On the Performance of Quantum Key Distribution FSO Systems Under a Generalized Pointing Error Model

Hui Zhao, *Student Member, IEEE,* and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—In this letter, the performance of a quantum key distribution (QKD) free-space optical (FSO) system is analyzed while taking a generalized pointing error model into account. More specifically, closed-form expressions for the average received powers at both the legitimate receiver and eavesdropper are derived. In addition, their corresponding asymptotic results valid in the high telescope gain regime are also presented. To capture the secure performance, we also investigate the ratio of received powers at the eavesdropper and at the legitimate receiver. Further, in some special cases, we find the optimal telescope gains for the received powers at both the legitimate receiver and eavesdropper, as well as the power ratio, which is important and useful for a secure QKD FSO system design. Finally, some selected numerical results are presented to illustrate the mathematical formalism and validate the accuracy of the derived analytical expressions.**

***Index Terms*—Free-space optical, generalized pointing errors, secure performance, and quantum key distribution.**

I. Introduction

To achieve confidential communications, a one-time-pad scheme was proposed by [1], where a secret key is shared between two legitimate parties. Due to the reliance only on the computational complexity, this traditional key distribution method is fundamentally insecure [2]. This is particularly true with the fast development of large-scale quantum computers over the last decade, which is making the current public key infrastructure more and more vulnerable [3]. In this context, quantum key distribution (QKD), a promising application of cryptography, provides unconditional security based on the law of quantum physics and quantum non-cloning theorem [4]. QKD can be implemented in two kinds of medium, namely optical fiber and free-space optical (FSO) links. Due to its cost-effectiveness, high-bandwidth availability, deployment flexibility and interference-immunity, FSO is an excellent choice for the terrestrial backhaul solution [1] and the feeder link of very high throughput satellites [2]. However, in the FSO systems, stochastic jitter and vibration of the pointing direction caused by atmospheric turbulence or building sway should be taken into account [5], [6], [7].

An inevitable drawback in the QKD FSO systems is backflash in the legitimate receiver side, when the legitimate receiver adopts a common detection method, relying on a single photon avalanche photodiode (SPAD) [8], [9], [10]. Indeed, with the SPAD detection scheme, an avalanche happens, resulting in the emission of a secondary photon, i.e., backflash, which can be captured by eavesdroppers. Kupferman and Arnon in [10] have recently presented an analytical framework to evaluate the impact of backflash on the performance of QKD FSO systems. However, in their investigation, the adopted model for the azimuth and elevation pointing error angles assumed zero mean and equal variance for both angles, and the pointing error angle at eavesdroppers was set to zero. However, for real life deployment, QKD FSO systems may have to operate under different and more general conditions. Further, the authors in [10] did not investigate the optimal point of the telescope gain to maximize the received power at the legitimate receiver.

In this letter, we consider a generalized pointing error model, in which the azimuth and elevation pointing error angles at the legitimate receiver have arbitrary and different mean and variance. In addition, we do not limit the pointing error angle at the eavesdropper to be very close to zero. Under this general setup, we are still able to offer closed-form expressions for the average received powers at both the legitimate receiver and eavesdropper. Moreover, the corresponding maximum point of the telescope gain are found in some special cases. To simplify the expressions and get obviously some additional insights, we also derive simple asymptotic expressions when the telescope gain is sufficiently large. Finally, the ratio of the received powers at the eavesdropper and legitimate receiver is analyzed, and the corresponding extreme point of the telescope gain is also obtained in a particular case of interest.

II. System Model

In an QKD FSO system, an absolutely static source (S) transmits an information photon to a destination (D) on a vibrating platform (such as a laser satellite), resulting in a random pointing error at D. Due to the avalanche of the SPAD detection method, a secondary photon will be emitted, called backflash, which can be detected by a third party, i.e., eavesdropper (E). This communications scenario is presented in Fig. 1 of [10].

The pointing error angle (θ) at D can be divided into two parts, i.e., $\theta = \sqrt{\theta_V^2 + \theta_H^2}$, where θ_H and θ_V are the azimuth and elevation pointing error angles, respectively. Like in [10], we assume that θ_H and θ_V are Gaussian random variables (RVs). However, we consider the general case in which these

Manuscript Received June 15, 2019; accepted July 9, 2019. This work was funded by the office of sponsored research (OSR) at KAUST. The work of H. Zhao was done while he was studying at KAUST. The associate editor coordinating the review of this paper and approving it for publication was M. Koca. (*Corresponding author: Hui Zhao.*)

H. Zhao was with the Computer, Electrical, and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia, and he is now with the Communication Systems Department, EURECOM, Sophia Antipolis 06410, France (email: hui.zhao@kaust.edu.sa).

M.-S. Alouini is with the Computer, Electrical, and Mathematical Science and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia (email: slim.alouini@kaust.edu.sa).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2019.2929037, IEEE Communications Letters

RVs are not necessarily with zero mean and the same variance. That is $\theta_V \sim \mathcal{N}\left(\mu_V, \sigma_V^2\right)$ and $\theta_H \sim \mathcal{N}\left(\mu_H, \sigma_H^2\right)$, where μ_V and σ_V^2 (or μ_H and σ_H^2) are the mean and variance of θ_V (or θ_H). In this case, it is well known that θ follows the Beckmann distribution [11], where the moment-generating function (MGF) of θ^2 is known to be given by [11]

$$\mathcal{M}_{\theta^2}\left(s\right) = \mathbb{E}\left\{\exp\left(s\theta^2\right)\right\} = \frac{\exp\left(\frac{\mu_V^2 s}{1-2\sigma_V^2 s} + \frac{\mu_H^2 s}{1-2\sigma_H^2 s}\right)}{\sqrt{\left(1-2\sigma_V^2 s\right)\left(1-2\sigma_H^2 s\right)}}, \tag{1}$$

where $\mathbb{E}\{\cdot\}$ represents the average operator. By setting some specific values for the parameters of the MGF of the Beckmann distribution in (6) of [12], the form of (1) can be also easily obtained.

III. Received Power at D

From [5], [10], the received power at D is given by

$$P_D\left(\theta\right) = K_1 G_D L\left(\theta\right), \tag{2}$$

where G_D is the telescope gain of D and $L\left(\theta\right) = \exp\left(-G_D\theta^2\right)$ is the corresponding pointing loss factor. In (2), K_1 is constant, depending on the system characteristic, given by

$$K_1 = \eta_q P_S \eta_S \eta_D \frac{L_A\left(D_1\right)}{D_1^2}\left(\frac{\lambda}{4\pi}\right)^2, \tag{3}$$

where η_q is the quantum efficiency, λ is the wavelength, P_S and G_S are the transmit power and telescope gain of S, respectively, $L_A(D_1)$ is the atmospheric loss with respect to the distance D_1, and η_S and η_D are the optical efficiencies at S and D, respectively.

The average received power at D with respect to θ can be written as

$$\begin{aligned}\overline{P}_D &= \mathbb{E}_\theta\left\{K_1 G_D L\left(\theta\right)\right\} = K_1 G_D \mathbb{E}_\theta\left\{\exp\left(-G_D\theta^2\right)\right\} \\ &= K_1 G_D \mathcal{M}_{\theta^2}\left(-G_D\right).\end{aligned} \tag{4}$$

Substituting the MGF of θ^2 in (1) into (4) yields

$$\overline{P}_D = \frac{K_1 G_D \exp\left(\frac{-G_D\mu_V^2}{1+2\sigma_V^2 G_D} + \frac{-G_D\mu_H^2}{1+2\sigma_H^2 G_D}\right)}{\sqrt{\left(1+2\sigma_V^2 G_D\right)\left(1+2\sigma_H^2 G_D\right)}}. \tag{5}$$

A. Asymptotic Result

When $G_D \to \infty$, we have

$$\begin{aligned}\lim_{G_D\to\infty}\overline{P}_D &= \lim_{G_D\to\infty}\frac{K_1 G_D \exp\left(\frac{-G_D\mu_V^2}{1+2\sigma_V^2 G_D} + \frac{-G_D\mu_H^2}{1+2\sigma_H^2 G_D}\right)}{\sqrt{\left(1+2\sigma_V^2 G_D\right)\left(1+2\sigma_H^2 G_D\right)}} \\ \simeq K_1 &\frac{\exp\left(-\frac{\mu_V^2}{2\sigma_V^2} - \frac{\mu_H^2}{2\sigma_H^2}\right)}{\sqrt{2\sigma_V^2 2\sigma_H^2}} = \frac{K_1}{2\sigma_V\sigma_H}\exp\left(-\frac{\mu_V^2}{2\sigma_V^2} - \frac{\mu_H^2}{2\sigma_H^2}\right),\end{aligned} \tag{6}$$

which shows a bound for $\overline{P}_D$. It implies when the telescope gain of D is sufficiently large, the received power at D reaches a constant asymptotic value.

B. Maximization of $\overline{P}_D$

When $\sigma_V = \sigma_H = \sigma$, taking the natural base of both sides in (5) yields

$$\begin{aligned}\ln\overline{P}_D = &\ln K_1 + \ln\left(\frac{G_D}{1+2\sigma^2 G_D}\right) \\ &- \frac{G_D\mu_V^2}{1+2\sigma^2 G_D} - \frac{G_D\mu_H^2}{1+2\sigma^2 G_D}.\end{aligned} \tag{7}$$

Let $x = \frac{G_D}{1+2\sigma^2 G_D}$ and $f(x) = \ln\overline{P}_D$. (7) can be further written as

$$f\left(x\right) = \ln K_1 + \ln x - \left(\mu_V^2 + \mu_H^2\right)x. \tag{8}$$

Let the first derivative of $f(x)$ with respect to x be equal to zero, and a unique stationary point can be obtained as

$$\frac{\partial f\left(x\right)}{\partial x} = \frac{1}{x} - \left(\mu_V^2 + \mu_H^2\right) = 0 \Rightarrow x^\star = \frac{1}{\mu_V^2 + \mu_H^2}. \tag{9}$$

From the first derivative of $f(x)$, we can easily see that for $x > x^\star$, $\frac{\partial f(x)}{\partial x} < 0$, and for $x < x^\star$, $\frac{\partial f(x)}{\partial x} > 0$. Therefore, $f(x)$ is an increasing function over $(0, x^\star)$, and a decreasing function over $(x^\star, +\infty)$. To summarize, $x^\star$ is the uniquely maximum point for $f(x)$. In view of the positive property of G_D and the function property of $x = \frac{G_D}{1+2\sigma^2 G_D}$, the corresponding optimal point G_D that maximizes $\overline{P}_D$ can be written as

$$G_D^\star = \begin{cases}\left(\mu_V^2 + \mu_H^2 - 2\sigma^2\right)^{-1}, & \text{if } \mu_V^2 + \mu_H^2 > 2\sigma^2; \\ +\infty, & \text{otherwise.}\end{cases} \tag{10}$$

IV. Received Power at E

The information intercept relies on the backflash, so the received power at E is given by [10]

$$P_E = P_D\left(\theta\right)K_2 L\left(\theta_E\right)G_D = K_1 K_2 G_D^2 L\left(\theta\right)L\left(\theta_E\right), \tag{11}$$

where $L\left(\theta_E\right) = \exp\left(-G_D\theta_E^2\right)$, $\theta_E = \sqrt{\left(\theta_V + \alpha\right)^2 + \theta_H^2}$, and α is the pointing direction error angle due to backflash. In (11), K_2 is given by

$$K_2 = \eta_f \eta_q \eta_B G_E \eta_E \frac{L_A\left(D_2\right)}{D_2^2}\left(\frac{\lambda}{4\pi}\right)^2, \tag{12}$$

where $L_A(D_2)$ is the atmospheric loss with respect to the distance D_2, and η_f, η_E and G_E are the backflash probability, optical efficiency and telescope gain of E, respectively.

The average received power at E can be written as

$$\begin{aligned}\overline{P}_E &= \mathbb{E}\left\{K_1 K_2 G_D^2 L\left(\theta\right)L\left(\theta_E\right)\right\} \\ &= K_1 K_2 G_D^2 \mathbb{E}\left\{\exp\left(-G_D\theta^2 - G_D\theta_E^2\right)\right\} \\ &= K_1 K_2 G_D^2 \mathbb{E}\left\{\exp\left(-G_D\left(2\theta_V^2 + 2\theta_H^2 + 2\alpha\theta_V + \alpha^2\right)\right)\right\},\end{aligned} \tag{13}$$

where the expectation term can be further written as

$$\begin{aligned}&\mathbb{E}\left\{\exp\left(-G_D\left(2\theta_V^2 + 2\theta_H^2 + 2\alpha\theta_V + \alpha^2\right)\right)\right\} \\ &= \exp\left(-G_D\alpha^2\right)\mathbb{E}\left\{\exp\left(-2G_D\left(\theta_V^2 + \theta_H^2 + \alpha\theta_V\right)\right)\right\} \\ &= \exp\left(-G_D\alpha^2\right)\mathbb{E}\left\{\exp\left(-2G_D\theta_H^2\right)\right\} \\ &\quad \mathbb{E}\left\{\exp\left(-2G_D\left(\theta_V^2 + \alpha\theta_V\right)\right)\right\}.\end{aligned} \tag{14}$$

By using the probability density functions of θ_V and θ_H, closed-form expressions for the two expectation operators in (14) can be derived as

$$\begin{aligned}&\mathbb{E}_{\theta_E}\left\{\exp\left(-2G_D\left(\theta_V^2+\alpha\theta_V\right)\right)\right\}\\ &=\frac{\exp\left(-\frac{\mu_V^2}{2\sigma_V^2}\right)}{\sqrt{4G_D\sigma_V^2+1}}\exp\left(\frac{\left(2\alpha G_D-\frac{\mu_V}{\sigma_V^2}\right)^2}{8G_D+\frac{2}{\sigma_V^2}}\right),\end{aligned} \tag{15}$$

$$\begin{aligned}&\mathbb{E}_{\theta_E}\left\{\exp\left(-2G_D\theta_H^2\right)\right\}\\ &=\frac{\exp\left(-\frac{\mu_H^2}{2\sigma_H^2}\right)}{\sqrt{4\sigma_H^2G_D+1}}\exp\left(\frac{\left(\frac{\mu_H}{\sigma_H^2}\right)^2}{8G_D+\frac{2}{\sigma_H^2}}\right),\end{aligned} \tag{16}$$

respectively.

A closed-form expression for $\overline{P}_E$ can finally be derived for arbitrary μ_V, μ_H, σ_V, σ_H, and α as

$$\begin{aligned}\overline{P}_E=&\frac{K_1K_2G_D^2\exp\left(-\frac{\mu_V^2}{2\sigma_V^2}-\frac{\mu_H^2}{2\sigma_H^2}\right)}{\sqrt{\left(4G_D\sigma_V^2+1\right)\left(4\sigma_H^2G_D+1\right)}}\\ &\exp\left(\frac{\left(2\alpha G_D-\frac{\mu_V}{\sigma_V^2}\right)^2}{8G_D+\frac{2}{\sigma_V^2}}+\frac{\left(\frac{\mu_H}{\sigma_H^2}\right)^2}{8G_D+\frac{2}{\sigma_H^2}}-G_D\alpha^2\right).\end{aligned} \tag{17}$$

A. Special Cases

If $\alpha=0$, which means that E is in the vicinity of S, $\overline{P}_E$ becomes

$$\begin{aligned}\overline{P}_E&=K_1K_2G_D^2\mathbb{E}\left\{\exp\left(-2G_D\left(\theta_V^2+\theta_H^2\right)\right)\right\}\\ &=\frac{K_1K_2G_D^2\exp\left(\frac{-2\mu_V^2G_D}{1+4\sigma_V^2G_D}-\frac{2\mu_H^2G_D}{1+4\sigma_H^2G_D}\right)}{\sqrt{\left(1+4\sigma_V^2G_D\right)\left(1+4\sigma_H^2G_D\right)}}.\end{aligned} \tag{18}$$

In the $\alpha=0$ case, when $G_D\to+\infty$, $\overline{P}_E$ is approximately equal to

$$\begin{aligned}&\lim_{G_D\to+\infty}\frac{K_1K_2G_D^2\exp\left(\frac{-2\mu_V^2G_D}{1+4\sigma_V^2G_D}-\frac{2\mu_H^2G_D}{1+4\sigma_H^2G_D}\right)}{\sqrt{\left(1+4\sigma_V^2G_D\right)\left(1+4\sigma_H^2G_D\right)}}\\ &\simeq\frac{K_1K_2\exp\left(-\frac{\mu_V^2}{2\sigma_V^2}-\frac{\mu_H^2}{2\sigma_H^2}\right)}{4\sigma_V\sigma_H}G_D,\end{aligned} \tag{19}$$

which shows that $\overline{P}_E$ is approximately proportional to G_D for $G_D\to+\infty$ and $\alpha=0$.

B. Maximization of $\overline{P}_E$

For $\mu_V=\mu_H=0$ and $\sigma_V=\sigma_H=\sigma$, $\overline{P}_E$ can be simplified as

$$\overline{P}_E=\frac{K_1K_2G_D^2}{4\sigma^2G_D+1}\exp\left(\frac{2\sigma^2\alpha^2G_D^2}{4\sigma^2G_D+1}-G_D\alpha^2\right). \tag{20}$$

The first derivative of $\overline{P}_E$ with respect to G_D is given by (21), where the positive or negative value depends only on the last term, i.e.,

$$\begin{aligned}\Theta=&-16\sigma^4\alpha^2G_D^3+\left(32\sigma^4-8\sigma^2\alpha^2\right)G_D^2\\ &+\left(24\sigma^2-2\alpha^2\right)G_D+4,\end{aligned} \tag{22}$$

which is a standard univariate cubic equation with respect to G_D. If σ and α are known, we can easily find the roots for $\Theta=0$ and the positive and negative value intervals for $\frac{\partial\overline{P}_E}{\partial G_D}$, and thereby finding the extreme points for $\overline{P}_E$. Specially, when $G_D=0$, $\Theta=4$ is positive, so over $G_D\in(0,+\infty)$, $\overline{P}_E$ must increase first. The trend and extreme point of $\overline{P}_E$ are very useful and important for the secure system design.

V. Ratio of $\overline{P}_E$ to $\overline{P}_D$

An important metric for the secure analysis is the ratio of $\overline{P}_E$ to $\overline{P}_D$, which can be easily derived by using the closed-form expressions for $\overline{P}_E$ and $\overline{P}_D$, is given by

$$\begin{aligned}\Delta=&\frac{\overline{P}_E}{\overline{P}_D}=\frac{K_2G_D\sqrt{\left(1+2\sigma_V^2G_D\right)\left(1+2\sigma_H^2G_D\right)}}{\sqrt{\left(4\sigma_V^2G_D+1\right)\left(4\sigma_H^2G_D+1\right)}}\\ &\exp\left(-\frac{\mu_V^2}{2\sigma_V^2}-\frac{\mu_H^2}{2\sigma_H^2}\right)\exp\left(\frac{G_D\mu_V^2}{1+2\sigma_V^2G_D}+\frac{G_D\mu_H^2}{1+2\sigma_H^2G_D}\right)\\ &\exp\left(\frac{\left(2\alpha G_D-\frac{\mu_V}{\sigma_V^2}\right)^2}{8G_D+\frac{2}{\sigma_V^2}}+\frac{\left(\frac{\mu_H}{\sigma_H^2}\right)^2}{8G_D+\frac{2}{\sigma_H^2}}-\alpha^2G_D\right).\end{aligned} \tag{23}$$

This expression is relatively complicated, and does not provide us some useful insights for the secure system design. Here, we consider some special cases to analyze this ratio.

For $\mu_V=\mu_H=0$ and $\sigma_V=\sigma_H=\sigma$, the expression for Δ can be simplified as

$$\Delta=\frac{\left(1+2\sigma^2G_D\right)K_2G_D}{4\sigma^2G_D+1}\exp\left(\frac{\alpha^2G_D^2}{2G_D+\frac{1}{2\sigma^2}}-\alpha^2G_D\right). \tag{24}$$

The first derivative of Δ with respect to G_D is shown in (25), where the positive or negative value of $\frac{\partial\Delta}{\partial G_D}$ depends only on Θ_2, a standard univariate quartic equation. If α and σ are known, the roots for $\Theta_2=0$ can be easily derived, and the positive and negative value intervals can be also determined. Thus, we can analyze the changing trend of Δ and derive the extreme points.

When $\alpha=0$, $\mu_V=\mu_H=0$ and $\sigma_V=\sigma_H=\sigma$, Δ becomes

$$\Delta=\frac{\left(1+2\sigma^2G_D\right)K_2G_D}{4\sigma^2G_D+1}. \tag{26}$$

The first derivative of Δ with respect to G_D in (26) is

$$\frac{\partial\Delta}{\partial G_D}=\frac{K_2+4\sigma^2K_2G_D^2+8\sigma^4K_2G_D^2\left(2G_D-1\right)}{\left(4\sigma^2G_D+1\right)^2}. \tag{27}$$

It is obvious that for $G_D>\frac{1}{2}$, $\frac{\partial\Delta}{\partial G_D}$ must be positive. As $G_D\gg1$ in the most practical cases, we can treat $\frac{\partial\Delta}{\partial G_D}$ as a positive value, and therefore, Δ always increases as G_D grows. If G_D is sufficiently large, Δ can be approximately obtained by

$$\Delta\simeq\frac{K_2G_D}{2}. \tag{28}$$

$$\frac{\partial \overline{P}_E}{\partial G_D} = \frac{K_1 K_2 G_D \exp\left(-\frac{\alpha^2 G_D \left(4\sigma^2 G_D + 2\right)}{8\sigma^2 G_D + 2}\right)}{2\left(4\sigma^2 G_D + 1\right)^3} \left[-\left(4\sigma^2\right)^2 \alpha^2 G_D^3 + \left(2\left(4\sigma^2\right)^2 - 2\cdot 4\sigma^2\alpha^2\right) G_D^2 + \left(6\cdot 4\sigma^2 - 2\alpha^2\right) G_D + 4\right]. \tag{21}$$

$$\frac{\partial \Delta}{\partial G_D} = \frac{K_2 \exp\left(-\frac{\alpha^2 G_D \left(2\sigma^2 G_D + 1\right)}{4\sigma^2 G_D + 1}\right)}{\left(4\sigma^2 G_D + 1\right)^3} \underbrace{\left[-16\alpha^2\sigma^6 G_D^4 - \left(16\sigma^4\alpha^2 - 32\sigma^6\right) G_D^3 - \left(6\sigma^2\alpha^2 - 24\sigma^4\right) G_D^2 - \left(\alpha^2 - 8\sigma^2\right) G_D + 1\right]}_{\Theta_2}. \tag{25}$$

VI. Numerical Results

To simplify the parameter setting, $D_1 = D_2 = 900$ km, $L_A(D1) = L_A(D2) = 0.5$, $\lambda = 780$ nm, $P_S = 0$ dB, $G_S = G_E = 10^{11}$, $\eta_f = 0.04$, $\eta_q = 0.1$, and $\eta_S = \eta_D = 0.9$ are assumed in the following simulation results. In each Monte-Carlo simulation result, 10^7 realizations are generated to get the corresponding average value according to the statistical properties, i.e., μ_V, μ_H, σ_V and σ_H.

As shown in Fig. 1, the received power at D increases as G_D grows, due to the improved telescope gain. When G_D is sufficiently large, $\overline{P}_D$ reaches an asymptotic bound, as proved in (6). It is obvious that $\overline{P}_D$ is improved with increasing μ_H, because a smaller μ_H means a better pointing direction. The maximum points are also marked in Fig. 1, which are derived from the maximization analysis for $\overline{P}_D$, where the maximum points for $\mu_V^2 + \mu_H^2 < 2\sigma^2$ are infinity.

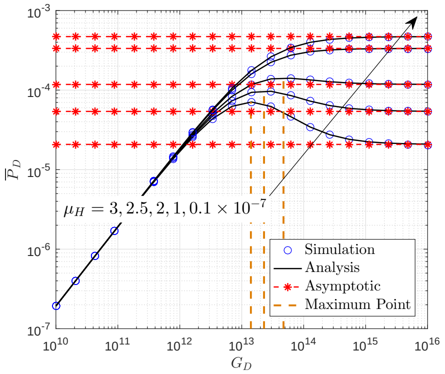

Fig. 1. $\overline{P}_D$ versus G_D with various values of μ_H for $\sigma_V^2 = \sigma_H^2 = 1.44 \times 10^{-14}$, and $\mu_V = 1 \times 10^{-7}$.

Fig. 2 plots $\overline{P}_E$ versus G_D for different values of α. $\overline{P}_E$ for $\alpha > 0$ increases first, and reaches a vertex before a sharp decline, while $\overline{P}_E$ for $\alpha = 0$ always increases with increasing G_D, where the asymptotic results are derived by (19). When G_D is sufficiently large, $\overline{P}_E$ becomes lower as α grows, because a larger α means a larger distance between the transmitter and eavesdropper. The maximum points in Fig. 2 are obtained in the analysis of Subsection IV-B.

To validate the correctness of (17) for the general pointing errors, we also vary the values of μ_V and σ_V^2 in Figs. 3-4, respectively. From Figs. 3-4, we can easily see that a large μ_V (or σ_V^2) results in a larger $\overline{P}_E$. More specifically, $\overline{P}_E$ under different values of μ_V almost converges in the low and high G_D regions, and the gap is only obvious in the medium G_D region. In the σ_V^2 changing case, the gap of $\overline{P}_E$ under different σ_V^2 becomes larger with increasing G_D.

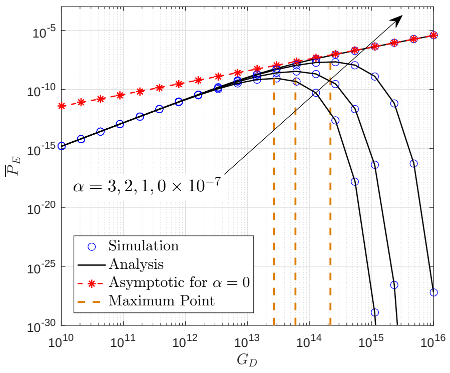

Fig. 2. $\overline{P}_E$ versus G_D with various values of α for $\sigma_V^2 = \sigma_H^2 = 1 \times 10^{-14}$, and $\mu_V = \mu_H = 0$.

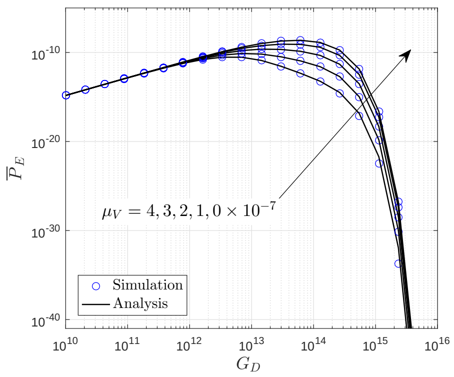

Fig. 3. $\overline{P}_E$ versus G_D with various values of μ_V for $\sigma_V^2 = \sigma_H^2 = 1 \times 10^{-14}$, $\mu_H = 1 \times 10^{-7}$, and $\alpha = 2 \times 10^{-7}$.

In Fig. 5, Δ for $\alpha > 0$ increases first before achieving a vertex after which this figure is rapidly falling, rather than a continuous growth in the figure for $\alpha = 0$, where the asymptotic results are obtained by (28). The maximum points for (24) are also presented in Fig. 5, where the decreasing trend of maximum points are obvious with increasing α.

To present more general pointing error cases, we consider

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LCOMM.2019.2929037, IEEE Communications Letters

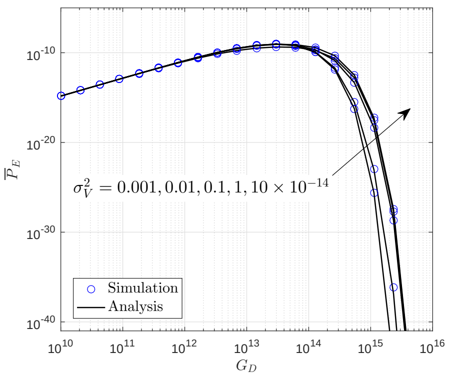

Fig. 4. $\overline{P}_E$ versus G_D with various values of σ_V^2 for $\sigma_H^2 = 1 \times 10^{-14}$, $\mu_V = \mu_H = 1 \times 10^{-7}$, and $\alpha = 2 \times 10^{-7}$.

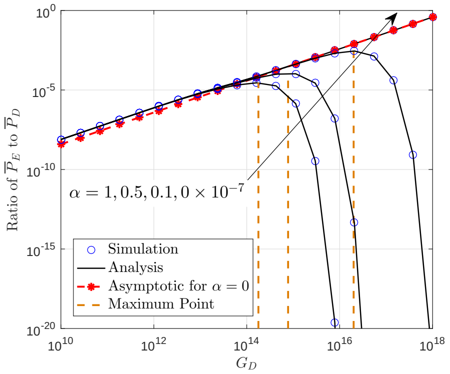

Fig. 5. Δ versus G_D with various values of α for $\sigma_V^2 = \sigma_H^2 = 1 \times 10^{-14}$, and $\mu_V = \mu_H = 0$.

different values of μ_V and μ_H, and set the same variance of θ_V and θ_H in Fig. 6. There is an increasing trend of Δ as the variance grows, although the difference of Δ among different variances is not obvious in the low G_D region.

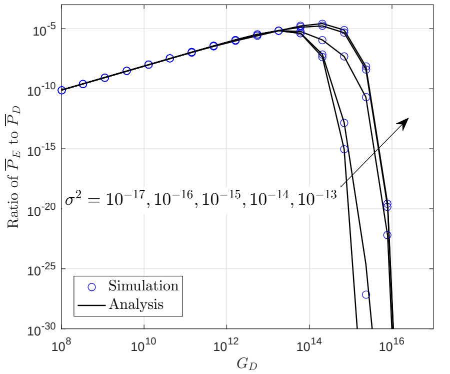

Fig. 6. Δ versus G_D with various values of $\sigma_V^2 = \sigma_H^2 = \sigma^2$ for $\mu_V = 1 \times 10^{-7}$, $\mu_H = 0$, and $\alpha = 1 \times 10^{-7}$.

VII. Conclusion

In this letter, closed-form expressions for $\overline{P}_D$, $\overline{P}_E$, and Δ were derived, and simplified expressions in some special cases were also given. To get more design insights, we performed an analytical maximization for $\overline{P}_D$, $\overline{P}_E$, and Δ based on some special settings of some selected parameters. In the numerical section, we used the Monte-Carlo simulations to validate the correctness of our newly derived expressions. From both the derived expressions and numerical results, we can get some design guidelines for the telescope gain at the legitimate receiver to achieve a specific purpose, shown as follows:

- If the legitimate receiver only wants to improve its received power (without taking the eavesdropper into account) in the $\sigma_V^2 = \sigma_H^2$ case, the optimal G_D can be found by (10), which depends on the parameter setting, i.e., may not just make G_D as large as possible (shown in Fig. 1).
- If we only want to make $\overline{P}_E$ lower, the legitimate receiver should avoid the optimal G_D for $\overline{P}_E$, where the impact of $\overline{P}_D$ is neglected due to the priority of security. From Fig. 2, we should make G_D as small (or large) as possible to avoid the vertex for $\alpha \neq 0$. When $\alpha = 0$, decreasing G_D is the only way to get better security.
- If we need to balance the received power performance between the legitimate receiver and eavesdropper, Δ should be taken into account, which reflects the joint effect of G_D on $\overline{P}_D$ and $\overline{P}_E$. From Figs. 5-6, to make $\overline{P}_D$ larger and $\overline{P}_E$ smaller for $\alpha \neq 0$, the legitimate receiver can increase G_D until arriving to a specific threshold. If $\alpha = 0$, we have no choice but to decrease G_D.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656-715, 1949.

[2] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over FSO: Current development and future perspectives," in *Proc. Electromagnetics Research Symposium (PIERS-Toyama)*, Aug. 2018, pp. 1672-1679.

[3] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116-120, 2017.

[4] K. Inoue, "Quantum key distribution technologies," *IEEE J. Sel. Topics Quantum Electron.*, vol. 12, no. 4, pp. 888-896, Aug. 2006.

[5] S. Arnon, "Effects of atmospheric turbulence and building sway on optical wireless-communication systems," *Opt. Lett.*, vol. 28, no. 2, pp. 129-131, Jan. 2003.

[6] I. S. Ansari, M.-S. Alouini, and J. Cheng, "Ergodic capacity analysis of free-space optical links with nonzeros boresight pointing errors," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4248-4264, Aug. 2015.

[7] H. AlQuwaiee, H.-C. Yang, and M.-S. Alouini, "On the asymptotic capacity of dual-aperture FSO systems with generalzied pointing error model," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6502-6512, Sep. 2016.

[8] A. Lacaita, S. Cova, A. Spinelli, and F. Zappa, "Photon-assisted avalanche spreading in reach-through photodiodes," *Appl. Phys. Lett.*, vol. 62, no. 6, pp. 606-608, Feb. 1993.

[9] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," *Light Sci. Appl.*, vol. 6, no. pp. e16261, 2017.

[10] J. Kupferman, and S. Arnon, "Zero-error attacks on a quantum key distribution FSO system," *OSA Continuum*, vol. 1, no. 3, pp. 1079-1086, Nov. 2018.

[11] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*. New York, NY, USA: Wiley, 2000.

[12] P. Pena-Martin, J. M. Romero-Jerez, and F. J. Lopez-Martinez, "Generalized MGF of Beckmann fading with applications to wireless communications performance analysis," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3933-3943, Sep. 2017.