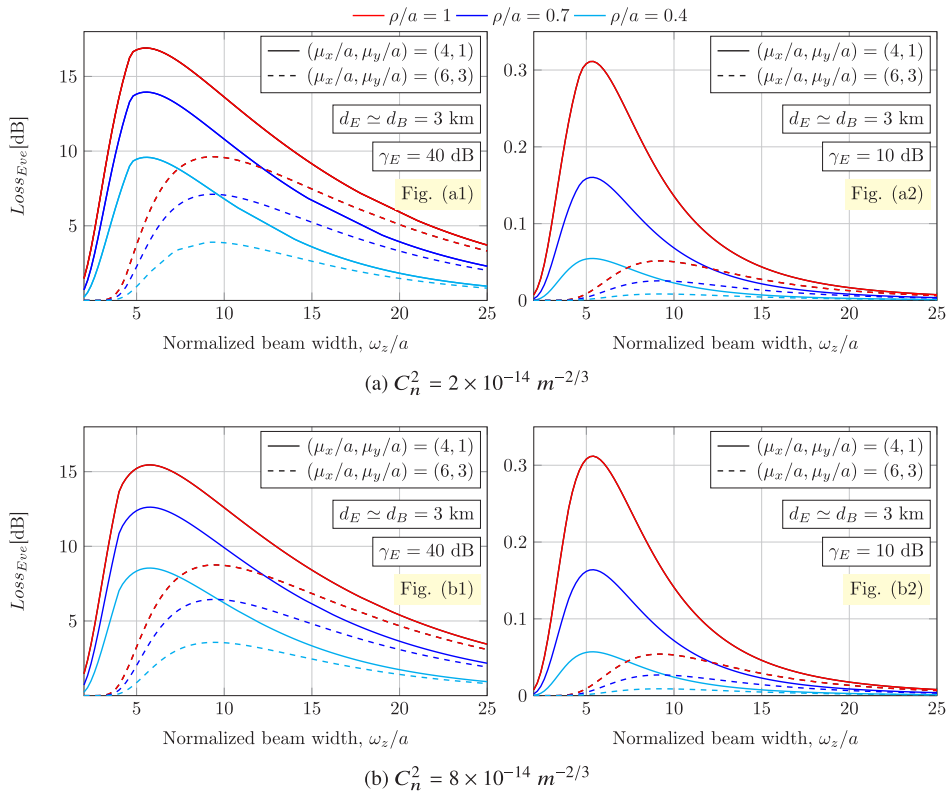
Fig. 4. Loss, $Loss_{\text{Eve}}$[dB], for (a) moderate, and (b) strong turbulence conditions as a function of γ_E when an expected secrecy rate of $R_s = 0.5$ bits/channel use and different eavesdropper's locations and different severity of pointing errors are assumed.

rotation parameter as well as the larger value of γ_E, the closer to the outage capacity with no eavesdropper when pointing errors are not significant. On the other hand, when pointing errors become significant, for instance in Figs. 6(a3) and 6(b3) for $\sigma_s/a = 6$, this can result in improving the SOP performance, permitting the eavesdropper to recollect less radiated power.

As we said in Section 2, we have considered in this paper that both the legitimate receiver Bob and the eavesdropper's receiver Eve are located in the top of the same building. For that reason, only small variations along the z-axis could take place in a real FSO scenario. On the one hand, the corresponding parameters of atmospheric turbulence, i.e. α_m and β_m, take the same value approximately for small variations over FSO distances when this one is on the order of a few kilometers [40]. On the other hand, according to the expression of the beam waist of a Gaussian beam propagating in atmospheric turbulence [43], the beamwidth also take the same value approximately for small variations over long distances. This comments have been confirmed by Monte Carlo simulations. Hence, the same outcomes are derived for small variations of the eavesdropper's location along the z-axis.

In the light of these results, we can observe in Figs. 4, 5 and 6 how secrecy performance depends strongly on the location and the orientation of the eavesdropper. From the SOP performance point of view, the worst FSO scenario and, at the same time, the FSO scenario that is less likely to happen is when the normalized rotation parameters is set to $\rho/a = 1$, i.e., when the optical beamwidth is also orthogonal with respect to the photodetector plane at Eve. In this case, the SOP performance decreases considerably since Eve is able to capture more radiated power

Optics EXPRESS



(a) $C_n^2 = 2 \times 10^{-14}\ m^{-2/3}$

(b) $C_n^2 = 8 \times 10^{-14}\ m^{-2/3}$

Fig. 5. Loss, $Loss_{\text{Eve}}$[dB], for (a) moderate, and (b) strong turbulence conditions as a function of γ_E when an expected secrecy rate of $R_s = 0.5$ bits/channel use and a value of the normalized jitter variance of $\sigma_s/a = 2$ are assumed.

in comparison with other FSO scenarios such as $\rho/a = \{0.4, 0.7\}$, where the optical beam is non-orthogonal with respect to the photodetector plane.

Last but not least, the effect of different turbulence conditions, i.e. from moderate to strong, on $Loss_{\text{Eve}}$[dB] has also been studied. As we can observe in Figs. 4, 5 and 6, it can be concluded that in general strong turbulence channels present a greater robustness to eavesdropping than moderate turbulence channels. Furthermore, from the viewpoint of the normalized beamwidth at the receiver-side, we can quantify from Fig. (5) the impact of the strength of turbulence when $\gamma_E = 40$ dB by obtaining values of $Loss_{\text{Eve}} = \{1.5, 1.35, 1.04\}$ dB for different eavesdropper's orientation of $\rho/a = \{1, 0.7, 0.4\}$ when the eavesdropper's location is set to $(\mu_x/a, \mu_y/a) = (4, 1)$, and values of $Loss_{\text{Eve}} = \{0.87, 0.66, 0.34\}$ dB for different eavesdropper's orientation of $\rho/a = \{1, 0.7, 0.4\}$ when the eavesdropper's location is set to $(\mu_x/a, \mu_y/a) = (6, 3)$. Thus, we can conclude that the impact of the strength of turbulence gradually decreases as the eavesdropper gets further away from the beam center. At the same time, the eavesdropper's capacity to capture more radiated power also decreases with increasing the strength of turbulence. On the other hand, when the quality of the eavesdropper's channel is low, for instance when $\gamma_E = 10$ dB, the impact of the strength of turbulence is not significant since the secrecy performance is really close to the outage performance with no eavesdropper regardless of the turbulence conditions.

Optics EXPRESS

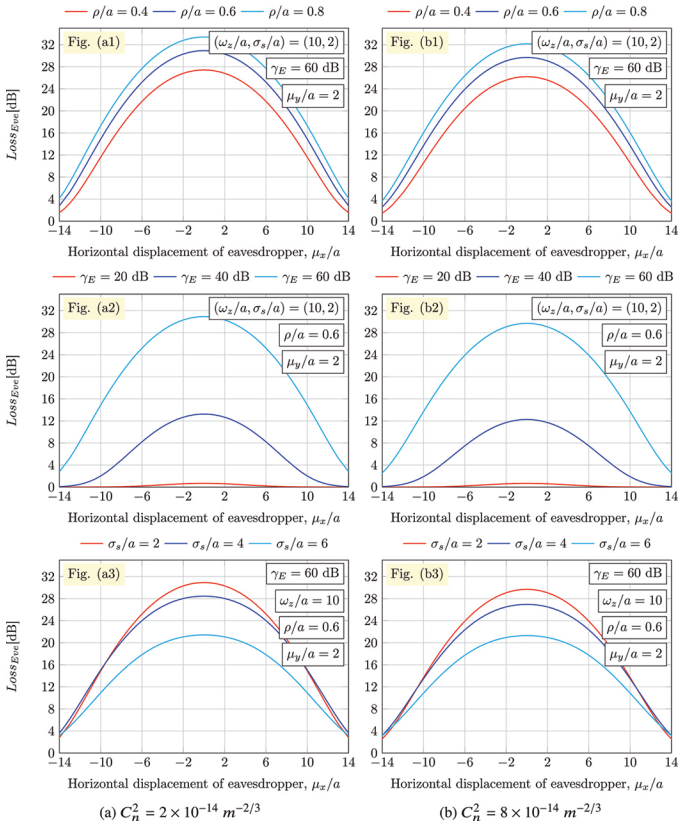


Fig. 6. Loss, $Loss_{\text{Eve}}$[dB], for (a) moderate, and (b) strong turbulence conditions as a function of the normalized horizontal displacement of the eavesdropper μ_x/a when an expected secrecy rate of $R_s = 0.5$ bits/channel use is assumed and the normalized vertical displacement is set to $\mu_y/a = 2$.

6. Concluding remarks

This paper carefully investigates the secrecy performance over GG fading channels with pointing errors in the presence of an external eavesdropper with generic location and orientation. New bounds for the SOP and the probability of SPSC have been obtained, which have been verified by exact Monte Carlo simulations for moderate-to-strong turbulence conditions.

On the one hand, our findings suggest that adding the eavesdropper's location to the wiretap FSO channel model along with the orientation represents a step forward in physical layer security for FSO communication. The secrecy performance in FSO systems is fully dependent not only on the eavesdropper's location and its orientation, but also on the beam footprint at the receiver-side, which is non-orthogonal with respect to the photodetector plane at Eve. The results presented here conclude that the secrecy performance is strongly dependent on the location and the orientation of the eavesdropper, resulting in a less secure communication between peers as a consequence of Eve. In fact, a greater normalized beamwidth as well as larger amounts of misalignment could increase the achievable secrecy rate, permitting the eavesdropper to recollect less radiated power and, hence, making the communication robuster. In short, the secrecy performance for terrestrial FSO links results in being a sophisticated balance of the normalized beamwidth, the eavesdropper's location and its orientation, as well as how significant pointing errors are at the receiver-side.

Optics EXPRESS

On the other hand, the robustness of FSO communication to some optical tapping risks has been confirmed since the secrecy performance is quite close to the performance with no observer for small values of the SNR at Eve or when the observer is not located near Bob. Moreover, from the behavior of the SOP at high SNR, we conclude that the secrecy diversity order does not depend on the eavesdropper channel, being completely dependent on the main channel. Nevertheless, the eavesdropper channel presents a remarkable impact on the secrecy gain.

Finally, the secrecy performance of FSO communication could be enhanced via MIMO schemes to significantly mitigate the effect of fading in FSO channels by creating spatial diversity. This finding is promising and should be also explored in drone-based FSO communication to be able to study how larger amounts of misalignment impact on the performance of this upcoming systems, where the optical beam is non-orthogonal with respect to the photodetector plane.

Appendix A

As a first step, let us assume that the effective area in the transverse plane of the incident wave is an ellipse, where the lengths of the semi-axes are a and b along the x-axis and y-axis, respectively. Thus, the fraction of the collected power at the eavesdropper's receiver can be expressed as

$$h_p^{Eve_x}(r;z) = \int_{-a}^{a} \int_{\frac{-b}{a}\sqrt{a^2-x^2}}^{\frac{b}{a}\sqrt{a^2-x^2}} \frac{2}{\pi\omega_z^2} \exp\left(-2\frac{(x-r^2)+y^2}{\omega_z^2}\right) dydx. \tag{23}$$

From the above integral, we can observe that the resultant ellipse presents a major and minor axis of a and b, respectively. Due to the asymmetry nature of the problem, the loss factor due to pointing errors h_p^{Eve} is sensitive to the direction of integration. For this reason, the fraction of the collected power can also be calculated as

$$h_p^{Eve_y}(r;z) = \int_{-a}^{a} \int_{\frac{-b}{a}\sqrt{a^2-x^2}}^{\frac{b}{a}\sqrt{a^2-x^2}} \frac{2}{\pi\omega_z^2} \exp\left(-2\frac{x^2+(y-r^2)}{\omega_z^2}\right) dydx. \tag{24}$$

It is true that h_p^{Eve} should be evaluated in 3D dimensions, but for the sake of simplicity we can take the average result between the best and the worst cases, i.e., the average result between Eqs. (26) and (27) as follows

$$h_p^{\text{Eve}}(r;z) \approx \frac{1}{2} h_p^{Eve_x}(r;z) + \frac{1}{2} h_p^{Eve_y}(r;z). \tag{25}$$

The above integral can be approximated by using the same approach as in [30, appendix] as

$$h_p^{\text{Eve}}(r;z) \approx A_0 \exp\left(\frac{-2r^2}{\omega_{z_{eq}}^2}\right). \tag{26}$$

The accuracy of the above approximation will be checked at the end of this appendix.

As a second step, we assume that the eavesdropper's receiver is rotated by an angle θ in x-axis, and by an angle ϕ in the y-axis, as shown in Fig. 1. Now, we will demonstrate that the rotation of the eavesdropper's receiver in both axis results in an effective area that is equivalent to a rotated ellipse where one of the axis is a (the radius of the circular receiver aperture at Eve) and the other one is defined as $a\cos\phi \cdot \cos\theta$. In other words, in this second step we can see that the rotation of the eavesdropper's receiver reduces to the considered one in the first step with $b = a\cos\phi \cdot \cos\theta$.

Let us assume that the rotation is made first in the y-axis and, then, in the x-axis since this operation is not commutative. To do that, we have to apply rotation matrix to the rotated circular aperture (Eve) to compute the projected geometric figure in the xy-plane, which is a rotated ellipse. The following two basic rotation matrices rotate vectors with a general 3-D rotation

Optics EXPRESS

through counterclockwise angles θ and ϕ about the x-, y-axis, respectively. They are used here to produce the desired effect, i.e the rotated ellipse, and expressed as follows

$$R_x(\theta) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}, \qquad R_y(\phi) = \begin{bmatrix} \cos\phi & 0 & \sin\phi \\ 0 & 1 & 0 \\ -\sin\phi & 0 & \cos\phi \end{bmatrix}. \tag{27}$$

Using the sine and cosine functions, a parametric representation of the circle $x^2 + y^2 = a^2$ can be obtained as

$$[x, y, z]^\intercal = [a\cos u, a\sin u, 0]^\intercal, \qquad 0 \le u \le 2\pi. \tag{28}$$

Now, we apply the rotation matrices in Eq. (27) to the circular aperture by using its parametric equation as follows

$$R_x(\theta)\cdot R_y(\phi)\cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\phi & 0 & \sin\phi \\ 0 & 1 & 0 \\ -\sin\phi & 0 & \cos\phi \end{bmatrix} \cdot \begin{bmatrix} a\cos u \\ a\sin u \\ 0 \end{bmatrix}. \tag{29}$$

By solving the above product of matrices, we can obtain the following projected rotated ellipse in the xy-plane as follows

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a\cos u\cdot\cos\phi \\ a\cos\theta\cdot\sin u + a\cos u\cdot\sin\theta\cdot\sin\phi \\ 0 \end{bmatrix}. \tag{30}$$

By making some algebraic manipulations, we obtain the quadratic form of a rotated ellipse as

$$x^2\left(\sec^2\phi + \tan^2\theta\tan^2\phi\right) + y^2\left(\sec^2\theta\right) - xy\left(2\sec\theta\tan\theta\tan\phi\right) = a^2. \tag{31}$$

From the above equation, we can observe that the projected figure is a rotated ellipse due to the fact that the cross product is not equal to zero. Additionally, the quadratic form can be easily written in matrix notation, yielding

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \underbrace{\begin{bmatrix} \sec^2\phi + \tan^2\theta\tan^2\phi & \sec\theta\tan\theta\tan\phi \\ \sec\theta\tan\theta\tan\phi & \sec^2\theta \end{bmatrix}}_{M} \begin{bmatrix} x \\ y \end{bmatrix} = a^2, \tag{32}$$

where the matrix M is called the matrix of the quadratic form. For the sake of clarity, we can see in Fig. 1 that the original xy-coordinate system with origin O is moved to the uv-coordinate system with the same origin O, i.e., the projected figure is a rotated ellipse, where the coordinate axes are rotated. Note that as M is a symmetric matrix then M is orthogonally diagonalizable. In

Optics EXPRESS

this way, Eq. (32) can be expressed as

$$\begin{bmatrix} u & v \end{bmatrix} \cdot \underbrace{\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}}_{D} \cdot \begin{bmatrix} u \\ v \end{bmatrix} = 1, \tag{33}$$

where D is the diagonal matrix, and $\lambda_1 = a^2$ and $\lambda_2 = a^2 \cos^2\theta \cos^2\phi$ are the eigenvalues of the matrix M. Hence, the quadratic form of this new ellipse is given by

$$\frac{u^2}{a^2} + \frac{v^2}{a^2 \cos^2\theta \cos^2\phi} = 1. \tag{34}$$

We have demonstrated that the rotation of the eavesdropper's receiver by an angle ϕ in the y-axis and by an angle θ in x-axis results in an effective area that is equivalent to a rotated ellipse in the xy-plane, where the semi-axis length along the x-axis is a (the radius of the circular aperture at Eve), and the semi-axis length along the y-axis is defined as $\rho = a\cos\phi \cdot \cos\theta$. Therefore, the fraction of the collected power at the eavesdropper's receiver of radius a in the transverse plane of the incident wave can be expressed from Eq. (25) and substituting $b = \rho$ as

$$h_p^{\text{Eve}}(r;z) \approx \frac{1}{2} h_p^{Eve_x}(r;z)\Big|_{b=a\cos\phi\cdot\cos\theta} + \frac{1}{2} h_p^{Eve_y}(r;z)\Big|_{b=a\cos\phi\cdot\cos\theta}. \tag{35}$$

The above integral can be approximated in the same way as Eq. (26) as

$$h_p^{\text{Eve}}(r;z) \approx A_0 \exp\left(\frac{-2r^2}{\omega_{z_{eq}}^2}\right), \tag{36}$$

where $A_0 = [\text{erf}(v^2)]$ is the fraction of the collected power at $r = 0$, $v = \sqrt{\pi}\sqrt{a^2\cos\theta\cos\phi}/\sqrt{2}\omega_z$, and $\omega_{z_{eq}}^2 = \omega_z^2\sqrt{\pi}\text{erf}(v)/2v\exp(-v^2)$ is the equivalent beamwidth. Both the exact expression in Eq. (23) and the approximate expression when the effective area is a rotated ellipse in Eq. (35) are illustrated in Fig. 7.

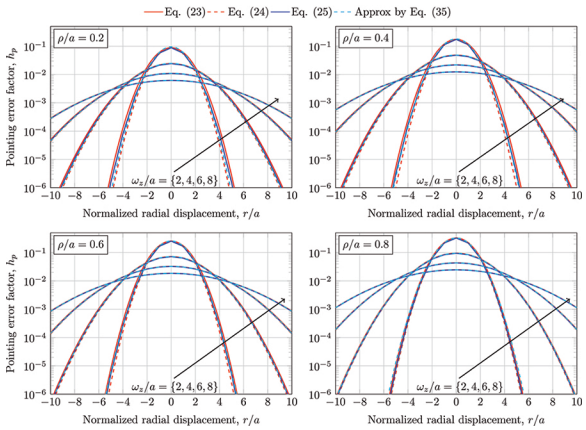


Fig. 7. Exact and approximate values of h_p when the effective area is a rotated ellipse for different values of the normalized rotation parameter ρ/a and the normalized beamwidth ω_z/a. Note that Eqs. (26), (27) and (28) have been evaluated through numerical integration.

Optics EXPRESS

Funding

Qatar National Library (QNL); Ooredoo Research Sponsorship 2015; Texas A&M University at Qatar (TAMUQ) RRSG 2019.

References

1. A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," IEEE Access **4**, 6121–6132 (2016).
2. N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," IEEE Commun. Mag. **54**(8), 110–117 (2016).
3. K. Guan, J. Cho, and P. J. Winzer, "Physical layer security in fiber-optic MIMO-SDM systems: An overview," Opt. Commun. **408**, 31–41 (2018).
4. H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone, P. Villoresi, T. Aoki, and M. Sasaki, "Free-space optical channel estimation for physical layer security," Opt. Express **24**(8), 8940–8955 (2016).
5. J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," IEEE Trans. Commun. **66**(12), 6423–6436 (2018).
6. J.-Y. Wang, H. Ge, M. Lin, J.-B. Wang, J. Dai, and M.-S. Alouini, "On the secrecy rate of spatial modulation based indoor visible light communications," arXiv preprint arXiv:1906.09512 (2019).
7. M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, C. Assi, M. Safari, and H. Haas, "Physical layer security for visible light communication systems: A survey," arXiv preprint arXiv:1905.11450 (2019).
8. M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," Commun. Surv. & Tutorials, IEEE **16**(4), 2231–2258 (2014).
9. M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," IEEE/OSA J. Opt. Commun. Netw. **6**(8), 684–694 (2014).
10. M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008).
11. Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," IEEE Trans. Inf. Theory **54**(6), 2470–2492 (2008).
12. H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over $\alpha - \mu$ fading channels," IEEE Commun. Lett. **21**(6), 1445–1448 (2017).
13. Z. Rezki, B. Alomair, and M.-S. Alouini, "On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, 1602–1607 (2014).
14. H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-*m* channels," IEEE Trans. Veh. Technol. **65**(12), 10126–10132 (2016).
15. L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," IEEE Transactions on Wirel. Commun. **13**(11), 6054–6067 (2014).
16. B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," IEEE Commun. Mag. **56**(11), 131–137 (2018).
17. F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," IEEE Photonics J. **7**(2), 1–2 (2015).
18. 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 Photonics J. **9**(4), 1–14 (2017).
19. 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. **66**(12), 6384–6395 (2018).
20. H. Lei, H. Luo, K.-H. Park, Z. Ren, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," IEEE Photonics J. **10**(3), 1–13 (2018).
21. J. Wang, C. Liu, J. Wang, J. Dai, M. Lin, and M. Chen, Secrecy outage probability analysis over Malaga-Malaga fading channels, in *International Conference on Communications (ICC), 2018 IEEE*, 1, 6, (2018).
22. 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 **7**, 66725–66730 (2019).
23. M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," IEEE Wirel. Commun. Lett. **6**(2), 274–277 (2017).
24. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J. **54**(8), 1355–1387 (1975).
25. S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, "Understanding the performance of free-space optics [invited]," J. optical Netw. **2**(6), 178–200 (2003).
26. R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and C. Castillo-Vázquez, "Impact of nonzero boresight pointing error on ergodic capacity of MIMO FSO communication systems," Opt. Express **24**(4), 3513–3534 (2016).
27. F. Yang, J. Cheng, and T. Tsiftsis, "Free-space optical communication with nonzero boresight pointing errors," IEEE Trans. Commun. **62**(2), 713–725 (2014).
28. R. Boluda-Ruiz, A. García-Zambrana, B. Castillo-Vázquez, and C. Castillo-Vázquez, "On the capacity of MISO FSO systems over gamma-gamma and misalignment fading channels," Opt. Express **23**(17), 22371–22385 (2015).

Optics EXPRESS

29. J. M. Kahn and J. R. Barry, "Wireless infrared communications," Proc. IEEE **85**(2), 265–298 (1997).
30. A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," J. Lightwave Technol. **25**(7), 1702–1710 (2007).
31. I. I. Kim, B. McArthur, and E. J. Korevaar, "Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications," in *Information Technologies 2000, (International Society for Optics and Photonics, 2001)*, 26, 37, (2000).
32. L. Andrews, R. Phillips, and C. Hopen, *Laser beam scintillation with applications* , vol. 99 (SPIE press, 2001).
33. R. Boluda-Ruiz, A. García-Zambrana, C. Castillo-Vázquez, and B. Castillo-Vázquez, "Novel approximation of misalignment fading modeled by Beckmann distribution on free-space optical links," Opt. Express **24**(20), 22635–22649 (2016).
34. M. Najafi, H. Ajam, V. Jamali, P. D. Diamantoulakis, G. K. Karagiannidis, and R. Schober, "Statistical modeling of FSO fronthaul channel for drone-based networks," in *2018 IEEE International Conference on Communications (ICC)*, 1–7, (2018).
35. H. Arezumand, H. Zamiri-Jafarian, and E. Soleimani-Nasab, "Exact and asymptotic analysis of partial relay selection for cognitive RF-FSO systems with non-zero boresight pointing errors," IEEE Access **7**, 58611–58625 (2019).
36. G. K. Varotsos, H. E. Nistazakis, W. Gappmair, H. G. Sandalidis, and G. S. Tombras, "SIMO subcarrier PSK FSO links with phase noise and non-zero boresight pointing errors over turbulence channels," IET Commun. **13**(7), 831–836 (2019).
37. A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and series Volume 3: More Special Functions*, vol. 3 (Gordon and Breach Science Publishers, 1999).
38. M. A. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," Opt. Eng. **40**(8), 1554 (2001).
39. A. Lapidoth, S. Moser, and M. Wigger, "On the capacity of free-space optical intensity channels," IEEE Trans. Inf. Theory **55**(10), 4449–4461 (2009).
40. N. Wang and J. Cheng, "Moment-based estimation for the shape parameters of the gamma-gamma atmospheric turbulence model," Opt. Express **18**(12), 12824–12831 (2010).
41. Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," IEEE Trans. Commun. **51**(8), 1389–1398 (2003).
42. C. Castillo-Vazquez, R. Boluda-Ruiz, B. Castillo-Vazquez, and A. Garcia-Zambrana, "Outage performance of DF relay-assisted FSO communications using time-diversity," IEEE Photonics Technol. Lett. **27**(11), 1149–1152 (2015).
43. J. C. Ricklin and F. M. Davidson, "Atmospheric turbulence effects on a partially coherent Gaussian beam: implications for free-space laser communication," J. Opt. Soc. Am. A **19**(9), 1794–1802 (2002).