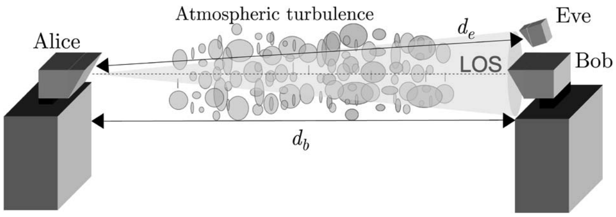
IEEE Photonics Journal
An IEEE Photonics Society Publication

Physical-Layer Security in Free-Space Optical Communications

Volume 7, Number 2, April 2015

F. Javier Lopez-Martinez, Member, IEEE
Gerardo Gomez
José María Garrido-Balsells



DOI: 10.1109/JPHOT.2015.2402158
1943-0655 © 2015 IEEE

Physical-Layer Security in Free-Space Optical Communications

F. Javier Lopez-Martinez, *Member, IEEE*, Gerardo Gomez, and José María Garrido-Balsells

Departamento de Ingenieria de Comunicaciones, Universidad de Malaga, 29071 Malaga, Spain

DOI: 10.1109/JPHOT.2015.2402158

Manuscript received January 8, 2015; revised February 4, 2015; accepted February 5, 2015. Date of publication February 10, 2015; date of current version March 2, 2015. This work was supported in part by Junta de Andalucia under Grant P11-TIC-7109, by the Spanish Government under Grant COFUND2013-40259 and Grant TEC2013-44442-P, by the University of Malaga and the European Union under Marie-Curie COFUND U-mobility program under Grant 246550, and by the Spanish Ministerio de Economía y Competitividad under Project TEC2012-36737. Corresponding author: F. J. Lopez-Martinez (e-mail: fjlopezm@ic.uma.es).

Abstract: The communication between two legitimate peers in the presence of an external eavesdropper is studied from a physical-layer security perspective in the context of free-space optical (FSO) communications. We discuss viable mechanisms to eavesdrop the communication and study the effect of random optical irradiance fluctuations inherent to FSO communications on the probability of achieving a secure transmission. We observe that the joint effect of laser-beam divergence and turbulence-induced fading on the received irradiance, under certain conditions, allows an external eavesdropper close to the legitimate receiver to compromise the communication. Interestingly, we also observe that an eavesdropper placed close to the legitimate transmitter can easily compromise the communication by taking advantage of the larger attenuation suffered by the signal when propagating through the FSO link.

Index Terms: Atmospheric turbulence, free-space optical communications, physical-layer security, scintillation, secrecy.

1. Introduction

The possibility of having a secure communication in the presence of an external eavesdropper is a classical problem in communication theory, ever since Wyner introduced the wiretap channel [1]. The original formulation of the problem was motivated by the potential insecurity of electrical signals transmitted through copper-wired links due to compromising emanations or physical wire-tapping. However, while fiber optic cables are extremely more secure than comparable copper cables, the interception of the optical signals transmitted through fiber is also possible [2]. For this reason, the problem of secure communications in optical links has also been a matter of study [3]–[5].

Wireless transmission is known to provide an additional layer of security to the communication between two legitimate peers in the presence of an eavesdropper [6], [7], due to the random fluctuations that affect the signals when propagating through air. As opposed to the conventional setup for the Gaussian wiretap channel [8] for wired links, fading allows for having a secure communication even when the average signal-to-noise ratio (SNR) at the eavesdropper is larger than the SNR at the legitimate receiver. This observation has boosted the interest of the research community in the field of physical layer security over the past few years [9]–[16], as a means to provide reliable secure communications, relaxing the complexity and complementing the performance of the required cryptographic technologies.

Similarly to what happens in wired links, wireless optical transmission is inherently more secure than radio-frequency (RF) transmission. Because of the high directionality of optical beams compared to the almost broadcast nature of RF signals, this makes them much harder, yet not impossible, to intercept. For this reason, the literature related to physical layer security in wireless optical communications is much scarcer, both for visible light [17] and free-space [18]–[20] optical (FSO) communications.

The propagation in FSO communications is affected by harmful effects, within which the most relevant one is the random fading characteristic of the received optical intensity. This phenomenon, referred to as scintillation, leads to a random SNR at the receiver that can cause a link outage. In this sense, the statistical behavior of the received optical irradiance has been analytically characterized by means of known statistical distributions that fit to experimental measures, such as Log-normal or Gamma-Gamma [21]–[23], modeling weak, moderate, or strong turbulence conditions.

Moreover, the specific nature of FSO communication systems imposes some restrictions on how an eavesdropper can effectively intercept the communication by the transmitter and receiver. A plausible mechanism for interception arises when part of the beam radiation is reflected by small particles, and then is detectable by an external observer not in the line-of-sight (LOS) of both communication peers. However, the amount of power received by the eavesdropper will be considerably smaller, compared to an equivalent RF scenario. An alternative scenario would have the eavesdropper blocking the laser beam in order to collect a larger amount of power. Should this be the case, then the legitimate receiver would notice that the average received power is decreased noticeably and therefore the communication can be stopped for security reasons. As we will later discuss, there can be other alternatives for designing physically realizable eavesdroppers that take advantage of the specific nature of optical transmission.

In this paper, we provide a theoretical characterization of the probability of secure transmission in FSO communication systems. Specifically, we consider two legitimate peers that wish to communicate securely in the presence of an external observer. We characterize the security of the FSO link in terms of the probability of having a secure transmission, using the probability of strictly positive secrecy capacity as performance metric [6]. We obtain novel closed-form expressions for this metric for most common FSO propagation models that allow us to study the interplay between the amount of power leaked to the eavesdropper and the propagation conditions when characterizing the communication from a physical layer security viewpoint.

2. System Model and Problem Definition

As previously mentioned, we consider the problem in which two legitimate peers, say Alice (transmitter) and Bob (receiver), wish to communicate over a wireless link in the presence of an eavesdropper, say Eve, that observes their transmission.[1] Here, a terrestrial FSO link which consists of a single-mode semiconductor laser as the transmitter and a photo-detector as the receiver is considered, assuming that an On-Off Keying (OOK) intensity modulation with direct detection scheme is employed. The noise at the receiver is modeled as Additive White Gaussian Noise (AWGN) with zero mean and variance σ_n^2, mainly associated to the high intensity shot noise produced by the ambient light, as detailed in [24].

We also consider the presence of an eavesdropping device (Eve) that can be understood as a sensing device that collects a fraction of the power radiated by Alice. As discussed in the introduction, the presence of Eve should not affect the received power at the legitimate receiver in a way that makes Bob aware of the attack and, therefore, able to request Alice to stop the

[1] We here use the standard placeholder names for denoting the different agents that take part in the communication, which is inherited from the field of cryptography and to the best of our knowledge can be traced back to the late 1970s [25]. This is also the usual nomenclature in quantum cryptography.

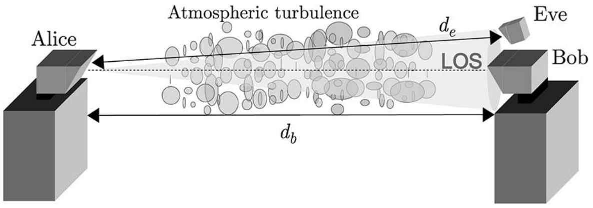


Fig. 1. Interception of an FSO link in the divergence region of the laser beam (case EnB).

communication for security reasons. Therefore, we consider that Eve collects a fraction r_e of the available power from the received laser beam whereas Bob receives a fraction r_b, being $r_e + r_b \leq 1$. The direct link between Alice and Bob, i.e., the line of sight (LOS), is characterized by a distance d_b whereas d_e represents the distance between Alice and Eve. Note that the parameters r_e and r_b are dependent on the method used to collect the optical power into each device.

With these settings, the instantaneous electrical SNR at the receiver side can be defined as $\gamma = (RI_0 I)^2/\sigma_n^2 = \gamma_0 I^2$, where R is the photo-diode responsivity, I_0 is the received optical irradiance in absence of signal fluctuations due to turbulence and I is a random variable that models the normalized irradiance received in an atmospheric scintillation scenario. Note that γ_0 represents the electrical SNR in the absence of atmospheric scintillation.

Hence, the instantaneous electrical SNR in the absence of atmospheric turbulence $\gamma_{0,x}$ received at Eve $(x = e)$ and Bob $(x = b)$ can be defined as

$$\gamma_{0,x} = \frac{(RI_{0,x})^2}{\sigma_n^2} = \frac{(Rr_x I_{tx} e^{-\delta d_x})^2}{\sigma_n^2} \tag{1}$$

where $I_{0,x} = r_x I_{tx} e^{-\delta d_x}$ is the optical irradiance received at x in absence of turbulence, I_{tx} represents the radiant emittance of the laser, and the term $e^{-\delta d_x}$ represents the intensity attenuation loss in free space, δ being an attenuation loss constant and d_x the distance from the transmitter to x.

Since the laser beam experiences divergence due to optical diffractions, one possibility for a successful eavesdropping is to locate Eve in the divergence region of the laser beam as suggested in [26]. In practice, this implies that Eve is placed close to Bob, as shown in Fig. 1. According to this model, the FSO link is inherently secure for small divergence angles. However, note that for long distances between legitimate peers, Eve has a stronger chance for eavesdropping on the FSO link, by collecting the power not captured by Bob. In this case, the parameters r_e and r_b depend on the aperture diameter of each device as well as the beam divergence angle.

In a different scenario, the eavesdropper could potentially intercept the communication by capturing power within the convergence zone of the beam. By doing so, there is a chance that Bob (or Alice) become aware of the presence of Eve. In our analysis, we will also discuss the implications of this situation on the security of the FSO link.

Let us denote as γ_b the instantaneous electrical SNR at the receiver for the link between Alice and Bob, and let γ_e be the instantaneous electrical SNR at the eavesdropper for the wiretap link between Alice and Eve. According to the information-theoretic formulation in [8], the secrecy capacity is the maximum transmission rate at which Eve is unable to extract any information and is defined as

$$C_S = C_b - C_e \tag{2}$$

where C_b is the instantaneous capacity of the main (Bob) channel

$$C_b = \log(1 + \gamma_b) \tag{3}$$

and C_e is the instantaneous capacity of the eavesdropper channel

$$C_e = \log(1 + \gamma_e) \tag{4}$$

where log is the base-2 logarithm. For the sake of simplicity, we assumed a normalized bandwidth $B = 1$ in the previous capacity definitions.

In this case, assuming that I_e and I_b are the normalized irradiance fluctuations at Eve and Bob, the instantaneous electrical SNR received at Eve (γ_e) and Bob (γ_b) can be expressed, respectively, as

$$\gamma_e = \gamma_{0,e} I_e^2 \tag{5}$$

and

$$\gamma_b = \gamma_{0,b} I_b^2. \tag{6}$$

Since channel capacity is by definition a non-negative metric, the secrecy capacity for a given realization of the fading links is, therefore, given by

$$C_S = \begin{cases} \log(1+\gamma_b) - \log(1+\gamma_e), & \gamma_b \geq \gamma_e \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Due to the different propagation effects inherent to FSO communications, both γ_e and γ_b are in general subject to random fluctuations that will impact the capacities of both links, and therefore the secrecy capacity. We consider that the random fading channel coefficients do not change over the transmission of a codeword [7]. Similarly, this consideration is also related to the availability of channel state information (CSI) at the receivers: in this situation, both Bob and Eve can estimate the channel very accurately and hence have almost perfect CSI. Furthermore, Alice is also able to know Bob's CSI through a feedback mechanism [27] or based on channel reciprocity [28]. We can also assume that Alice has some knowledge of Eve's channel. As we will later justify (cfr. Section 5), even though when Eve is a malicious passive eavesdropper for which CSI cannot be estimated by Alice, we can still consider that some kind of statistical CSI knowledge is available at Alice.

As previously mentioned, the atmospheric turbulence induces a random fluctuation on the received optical irradiance and, thus, on the electrical SNR, which is usually characterized by different stochastic models [23], [29]. Among these models, the most commonly used are the log-normal, usually applied under weak turbulence conditions, the negative exponential, for strong or extreme atmospheric conditions, and the Gamma-Gamma distribution. This last one was presented to provide a mathematically tractable model based on the multiplicative effect of large-scale and small-scale fluctuations [22]. This statistical distribution has been widely used to model from weak to strong turbulence induced scintillation.

In this work, we will use a probabilistic metric for the characterization of the secure communication as defined in [6], which is usually referred to as *probability of strictly positive secrecy capacity*

$$P_S^+ = \mathcal{P}(C_S > 0) \tag{8}$$

which can be regarded as the probability of existence of a secure communication.

3. Analysis

From previous equations, we find the following general relationship between the electrical SNR received at Bob and Eve in absence of atmospheric turbulence,

$$\gamma_{0,e} = \gamma_{0,b} \left(\frac{r_e}{r_b} e^{\delta(d_b - d_e)} \right)^2. \tag{9}$$

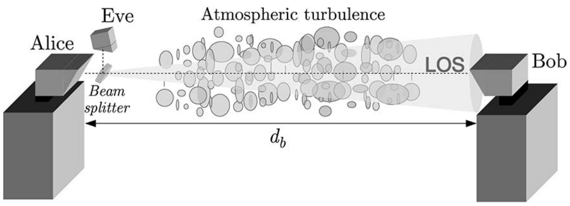


Fig. 2. Interception of an FSO link when Eve is close to the transmitter (case EnA).

From (7), in this situation the secrecy capacity C_S is not null whenever $\gamma_{0,b} > \gamma_{0,e}$, which is satisfied if

$$e^{-\delta d_e} < \frac{r_b}{r_e} e^{-\delta d_b} \tag{10}$$

that is, when the atmospheric attenuation loss experienced by Eve is lower than a scaled version of the atmospheric attenuation loss experienced by Bob. Note that in the scenario depicted in Fig. 1 and considered in [26], the secure communication is very likely to occur: in practice, the eavesdropper needs to be located in the proximity of Bob due to physical constraints (e.g., in the top of the same building) so that $d_e \approx d_b$; furthermore, the transmission between Alice and Bob is aligned in order to maximize the amount of received power, and therefore it is reasonable that in most scenarios $r_b > r_e$. However, an additional insight can be extracted from (10): in case Eve is located very close to the transmitter Alice (e.g., again, in the top of the same building), we have that $d_b \gg d_e$ or equivalently $d_e \approx 0$. Hence, even though the beam might not have diverged in the proximity of Alice, there is a chance that the secure communication between Alice and Bob is compromised even for $r_e \to 0$.

In a more realistic scenario, the presence of atmospheric turbulence must be considered. Hence, under random irradiance fluctuations, the probability of having a secure communication is given by

$$P_S^+ = \mathcal{P}(C_S > 0) = \mathcal{P}\left(\log \frac{1+\gamma_b}{1+\gamma_e} > 0\right) = \mathcal{P}\left(\frac{1+\gamma_{0,b} I_b^2}{1+\gamma_{0,e} I_e^2} > 1\right) = \mathcal{P}\left(I_b^2 > \frac{\gamma_{0,e}}{\gamma_{0,b}} I_e^2\right). \tag{11}$$

This general expression is independent on the statistical model used to described the effect of the atmospheric turbulence. In the next subsections, we analyze this secrecy capacity metric depending on the position of the eavesdropper for weak to strong turbulence intensities. As previously discussed yet without loss of generalization, and justified by the inherent characteristics of FSO links, we focus on two cases depending on whether the eavesdropper is located near the transmitter or near the receiver.

3.1. Case A: Eavesdropper Near the Transmitter

Let us first consider the case when an eavesdropping device is located near the transmitter. We will refer to this scenario as EnA (Eve near Alice). Due to the narrowness of the laser beam near Alice, a potential eavesdropper near the transmitter cannot intercept the beam without partially blocking the LOS between Alice and Bob, as shown in Fig. 2. From a practical implementation point of view, Eve must be a sufficiently sophisticated device so that it can get a small fraction r_e of the irradiance from the laser beam towards Eve and let pass a fraction r_b of the irradiance towards Bob, with $r_e + r_b \leq 1$, where the equality holds under the assumption of a lossless passive eavesdropper (for instance, a passive optical beam splitter based device carefully placed at the transmitter output). In this case, the parameters r_e and r_b also depend on the eavesdropper reflection/transmission ratio parameter.

In this scenario, since $d_e \approx 0$, we can assume absence of turbulence and attenuation for the channel between the transmitter (Alice) and the eavesdropper (Eve), i.e., $\gamma_e = \gamma_{0,e}$. However, the link between legitimate peers is subject to random fluctuations inherent to FSO links. Therefore, the probability of achieving a successful secure communication between Alice and the legitimate receiver, i.e., Bob, will be given by

$$P_S^+ = 1 - \mathcal{P}(C_S \leq 0) = 1 - F_b\left(\sqrt{\frac{\gamma_{0,e}}{\gamma_{0,b}}}\right) = 1 - F_b\left(\frac{r_e}{1 - r_e} e^{\delta d_b}\right) \tag{12}$$

where $F_b(\cdot)$ is the cumulative distribution function (cdf) of the normalized irradiance received at Bob I_b. Hence, this probability depends on the specific distribution used to model the FSO link between Alice and Bob, the fraction of power leaked to the eavesdropper (r_e), and the distance between Alice and Bob (d_b). Interestingly, P_S^+ in this scenario is fully characterized by the cdf of the electrical SNR at Bob. Note that the presence of fading leads to a non-zero secrecy capacity for the whole range of $r_e \in [0, 1)$, whereas in the absence of turbulence the set of values of r_e that ensures a certain strictly positive secrecy capacity is obtained from (10) as $r_e \in [0, 1/(e^{\delta d_b} + 1))$.

3.2. Case B: Eavesdropper Near the Receiver

We now consider the case in which Eve is located close to the receiver, that corresponds to the system depicted in Fig. 1. We will refer to this scenario as EnB (Eve near Bob). This is the scenario suggested in [26] as potentially likely to suffer from eavesdropping. In this situation, the received irradiances at Bob and Eve will be affected by random fluctuations induced by turbulences both in the small and large scale. Due to their spatial proximity, these random effects will be correlated [29]. Hence, the computation of the probability of strictly positive secrecy capacity in this scenario according to (11) must be carried out from the joint distribution of γ_b and γ_e.

In some practical situations, the correlation patterns for the small-scale and large-scale turbulences may have different behaviors. As in [30], we assume that the distance $d_b \approx d_e$ is much larger than the laser beam divergence, and also that Bob and Eve are sufficiently close. Hence, the signals received by both agents are likely to be deflected by the same eddies, implying that large-scale effects can be assumed to be the same for both receivers. However, as discussed in [30], the small-scale effects are assumed to be identically distributed and correlated due to spatial proximity, with this correlation depending on the relative position of Eve with respect to Bob.

Expressing the received optical irradiances in terms of their separated small-scale and large-scale components [22], we have

$$I_b = XY_b \tag{13}$$

$$I_e = XY_e \tag{14}$$

where X models the random effects of large-scale induced turbulence, whereas Y_b and Y_e model the small-scale fluctuations at Bob and Eve, respectively. Thus, (11) can now be reexpressed as

$$P_S^+ = \mathcal{P}\left(X^2(\gamma_{0,b} Y_b^2 - \gamma_{0,e} Y_e^2) > 0\right) = \mathcal{P}\left(\sqrt{\gamma_{0,b}} Y_b - \sqrt{\gamma_{0,e}} Y_e\right) > 0\right) = \mathcal{P}(r_b Y_b - r_e Y_e) > 0). \tag{15}$$

Interestingly, this latter metric does not depend on the distribution of the large-scale turbulence. The small-scale components Y_e and Y_b are usually modeled as Gamma random variables in most popular models in the literature (e.g., Gamma-Gamma or Gamma-Lognormal) [23], which can be correlated due to spatial proximity. Since the distribution of the difference of two correlated gamma variables is known to be connected with the McKay distribution [31], P_S^+ can be computed using the results in [32].

In this situation, if we denote $\Delta_b = r_b Y_b$ and $\Delta_e = r_e Y_e$, we have that both are Gamma distributed $\Delta_b \sim \mathcal{G}(\beta, \beta/r_b)$, and $\Delta_e \sim \mathcal{G}(\beta, \beta/r_e)$ and their marginal probability density functions (pdfs) have the following form:

$$f_{\Delta_b}(y) = \left(\frac{\beta}{r_b}\right)^{\beta} \frac{1}{\Gamma(\beta)} y^{\beta-1} \exp(-\beta y/r_b), \qquad y \geq 0 \tag{16}$$

$$f_{\Delta_e}(y) = \left(\frac{\beta}{r_e}\right)^{\beta} \frac{1}{\Gamma(\beta)} y^{\beta-1} \exp(-\beta y/r_e), \qquad y \geq 0 \tag{17}$$

where $\Gamma(\cdot)$ is the Gamma function, and β is the shape parameter of the Gamma distribution, related to the effective number of small-scale eddies that affect each link [22]. Note that for mean-normalized Y_x, as usually assumed, the average of Δ_x is $\mathrm{E}[\Delta_x] = r_x$. The pdf of $\Delta = \Delta_b - \Delta_e$ can be expressed in closed-form using [32, eq. 22a] as

$$\begin{aligned} f_\Delta(x) = &\frac{|x|^{\beta-1/2}}{\Gamma(\beta)\sqrt{\pi\theta_1\theta_2(1-\rho)}} \left(\frac{1}{(\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho}\right)^{\frac{2\beta-1}{4}} \\ &\times \exp\left(-\frac{x}{2(1-\rho)}\left(\frac{1}{\theta_1} - \frac{1}{\theta_2}\right)\right) K_{\beta-1/2}\left(|x| \frac{\sqrt{(\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho}}{2\theta_1\theta_2(1-\rho)}\right) \end{aligned} \tag{18}$$

for $x \neq 0$, where $\theta_1 = r_b/\beta$, $\theta_2 = r_e/\beta$, ρ is the correlation coefficient between Δ_1 and Δ_2 and $K_\nu(\cdot)$ is the modified Bessel function of the second kind and order ν. We see that the pdf of Δ has the form

$$f_\Delta(x) = C_0 x^{a-1} \exp(-bx) K_{a-1}(cx) \tag{19}$$

with $C_0 = 1/(\Gamma(\beta)\sqrt{\pi\theta_1\theta_2(1-\rho)}) \cdot (1/((\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho))^{(2\beta-1)/4}$, and the parameters $a = \beta + 0.5$, $b = 0.5/(1-\rho) \cdot (1/\theta_1 - 1/\theta_2)$, and $c = \sqrt{((\theta_1+\theta_2)^2 - 4\theta_1\theta_2\rho)}/(2\theta_1\theta_2(1-\rho))$.

Therefore, after plugging (18) into (15), the following integral needs to be solved in order to characterize the secrecy metric P_S^+

$$P_S^+ = \int_0^\infty f_\Delta(x)dx = C_0 \int_0^\infty x^{a-1} \exp(-bx) K_{a-1}(cx) dx = C_0 \cdot \mathcal{I}(a, b, c). \tag{20}$$

This integral can be solved using [33, 6.621.3], yielding

$$\mathcal{I}(a,b,c) = 2^{-a} c^{a-1} (b^2 - c^2)^{1/2-a} \Gamma(1-a)\Gamma(2a-1) + \frac{2^{a-2} c^{1-a} \Gamma(a-1)}{b} {}_2F_1\left(\frac{1}{2}, 1; 2-a; \frac{c^2}{b^2}\right) \tag{21}$$

$$= \frac{\sqrt{\pi}(2c)^{a-1}}{(b+c)^{2a-1}} \frac{\Gamma(2a-1)}{\Gamma(a+1/2)} {}_2F_1\left(2a-1, a-\frac{1}{2}; a+\frac{1}{2}; \frac{b-c}{b+c}\right) \tag{22}$$

where ${}_2F_1(\cdot, \cdot; \cdot; \cdot)$ is the Gauss Hypergeometric function. Specializing for $\beta = 1$, which corresponds to the case of very strong turbulence intensity, the secrecy metric has a simpler expression in terms of elementary functions as

$$P_S^+ = \frac{1}{2} \frac{r_b - r_e + \sqrt{(re + rb)^2 - 4 r_e r_b \rho}}{\sqrt{r_e^2 + r_b^2 + 2 r_e r_b (1 - 2\rho)}}. \tag{23}$$

The particular cases of total correlation and zero correlation for the small-scale components have special interest as they represent limiting behaviors. In the first situation, $Y_e = Y_b$, and

TABLE 1

Parameter values for different turbulence conditions

Turbulence intensity	Scintillation parameters
Weak	$\sigma_l^2 = 0.3$
Moderate	$\sigma_l^2 = 1.6 \to \alpha = 4, \beta = 1.9$
Strong	$\sigma_l^2 = 3.5 \to \alpha = 4.2, \beta = 1.4$

hence, the probability of strictly secrecy capacity is simplified to

$$\mathcal{P}(C_S > 0) = \mathcal{P}(\gamma_{0,b} > \gamma_{0,e}) = \begin{cases} 1, & r_b > r_e \\ 0, & \text{otherwise} \end{cases} \tag{24}$$

which exhibits a binary behavior as in the classical setup for the Gaussian wiretap channel [1].

On the contrary, if total independence is assumed for the small-scale turbulence induced fading, we observe a very different behavior. As both agents, Eve and Bob, experience uncorrelated small-scale fluctuations, the probability P_S^+ is maximized for a given β when $\rho = 0$. In the particular case of considering an exponential distribution for the received irradiance at Bob and Eve (i.e., very strong turbulence, $\beta = 1$), we obtain a very simple expression for this probability:

$$\mathcal{P}(C_S > 0) = \frac{r_b/r_e}{r_b/r_e + 1}. \tag{25}$$

The best possible eavesdropper would be able to ideally collect all the power not captured by Bob (i.e., $r_b = 1 - r_e$). Hence, (25) reduces to

$$\mathcal{P}(C_S > 0) = 1 - r_e = r_b. \tag{26}$$

4. Results

We have presented a detailed characterization of the information-theoretic security for FSO links in terms of the pdf and cdf of the SNRs at Eve and/or Bob. Hence, our approach applies in general for any choice of distribution, thus allowing for considering different propagation conditions. Next, the expressions derived in the previous section are evaluated numerically to discuss the main implications that arise in practical scenarios of interest.

We will first focus on the EnA scenario described in Section 3.1. Since the secrecy metrics calculated in this situation are expressed in terms of the cdf of the normalized irradiance received at Bob, conveniently scaled by the rest of system parameters (i.e., d_b and r_e), we can easily evaluate them in different atmospheric turbulence conditions. Specifically, we will use the Gamma-Gamma (GG) distribution [22] to model both moderate and strong turbulence, whereas the scenarios affected by weak turbulences will be modeled by the Log-normal (LN) distribution, respectively. The cdfs for both turbulence fading models are, respectively, given by

$$F_{GG}(I) = \frac{1}{\Gamma(\alpha)\Gamma(\beta)} G_{1,3}^{2,1}\left[\alpha\beta I \middle| \begin{matrix} 1 \\ \alpha, \beta, 0 \end{matrix}\right] \tag{27}$$

$$F_{LN}(I) = \frac{1}{2}\text{erfc}\left(-\frac{\ln I + \sigma_I^2/2}{\sigma_I\sqrt{2}}\right) \tag{28}$$

where σ_I^2 is the log-intensity variance, and α and β are the effective number of large-scale and small-scale eddies of the scattering process, respectively, whose values depend on σ_I^2. Besides, erfc$(\cdot)$ is the complementary error function, and $G_{m,n}^{p,q}[\cdot|\cdot]$ is the Meijer function. The values for the log intensity variance σ_I^2 assumed in this scenario are listed in Table 1. For the sake of simplicity, the equivalent Gamma-Gamma shape parameters α and β have been obtained from [22, Eq. (18)] and [22, Eq. (19)], respectively, assuming plane wave and negligible inner scale.

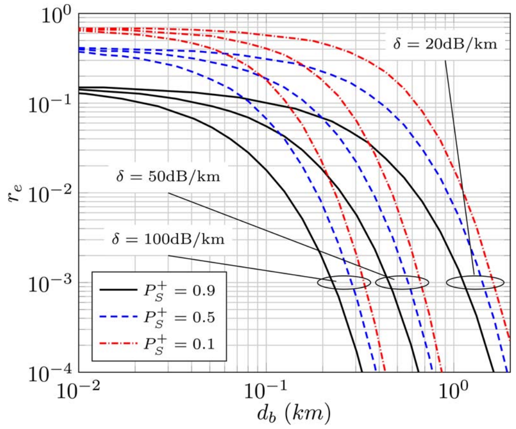


Fig. 3. Value of r_e that satisfies a certain strictly secrecy capacity as a function of the distance d_b between Alice and Bob. EnA scenario with moderate turbulence. Parameter values: $\alpha = 4$, $\beta = 1.9$, and $r_b = 1 - r_e$.

In Fig. 3, we investigate the value of r_e (fraction of the laser beam leaked to Eve) that leads to a certain value of probability of strictly secrecy capacity, as a function of the distance d_b between Alice and Bob. The set of values for this probability is 0.1, 0.5 and 0.9, meaning that in the presence of an eavesdropper, a secure communication is only possible with a 10%, 50% or 90% of probability at a given distance. Typical values for the atmospheric attenuation loss δ are considered [34], as well as a moderate turbulence scenario modeled by the Gamma-Gamma distribution with $\alpha = 4.0$ and $\beta = 1.9$.

We observe a huge dependence with the atmospheric attenuation loss experienced by Bob. For instance, if we want to guarantee a probability of positive secrecy capacity of 0.9 in the presence of an eavesdropper with $r_e = 0.01$ located near the transmitter, a maximum distance of 100–500 m is feasible for the FSO link (assuming an attenuation loss of 100 dB/km and 20 dB/km, respectively). Longer distances would be possible by reducing either the secrecy constraints, the fraction of transmit power received by Eve (r_e) or the attenuation losses. We must note that those values of $r_e > 10^{-2}$ would cause a noticeable power reduction at Bob and hence are likely to make the legitimate peers aware of Eve. However, we also see that in general the EnA scenario is very sensitive to eavesdropping for very low values of r_e. This somehow conflicts with the popular belief that FSO links are inherently secure thanks to the directivity of the laser beam. Hence, this fact must be taken into account when designing FSO communication systems with secrecy constraints.

The strictly positive secrecy capacity as a function of the distance d_b is represented in Fig. 4, for different turbulence conditions. A value of $r_e = 0.01$ and $r_b = 1 - r_e$ has been assumed. Weak turbulence is modeled by a log-normal distribution with $\sigma_I^2 = 0.3$, moderate turbulence is modeled by the Gamma-Gamma distribution with $\alpha = 4$, $\beta = 1.9$, and strong turbulence is modeled by the Gamma-Gamma distribution with $\alpha = 4.2$, $\beta = 1.4$.

In the EnA scenario, we observe two different behaviors that illustrate very insightful effects: for shorter distances, perfect secrecy starts being compromised first as the turbulence becomes more severe. This is in coherence with the fact that a stronger turbulence means a larger fluctuation in the SNR; therefore, even though in this situation the average SNR at Bob is larger than the average SNR at Eve, there is a non-negligible probability of Eve experiencing an *instantaneous* SNR better than Bob. It is interesting to see how the behavior of the secrecy metric becomes very abrupt as the turbulence is weaker. This is in good agreement with the fact that in the limit case of no turbulence, we have no random fluctuations affecting the signal and hence perfect secrecy is achieved if the average SNR at Bob is better than the average SNR at Eve (i.e., P_S^+ has a binary behavior as in the Gaussian wiretap channel setup).

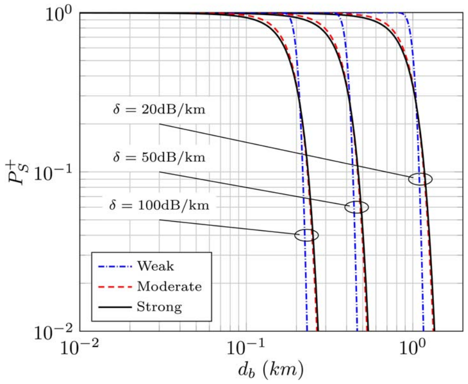


Fig. 4. Strictly secrecy capacity as a function of the distance d_b. EnA scenario. Parameter values: $\sigma_I^2 = 0.3$, $\alpha_{\text{mod}} = 4$, $\beta_{\text{mod}} = 1.9$, $\alpha_{\text{str}} = 4.2$, $\beta_{\text{str}} = 1.4$, $r_e = 10^{-2}$, and $r_b = 1 - r_e$.

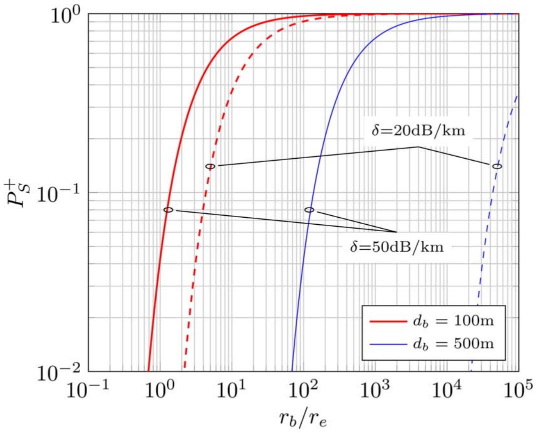


Fig. 5. Probability of strictly secrecy capacity as a function of the ratio r_b/r_e. EnA scenario with very strong turbulence, $r_e + r_b = 1$.

For longer distances, we observe the complete opposite situation: when the attenuation is large enough to provoke that the average SNR at Bob is smaller than the average SNR at Eve, random fluctuations are now allowing to have a secure communication even though it wouldn't be possible in the absence of turbulence. Since the more severe the turbulence, the larger the fluctuation, this explains why the decay of the secrecy metric is less abrupt for strong turbulence. We also note that regardless of the turbulence severity, the range of values of d_b for which secure communication is possible goes down as the atmospheric attenuation loss δ grows.

In Fig. 5, we now study the secrecy metric P_S^+ as a function of the ratio r_b/r_e in the EnA scenario. Since we are interested in understanding how random fluctuations affect the communication secrecy, we assume a very strong turbulence regime. For this reason, we use the well-known negative exponential model, for which the pdf has exponential form.

We observe that for low values of the ratio r_b/r_e, secure communication in the EnA scenario is practically unattainable. However, this situation has little impact in practice as this implies that the amount of power leaked to Eve is large enough, and hence, Alice and Bob could easily become aware of the presence of an eavesdropper. Specifically, $r_b/r_e = 1$ is the case on which Eve receives (and also blocks) 50% of the beam. From a practical viewpoint, the situation on which $r_b \gg r_e$ is much more interesting. We see that for the range of $r_b/r_e > 10^{-2}$, perfect secrecy is compromised with larger probability in two situations: when the distance between the legitimate peers d_b grows or when the atmospheric attenuation δ is more severe. Even for values

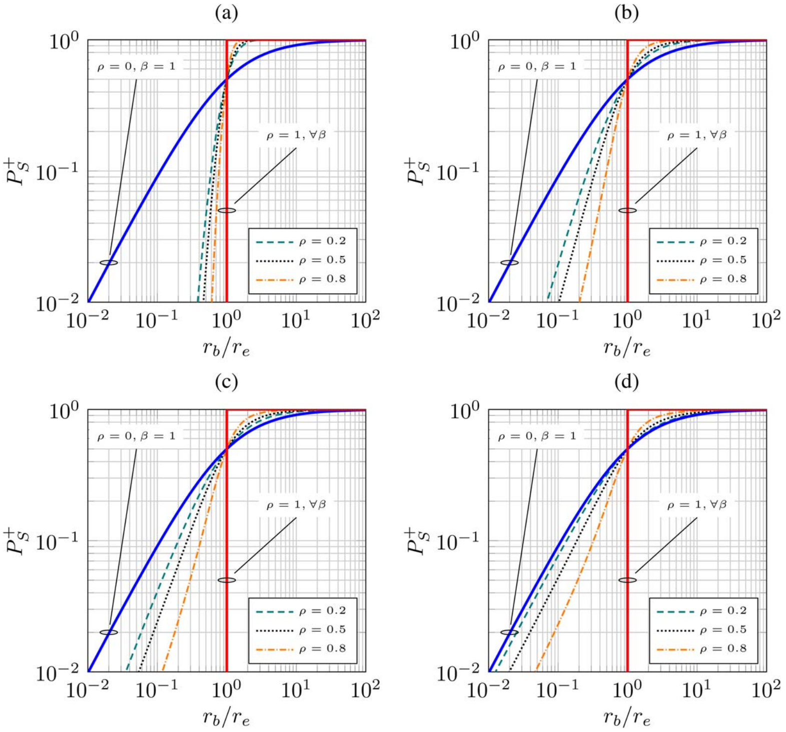


Fig. 6. Probability of strictly secrecy capacity as a function of the ratio r_b/r_e, for different turbulence severities and different values of correlation. EnB scenario: $r_e + r_b = 1$ (best possible eavesdropper assumption).

of $r_b/r_e > 10^{-2}$, achieving a secure communication with a 90% of probability clearly limits the maximum value of d_b.

We have certified that the EnA scenario is potentially susceptible to eavesdropping, despite the fact that the narrowness of the laser beam is an advantage from a security perspective. Now, we investigate the EnB scenario, on which Eve takes advantage of the laser beam divergence in order to eavesdropping the communication without affecting the amount of power received by Bob. Since the fully correlated approach for the large-scale fluctuations causes the secrecy metric P_S^+ to be independent of the large scale distribution, and assuming $d_e = d_b$ implies that P_S^+ is also independent of the distance, we will only pay attention to the impact of the small-scale fluctuations and the parameters r_e and r_b.

In Fig. 6, we illustrate how correlation between small-scale fading experienced by Bob and Eve has a very important impact on the secrecy. We consider the best possible eavesdropper implying $r_e + r_b = 1$; this means that Eve is able to collect the diverged part of the laser beam not captured by Bob, which corresponds to the worst case in terms of secrecy. We assume different turbulence severities, ranging from weak to very strong, modeled by means of Gamma-distributed random variables with different values of β. In the limit case of independence, we see that $P_S^+ > 0$ even if $r_b > r_e$; conversely, in the limit case of total correlation, both Bob and Eve have the exact same randomness since the channel realization is exactly the same. Therefore, the only difference is a constant scale factor that depends on r_e and r_b. This factor directly scales the average SNR at each receiver, and the scenario reduces to the Gaussian wiretap channel (i.e., no fading and only AWGN noise). Hence, in this limit situation perfect secrecy can be achieved provided that $r_b > r_e$, i.e., a binary behavior is observed. Since Bob is usually aligned with Alice, and assuming a reasonable value for the divergence of the laser beam, then $r_b \gg r_e$. This means that this limit case is indeed desirable for Alice and Bob, since perfect secrecy can be achieved.

Since a stronger turbulence implies a larger fluctuation, we observe that for a fixed value of r_b/r_e, secure communication is more likely to be compromised as β is decreased. We also see how as correlation grows, the secrecy metric tends to become more abrupt towards $r_b = r_e$. As previously mentioned, in practice Bob is aligned with Alice, which implies $r_b \gg r_e$. Hence, even though the EnB scenario is not perfectly secure when independence is assumed for the random fluctuations, we see that a secure communication is attained with a 90% of probability even in the case of $r_b = 10r_e$. We also see that if $r_b = r_e$, the curves cross at $P_S^+ = 50\%$; this is easily explained as in these cases, both Eve and Bob not only have the same average SNR but are equally distributed as well.

5. Discussion

In the previous sections, we have provided analytical results that allow us to understand how secure communication can be achieved in different scenarios of interest in the context of FSO communications. However, there are some aspects and details which deserve a deeper look.

First, the EnA and EnB scenarios have been chosen for being representative in real scenarios where FSO communications are used. Just like the legitimate transmitter and receiver in our system model are static devices placed at the top of buildings, we also thought that physically realizable devices suitable for eavesdropping would also need to be static and therefore placed in the proximities of Alice or Bob. However, it is indeed possible a more general scenario on which this restriction is eliminated. The effect of an eavesdropper placed in between the two legitimate peers can be mathematically analyzed through the general formulation in (11) and using the joint distribution of γ_b and γ_e for the probability calculation. In this case, it is harder for us to imagine the way an eavesdropper should look like in order to be able to physically intercept the message (compared to EnA and EnB). Perhaps more sophisticated scenarios, beyond the scope of this paper (e.g., one making use of an untrusted relay to communicate [35]) can also be considered.

Along the same lines, there also exists the possibility of having two non-colluding eavesdroppers (EnA and EnB scenarios at the same time). The exact mathematical formulation requires for more complicated probability calculations that the ones in this paper (cfr. [36] for the simpler Rayleigh fading model). However, we may infer what would happen in the specific context of FSO based on our analysis: it is more advantageous for an eavesdropper to be placed close to Alice, in order to take advantage of the path loss experienced by Bob. For an eavesdropper near Bob, there is not such advantage; moreover, such an eavesdropper also has to deal with having access to a smaller portion of power than the legitimate receiver. Hence, we can conclude that the scenario with two colluding eavesdroppers is very similar to the only EnA scenario in most circumstances.

Last, but not least, some knowledge of Eve's CSI is required in order to achieve a secure communication. Even though when Eve is a malicious passive eavesdropper for which CSI cannot be estimated by Alice, we can still assume some kind of statistical CSI knowledge at Alice: in the EnA scenario, Alice can assume that the average received power at Eve is a fraction of the transmitted power $r_e \cdot P_T$. The value of r_e is indeed unknown, but can be set to a worst case value (e.g. 10^{-2}) for designing the transmission. In the EnB scenario, the large-scale fading component can be assumed to be the same for Alice and Bob, whereas the small-scale fading component may take different instantaneous values (depending on correlation) but has the same statistical properties as Bob's CSI, conveniently scaling the variance through r_e/r_b. Once again, r_e may not be known but can be approximated in the worst case (best possible eavesdropper) as $r_e = 1 - r_b$.

It is however possible to use a secrecy formulation when neither Alice nor Bob have information regarding Eve's CSI. In such situation, the outage probability of secrecy capacity $\mathcal{P}\{C_S < R_S\}$ is a metric with operational significance, as it gives a probabilistic measure of how the instantaneous secrecy capacity is below a given secrecy rate R_S. Since no CSI of Eve is available at Alice, then Alice chooses to transmit at a constant rate R_S. This is equivalent to assuming that $\hat{C}_e = C_b - R_S$: therefore a secure communication can be achieved provided that $C_S < R_S$ (i.e., $C_e < \hat{C}_e$), whereas the communication is compromised if $C_S > R_S$ (i.e., $C_e > \hat{C}_e$). In the EnA scenario, this probability can be computed as

$$\mathcal{P}(C_S{<}R_S) = \mathcal{P}\left(I_b{<}\sqrt{\frac{2^{R_S}(1+\gamma_{0,e})-1}{\gamma_{0,b}}}\right) = F_b\left(\sqrt{\frac{2^{R_S}(1+\gamma_{0,e})-1}{\gamma_{0,b}}}\right). \tag{29}$$

Similarly, in the EnB scenario, the secrecy capacity outage probability is given by

$$\mathcal{P}(C_S{<}R_S) = \mathcal{P}\big(\gamma_{0,b}I_b^2{<}\big(2^{R_S}\gamma_{0,e}I_e^2 + 2^{R_S} - 1\big)\big). \tag{30}$$

While (29) can be expressed in terms of the distribution of the irradiance at Bob, the computation of (30) or other metrics such as the average secrecy capacity $\overline{C}_S = \mathbb{E}\{C_S\}$ using FSO-specific distributions seems to be challenging from a mathematical point of view.

6. Conclusion

We have discussed the implications of physical layer security in the context of FSO communications, using the probability of strictly secrecy capacity as performance metric. We have seen that for the sake of successfully compromising the communication between two legitimate peers, it is preferable for an eavesdropper to be located close to the transmitter. In this situation, referred to as EnA scenario, we have proved that a sufficiently sophisticated eavesdropper able to subtract a very small amount of power to the laser beam is capable of compromising the communication with a high probability. This probability is increased as the distance between legitimate peers grows.

We have also analyzed the case on which the eavesdropper is placed close to the receiver. This scenario, referred to as EnB, is shown to be inherently more secure than EnA. However, we have also seen that statistical independence of the small-scale fading experience by the legitimate receiver and the eavesdropper is detrimental in terms of security (i.e., beneficial for Eve): even though the average SNR at Bob is in practice larger than the average SNR at Eve, random fluctuations due to scintillation lead to having $P_S^+ < 1$, whereas in the absence of fading the communication between Alice and Bob would be perfectly secure.

We believe that these results open a new way of thinking when designing FSO communication systems, adding a new constraint in case a certain degree of security is demanded. Furthermore, the practical design of eavesdroppers able to operate in these scenarios is also a promising line for future research.

Acknowledgement

The authors would like to thank the associate editor for efficiently handling the review of this paper and the anonymous reviewers for their valuable suggestions and comments that helped to improve the quality of the paper. The authors also would like to thank Dr. I. Gasulla for her feedback on an earlier version of this paper.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[2] K. Shaneman and S. Gray, “Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection prevention,” in *Proc. IEEE MILCOM*, Oct. 2004, vol. 2, pp. 711–716.
[3] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, “Optical layer security in fiber-optic networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 725–736, Sep. 2011.
[4] K. Guan, P. Winzer, E. Soljanin, and A. Tulino, “On the secrecy capacity of the space-division multiplexed fiber optical communication systems,” in *Proc. IEEE Conf. CNS*, Oct. 2013, pp. 207–214.
[5] T. Eftimov, W. Bock, P. Balzhiev, V. Plachkova, and K. Zhelyazkova, “Securitized optical fiber communication and sensor systems using mode-selective couplers,” *J. Lightw. Technol.*, vol. 32, no. 21, pp. 3345–3355, Nov. 2014.

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

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[8] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[10] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE ISIT*, Jun. 2009, pp. 2442–2446.

[11] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[13] H. Alves, R. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[14] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel," *IEEE Wirel. Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[15] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[16] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[17] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE ICC*, 2014, Jun. 2014, pp. 3342–3347.

[18] V. G. Sidorovich, "Optical countermeasures and security of free-space optical communication links," in *Proc. Eur. Symp. Opt. Photon. Defence Security*, 2004, pp. 97–108, Int. Soc. Opt. Photon.

[19] A. Puryear and V. Chan, "Using spatial diversity to improve the confidentiality of atmospheric free space optical communication," in *Proc.IEEE GLOBECOM*, pp. 1–6, Dec. 2011.

[20] M. Agaskar and V. Chan, "Nulling strategies for preventing interference and interception of free space optical communication," in *Proc. IEEE ICC*, Jun. 2013, pp. 3927–3932.

[21] J. M. Kahn and J. R. Barry, "Wireless infrared communications," *Proc. IEEE*, vol. 85, no. 265, pp. 265–298, Feb. 1997.

[22] 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.*, vol. 40, no. 8, pp. 1554–1562, 2001.

[23] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*. Bellingham, WA, USA: SPIE, 2005.

[24] S. Hranilovic, *Wireless Optical Communication Systems*. New York, NY, USA: Springer-Verlag, 2005.

[25] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[26] M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," *J. Opt. Commun. Netw.*, vol. 6, no. 8, pp. 684–694, Aug. 2014.

[27] S. Z. Denic, I. Djordjevic, J. Anguita, B. Vasic, and M. A. Neifeld "Information theoretic limits for free-space optical channels with and without memory," *J. Lightw. Technol.*, vol. 26, no. 19, pp. 3376–3384, Oct. 2008.

[28] N. Wang, X. Song, J. Cheng, and V. C. M. Leung, "Enhancing the security of free-space optical communications with secret sharing and key agreement," *J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1072–1081, Dec. 2014.

[29] L. C. Andrews, R. L. Phillips, C. Y. Hopen, and M. A. Al-Habash, "Theory of optical scintillation," *J. Opt. Soc. Amer. A*, vol. 16, no. 6, pp. 1417–1429, Jun. 1999.

[30] J. M. Garrido-Balsells, A. Jurado-Navas, J. F. Paris, M. Castillo-Vázquez, and A. Puerta-Notario, "Spatially correlated gamma-gamma scintillation in atmospheric optical channels," *Opt. Exp.*, vol. 22, no. 18, pp. 21820–21833, Sep. 2014.

[31] A. McKay, "A Bessel function distribution," *Biometrika*, vol. 24, no. 1/2, pp. 39–44, May 1932.

[32] H. Holm and M.-S. Alouini, "Sum and difference of two squared correlated Nakagami variates in connection with the McKay distribution," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1367–1376, Aug. 2004.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*. Orlando, FL, USA: Academic, 7th ed., 2007.

[34] I. I. Kim and E. J. Korevaar, "Availability of free-space optics (FSO) and hybrid FSO/RF systems," in *Proc. ITCom 2001: Int. Symp. Convergence IT Commun.*, 2001, pp. 1–12, Int. Soc. Opt. Photon.

[35] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[36] A. Chorti, S. M. Perlaza, H. Zhu, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.