Performance of Free-Space QKD Systems using SIM/BPSK and Dual-Threshold/Direct-Detection

Phuc V. Trinh[1], Thanh V. Pham[1], Hung V. Nguyen[2], Soon Xin Ng[2], and Anh T. Pham[1]
[1]Computer Communications Laboratory, The University of Aizu, Japan 965-8580.
[2]School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.
Emails: phuc.v.trinh@ieee.org, m5182108@u-aizu.ac.jp, {hvn08r, sxn}@ecs.soton.ac.uk, pham@u-aizu.ac.jp

***Abstract*—This paper proposes a novel free-space quantum key distribution (QKD) system using subcarrier intensity-modulation (SIM) binary phase-shift-keying (BPSK) and dual-threshold/direct-detection (DT/DD) receiver with an avalanche photodiode (APD). The proposed system enables the adoption of well-developed analytical models in conventional free-space optical (FSO) communications and achieves the QKD function with a simple configuration. We analytically investigate the design criteria for transmitter and receiver, in particular, the modulation depth and the setting for dual-threshold in the context of security requirement of QKD systems. The quantum bit error rate (QBER) and the ergodic secret-key rate of the proposed system are analytically derived in closed-form expressions, considering the channel loss, atmospheric turbulence modeled by the log-normal distribution, and receiver noises. Monte-Carlo (M-C) simulations are also implemented to validate the analytical results, and numerical results confirm the feasibility of the proposed system.**

I. Introduction

Quantum key distribution (QKD) is one of the primary and well-developed applications of quantum communications that allows secret keys sharing between two parties (respectively, named Alice and Bob) in the presence of eavesdropper(s) [1]. The first QKD protocol, widely known as BB84 protocol, was proposed by Bennett and Brassard [2], by which the legitimate sender (Alice) and receiver (Bob) can achieve the secret-key sharing by the use of randomly generated signals using non-orthogonal quantum states. Over the years, two major implementation methods of QKD protocol, namely discrete variable (DV) and continuous variable (CV), have been proposed. While the key information is encoded on the properties of single photons such as the phase or polarization in DV-QKD systems [3], the quadrature variables of coherent states are used in CV-QKD [4]. Compared to DV-QKD, CV-QKD is much easier to implement as it is compatible with the standard optical telecommunication technologies and enables higher key generation rates by using heterodyne/homodyne detection instead of the single-photon counters. CV-QKD scheme has been theoretically studied and experimentally implemented both over optical fiber [5]-[8] and free-space optical (FSO) links [9]-[12].

The key issue with CV-QKD system comes from the heterodyne/homodyne detection receiver, which results in high cost due to the requirement of the sophisticated phase-stabilized local light at the receiver. To further simplify CV-QKD systems, intensity modulation with dual-threshold/direct detection (DT/DD) over *fiber* CV-QKD systems has been recently proposed employing on-off keying (OOK) with PIN receivers [13]. The channel-state information (CSI) is required at the receiver to optimize the dual thresholds, and CSI estimation can be easily done in the optical fiber environment due to the non-fading channel characteristics.

In this paper, we propose a novel *free-space* CV-QKD system using DT/DD and subcarrier-intensity modulation binary phase-shift-keying (SIM/BPSK) signaling. Practically, CSI estimation over fading channels in case of OOK signaling is complicated due to the asymmetry of binary signals (noise variances are different in bits "0" and "1"). Therefore, the use of SIM/BPSK signaling whose signals of bit "0" and "1" are symmetric over the "zero" level will relax the CSI estimation over the atmospheric fading channels. To confirm the feasibility of the proposed system, we analytically investigate the criteria for transmitter and receiver settings, especially, the modulation depth and the selection of values for the dual-threshold to maintain the security in QKD systems. Also, we analytically study the performance of the proposed system by deriving, in closed-form expressions, the quantum bit-error rate (QBER) and the ergodic secret-key rate, taking into account effects of atmospheric channel and receiver noises. In the performance analysis, the log-normal distribution is adopted to model the atmospheric turbulence, and the impact of different channel conditions on the QBER and the ergodic secret-key rate is comprehensively discussed. Monte-Carlo (M-C) simulations are also implemented to confirm the validity of the analytical results.

The remainder of this paper is organized as follows. Section II first revisits the BB84 QKD protocol and then highlights the design concept and the proposed system model. The atmospheric channel model is described in Section III. In Section IV, the system performance is theoretically analyzed, and selected numerical results are discussed in Section V. Finally, we conclude the paper in Section VI.

II. Design Concept and Proposed System Model

A. BB84 Protocol

The conventional BB84 QKD protocol can be described in four steps as follows.

Step 1: Alice randomly chooses between two linear polarization bases $\bigoplus$ or $\bigotimes$ for every bit that she wants to send.

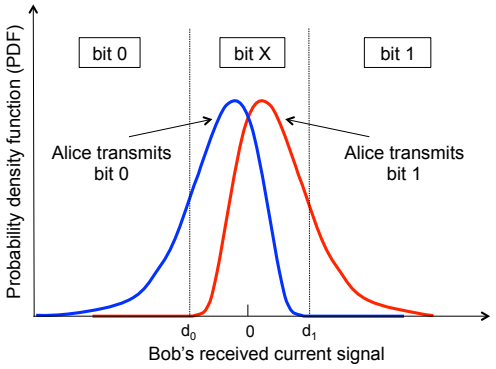

Fig. 1. The probability density function (PDF) of Bob's received signal over turbulence fading channel, d_0 and d_1 are two levels of the DT.

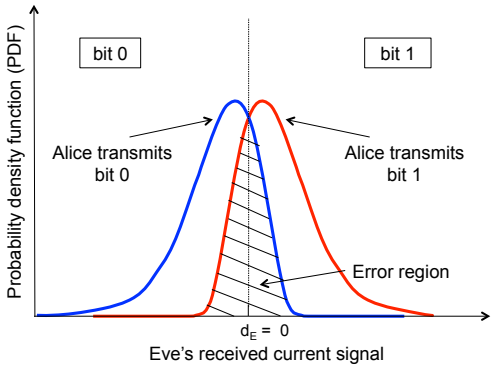

Fig. 2. The probability density function (PDF) of Eve's received signal over turbulence fading channel with the optimal threshold d_E.

For each chosen basis, Alice sends a random bit value, "0" or "1", using the following set of polarization codes

$$0 \rightarrow \begin{cases} 0^\circ & \text{if } \oplus \text{ was chosen} \\ -45^\circ & \text{if } \otimes \text{ was chosen,} \end{cases} \quad (1)$$

$$1 \rightarrow \begin{cases} 90^\circ & \text{if } \oplus \text{ was chosen} \\ 45^\circ & \text{if } \otimes \text{ was chosen.} \end{cases} \quad (2)$$

Step 2: At the receiver, Bob *randomly* selects a basis to measure each photon and has a detection only if he chooses the same basis as Alice. Bob then assigns the corresponding bit values to detected photons.

Step 3: Through a public channel, Alice broadcasts her basis choice for each bit of her raw key, but not the bit value. Bob then reveals on which detected photons he used the same basis (without revealing the bit value he assigned to each one). They both discard photon measurements where Bob used a different basis, which is 50% on average, leaving the remaining bits as their ***sifted keys***.

Step 4: In practice, Bob's sifted key may contain errors due to eavesdropping or channel/detector imperfections. To identify and remove the erroneous bits, Alice and Bob perform *information reconciliation* over the public channel, which is a form of error correction to ensure both sifted keys are identical, forming their error-free ***secret key***.

The security of BB84 protocol, according to the laws of quantum mechanics, lies in the fact that Alice encodes her information in ***non-orthogonal*** states $\oplus$ or $\otimes$ so that an eavesdropper Eve cannot sufficiently distinguish the two states and errors unavoidably occur when she eavesdrops [14].

B. Design Concept

In this section, we describe the design concept for the implementation of QKD by using SIM/BPSK signaling and DT/DD. Details are as follows.

Step 1: Alice transmits SIM/BPSK modulated signals with small modulation depth, corresponding to binary random numbers "0" or "1", over the free-space channel.

Step 2: The modulated signals are directly detected at Bob's receiver. Fig. 1 shows the probability density function (PDF) of Bob's received BPSK signal after the DD by an avalanche photodiode (APD). Two levels of the DT, d_0 and d_1, are symmetric over the "zero" level. The distribution of the received signal has two peaks corresponding to Alice's bit "0" and bit "1", which overlap with each other as the modulation depth is small. For the detected value x, the detection rule can be expressed as

$$\text{Decision} = \begin{cases} 0 & \text{if } (x \leq d_0) \\ 1 & \text{if } (x \geq d_1) \\ \text{X} & \text{otherwise,} \end{cases} \quad (3)$$

where X represents the case that Bob creates no bit, which corresponds to the case of wrong basis selection in the BB84 protocol.

Step 3: Using a classical channel, Bob notifies Alice of the time he created bits from detected signals. Now, Alice and Bob share an identical bit string, which is the ***sifted key***. By adjusting d_0 and d_1 in *Step 2,* and obtaining the CSI estimation at the receiver, the probability of sift can be controlled.

Step 4: As in the BB84 protocol, further information reconciliation can then be implemented over the public channel to obtain the error-free ***secret key***.

The security of this design concept can be explained as follows. *Firstly*, the modulation depth of the SIM/BPSK signal is very small. As a result, if Eve, in the beam-splitting attack for example, tries to decode the key using the optimal threshold (which is d_E at "zero" as illustrated in Fig. 2 in case

	DV-QKD	CV-QKD	Non-Coherent CV-QKD
Source	Weak laser pulse (single-photon)	Laser	Laser
Modulation	Polarization	Phase	Intensity
Detection	Single-photon detection	Coherent detection	Direct detection detectors
Complexity	Very high	High	Low
Cost	Very high	High	Low
Compatibility with Standard Technologies	No	Yes	Yes
Key Rate	Low	High	High
Free-space operation	Near-field	Far-field	Far-field

Fig. 3. Comparison between different QKD technologies.

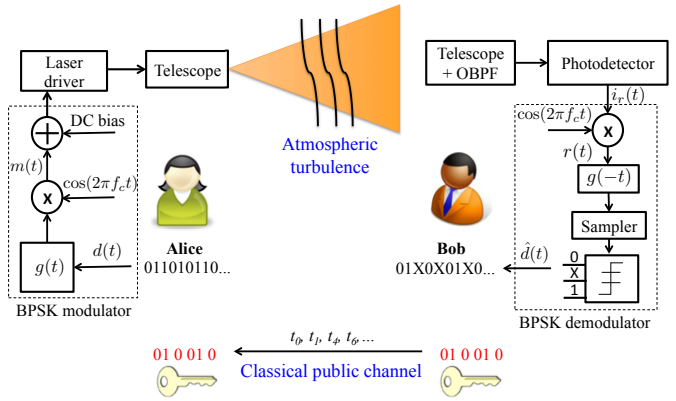

Fig. 4. Block diagram of the proposed free-space QKD system using SIM/BPSK and APD receiver.

of SIM/BPSK), she will suffer from a high error rate. With a proper setting of the modulation depth at the transmitter design, we can guarantee that Eve's error rate can be close to the probability that Eve chooses the incorrect basis in BB84 protocol. *Secondly*, as mentioned in *Steps 2* and *3*, the probability of sift can also be controlled by Bob via the DT setting. Additionally, Eve's signal fluctuation is uncorrelated with Bob's since they arise from quantum noise and channel fading. In case of intercept-resend eavesdropping by Eve, the probability that Alice and Bob identify the presence of Eve is sufficiently high with short key length (further discussions on this issue with validated data will be provided in Section V - Numerical Results).

Figure 3 summarizes key characteristics of the proposed system in comparison with DV-QKD and CV-QKD systems. The key features of the proposed system include simplicity and cost-efficiency, since phase-stabilized local laser or expensive single-photon detector is not required. In particular, Intensity Modulation/Direct Detection (IM/DD) systems are commercially available for high data rate, i.e., Gigabits per second (Gbps) and most advantageous for single-wavelength data transmission over short distances.

C. Proposed System Model

Figure 4 presents a block diagram of the proposed free-space CV-QKD system using SIM/BPSK and DT/DD receiver with an APD. At the transmitter, the source data $d(t)$ is first modulated onto a radio frequency (RF) subcarrier signal using BPSK scheme in which bits "0" and "1" are represented by two different phases 180° apart. The subcarrier signal $m(t)$ is sinusoidal having both positive and negative values; therefore a DC bias is added to $m(t)$ before it is used to modulate a continuous-wave laser beam.

Let $P_t(t)$ denote the transmitted power of the modulated laser beam, we have $P_t(t) = \frac{P}{2}[1+\delta m(t)]$, where P represents the peak transmitted power, δ is the intensity modulation depth to avoid overmodulation ($-1 < \delta m(t) < 1$). $m(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$, where $A(t)$ is the subcarrier amplitude, $g(t)$ is the rectangular pulse shaping function, f_c is the subcarrier frequency, and $a_i \in [0,1]$ represents the ith binary data. For the sake of simplicity, we normalize the power of $m(t)$ to unity.

At the receiver, the incoming optical field is passed through an optical bandpass filter (OBPF) before being converted into an electrical signal through DD at the APD. A standard RF coherent demodulator is employed to recover the source data $\hat{d}(t)$. Over an atmospheric channel with channel coefficient $h(t)$, the electrical signal at the output of the APD at the receiver can be written as

$$i_r(t) = \Re\bar{g}\frac{P}{2}h(t)[1+\delta\cos(2\pi f_c t + a_i\pi)] + n(t), \quad (4)$$

where $\Re = \frac{\eta q}{\tilde{h}v}$ is the responsivity (in units of A/W) of the APD with η is the quantum efficiency, q is the electron charge, $\tilde{h}$ is the Planck's constant, v is the optical frequency; $\bar{g}$ is the APD average gain, and $n(t)$ is the receiver noise. For BPSK demodulation, the output signal $r(t)$ is demodulated by the reference signal $\cos(2\pi f_c t)$ as

$$r(t) = \overline{i_r(t)\cos(2\pi f_c t)} = \begin{cases} i_0 = -\frac{1}{4}\Re\bar{g}P\delta h(t) + n(t) \\ i_1 = \frac{1}{4}\Re\bar{g}P\delta h(t) + n(t) \end{cases}, \quad (5)$$

where i_0 and i_1 represent the received current signals for bit "0" and bit "1", respectively. Assuming that the dark current is negligible, the receiver noises composing of shot noise, background noise and thermal noise can be modeled as additive white Gaussian noises (AWGN) with high accuracy [15]. Thus, $n(t)$ is the zero-mean AWGN with variance $\sigma_N^2 = \sigma_{sh}^2 + \sigma_b^2 + \sigma_{th}^2$, where σ_{sh}^2, σ_{bkg}^2, and σ_{th}^2 are respectively the variances of the APD shot noises caused by the received signal and background radiation, and receiver thermal noise, which can be expressed as

$$\sigma_{sh}^2 = 2q\bar{g}^2\Re F_A\left(\frac{1}{4}P\delta h\right)\Delta_f, \quad (6)$$

$$\sigma_b^2 = 2q\bar{g}^2\Re F_A P_b\Delta_f, \quad (7)$$

$$\sigma_{th}^2 = \frac{4k_B T F_n}{R_L}\Delta_f, \quad (8)$$

where $F_A = k_A\bar{g} + \left(2 - \frac{1}{\bar{g}}\right)(1-k_A)$ denotes the excess noise factor with k_A is the ionization factor, F_n is the amplifier noise figure, P_b is the average received background radiation power, $\Delta_f = \frac{R_b}{2}$ with R_b is the system bit rate, T is the receiver temperature in Kelvin degree, and R_L is the APD's load resistance. After demodulating process, the sampled electrical signal at the output of the receiver is used to reproduce the source transmitted binary bits "0" and "1" based on DT/DD as described in Section II-B.

III. Atmospheric Channel Models

In our model, the channel coefficient h can be described as $h = h^l h^t$, where h^l is the channel loss including atmospheric attenuation and geometric spreading loss, and h^t is the atmospheric turbulence-induced fading.

The channel loss can be formulated as

$$h^l = \frac{A}{\pi\left(\frac{\theta}{2}L\right)^2}\exp(-\beta_l L), \quad (9)$$

in which $A = \pi(D/2)^2$ is the area of the receiver aperture with D is the diameter, θ is the angle of divergence, β_l is the attenuation coefficient, and L is the transmission distance in kilometers [16]-[17].

Inhomogeneities in the temperature and pressure of the atmosphere lead to refractive index variations along the transmission path, which is commonly known as *atmospheric turbulence*. In this paper, the log-normal distribution model is adopted. Thus, the distribution of turbulence-induced fading coefficient h^t can be expressed as [18]

$$f_{h^t}(h^t) = \frac{1}{\sqrt{8\pi}h^t\sigma_x} \exp\left(-\frac{\left[\ln(h^t) - 2\mu_x\right]^2}{8\sigma_x^2}\right), \quad (10)$$

where μ_x and σ_x^2 are the mean and standard variance of log-amplitude fluctuation. To ensure that the fading does not attenuate or amplify the average power, we normalize the fading coefficient so that $\mathbb{E}[h^t] = 1$, with $\mathbb{E}[\cdot]$ denotes the statistical expectation. Doing so requires the choice of $\mu_x = -\sigma_x^2$. Assuming plane wave propagation, σ_x^2 can be given as [16]

$$\sigma_x^2 = 0.307\left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2, \quad (11)$$

where λ is the wavelength and L is the transmission distance in meters. C_n^2 stands for the refractive index structure coefficient.

IV. Performance Analysis

A. Quantum Bit Error Rate

The quantum bit error rate (QBER) is given as [3]

$$\text{QBER} = \frac{P_{error}}{P_{sift}}, \quad (12)$$

where P_{error} and P_{sift} are the probabilities of error and sift, respectively. In the proposed system, P_{sift} corresponds to the probability that Bob can detect bits "0" and "1" using the dual-threshold detection, and P_{error} is the probability that Bob decides "0" when "1" is received and "1" when "0" is received. These probabilities can be calculated through the joint probabilities between Alice and Bob as $P_{sift} = P_{A,B}(0,0)+P_{A,B}(0,1)+P_{A,B}(1,0)+P_{A,B}(1,1)$, and $P_{error} = P_{A,B}(0,1) + P_{A,B}(1,0)$, where $P_{A,B}(a,b)$ $(a,b \in \{0,1\})$ denotes the joint probability that Alice's bit a coincides with Bob's bit b. Using two detection thresholds d_0 and d_1, the joint probabilities, averaged over the fading channel, can be expressed as

$$P_{A,B}(a,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{i_a - d_0}{\sigma_N}\right) f_{h^t}\left(h^t\right) dh^t, \quad (13)$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_1 - i_a}{\sigma_N}\right) f_{h^t}\left(h^t\right) dh^t, \quad (14)$$

where $a \in \{0,1\}$, $i_0 = -\frac{1}{4}\Re\bar{g}P\delta h^l h^t$ and $i_1 = -i_0$. $Q(\cdot) \triangleq \frac{1}{\sqrt{2\pi}}\int_0^\infty \exp(-t^2/2)dt$ is the Gaussian Q-function.

To determine d_0 and d_1, we propose the DT selections with $d_0 = \mathbb{E}[i_0] - \zeta\sqrt{\sigma_N^2}$, and $d_1 = \mathbb{E}[i_1] + \zeta\sqrt{\sigma_N^2}$, where ζ is the *dual-threshold scale coefficient* to adjust d_0 and d_1. This dual-threshold selections depend on the modulation depth δ and the variance of noise σ_N adjusted by ζ. $\mathbb{E}[i_0]$ and $\mathbb{E}[i_1]$ are the mean values of i_0 and i_1, respectively. Thus, $\mathbb{E}[i_0] = -\frac{1}{4}\Re\bar{g}P\delta h^l$ and $\mathbb{E}[i_1] = \frac{1}{4}\Re\bar{g}P\delta h^l$ as $\mathbb{E}[h] = \mathbb{E}[h^l h^a] = h^l$ with $\mathbb{E}[h^a] = 1$.

To derive the closed-form expressions for the joint probabilities in (13) and (14), using the Gauss-Hermite quadrature formula $\int_{-\infty}^{\infty} g(y)\exp(-y^2) \approx \sum_{i=-k,i\neq 0}^{k} \omega_i g(x_i)$ [19], we have

$$P_{A,B}(a,0) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k,i\neq 0}^{k} \omega_i Q\left(\frac{\mp\frac{1}{4}\Re\bar{g}P\delta e^{2\sqrt{2}\sigma_x x_i + 2\mu_x} - d_0}{\sigma_{N-i}}\right), \quad (15)$$

$$P_{A,B}(a,1) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k,i\neq 0}^{k} \omega_i Q\left(\frac{d_1 \pm \frac{1}{4}\Re\bar{g}P\delta e^{2\sqrt{2}\sigma_x x_i + 2\mu_x}}{\sigma_{N-i}}\right), \quad (16)$$

where

$$\sigma_{N-i} = \sqrt{2qF_A\bar{g}^2\Re\left[h^l P\delta e^{2\sqrt{2}\sigma_x x_i + 2\mu_x} + P_b\right]\Delta f + \frac{4k_b T F_n}{R_L}\Delta f}. \quad (17)$$

Here, k is the order of approximation, $\{\omega_i\}$ and $\{x_i\}$ $(i = -k, -k+1, \ldots -1, 1, 2, \ldots, k)$ are the weight factors and the zeros of the Hermite polynomial, respectively [19]. From (15) and (16), the closed-form expression for the QBER can be obtained. It is noted that $k = 10$ gives accurate results for this approximation [18].

B. Ergodic Secret-Key Rate

To validate the security of the proposed system, especially in the case of beam-splitting eavesdrop, we analyze the ergodic secret-key rate over the atmospheric fading channels. First, we denote $H(B)$ and $H(E)$ as the information entropy of Bob and Eve, respectively. The conditional entropies of Bob-Alice and Eve-Alice are denoted as $H(B|A)$ and $H(E|A)$, respectively. The mutual information $I(A;B)$ and $I(A;E)$ are defined as the estimation of the information shared between Alice and Bob, and that shared between Alice and Eve, respectively. Thus, $I(A;B) = H(B) - H(B|A)$ and $I(A;E) = H(E) - H(E|A)$, in which the key is said to be secure if $I(A,B)$ is higher than $I(A,E)$ [20]. As a result, we define the ergodic secret-key rate S as the maximum transmission rate at which the eavesdropper is unable to decode any information, which is given as

$$S = I(A;B) - I(A;E). \quad (18)$$

1) Mutual information between Alice and Bob: Alice and Bob share information over the channel as depicted in Fig. 5, where x_i $(i \in \{1,2\})$ i.e. bits "0" and "1", and y_j $(j \in \{1,2,3\})$ i.e. bits "0", X, and "1", respectively. p and q denote the channel transition probabilities. α and $(1-\alpha)$ are the probabilities of transmitting bits "0" and "1". We define this new type of channel as the binary erasure channel (BEC) with

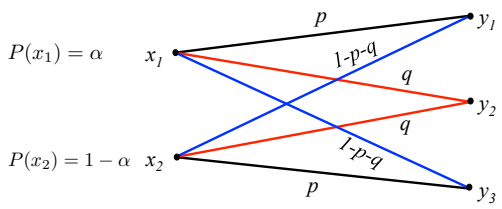

Fig. 5. Diagram of the binary erasure channel (BEC) with errors between Alice and Bob.

errors. Hence, the mutual information $I(A;B)$ can be derived as

$$\begin{aligned} I(A;B) = {} & p\log_2(p) + (1-p-q)p\log_2(1-p-q) \\ & -(\alpha p + (1-\alpha)(1-p-q))\log_2(\alpha p + (1-\alpha)(1-p-q)) \\ & -(\alpha(1-p-q) + (1-\alpha)p)\log_2((\alpha(1-p-q) + (1-\alpha)p)). \end{aligned} \tag{19}$$

Details of the proof of (19) are omitted due to space limitation. In our system, we have $\alpha = 0.5$. p, q, and $(1-p-q)$ are respectively the conditional probabilities that Bob creates bit y_j when Alice sends bit x_i, which can be deduced from the joint probabilities derived in Section IV-A.

2) Mutual information between Alice and Eve: In our system, Eve obtains a bit string through eavesdropping, whose bit values are partially identical to Alice's. Thus, we can consider that Alice and Eve share some information via binary symmetric channel (BSC). As a result, the mutual information $I(A;E)$ can be given as

$$I(A;E) = 1 + e\log_2(p) + (1-e)\log_2(1-e), \tag{20}$$

where e is *Eve's probability of error*, which is defined as $e = P_{A,E}(0,1) + P_{A,E}(1,0)$ with $P_{A,E}(0,1)$ and $P_{A,E}(1,0)$ are the joint probabilities that Eve falsely detects Alice's transmitted bits using threshold detection $d_E = 0$. Similar to Section IV-A, using Gauss-Hermite quadrature formula, $P_{A,E}(0,1)$ and $P_{A,E}(1,0)$, averaged over the fading channel, can also be derived in closed-form expressions.

V. Numerical Results

In this section, we investigate the criteria for transmitter and receiver settings to maintain the security of the proposed system under beam-splitting and intercept-resend attacks. Two performance metrics, QBER and ergodic secret-key rate S, are analytically analyzed and a good agreement with M-C simulations is confirmed. It is assumed that the atmospheric attenuation coefficient $\beta_l = 0.43$ dB/km and the system is operating at 1 Gbps.

In the beam-splitting attack, Eve tries to steal information by tapping the transmitted signal. To defend against this attack, Alice chooses a small value of modulation depth δ at the transmitter so that Eve will suffer from a high error rate, with $d_E = 0$. When Eve is close to Alice, e.g., $L_{A,E} = 1$ km, Fig. 6 shows the values of δ under different turbulence strengths versus Eve's probability of error e. To guarantee that

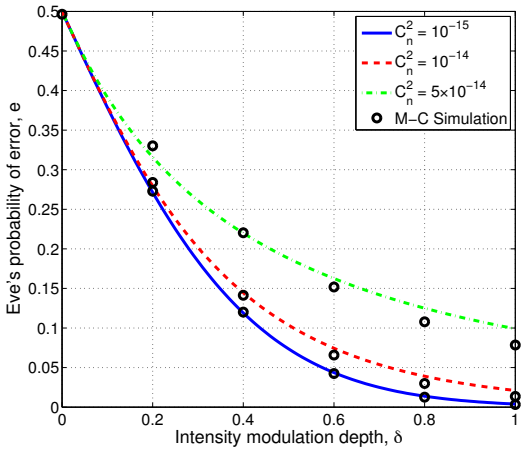

Fig. 6. Eve's probability of error versus the modulation depth δ. $L_{A,E} = 1$ km, $\bar{g} = 10$, $P = 0$ dBm.

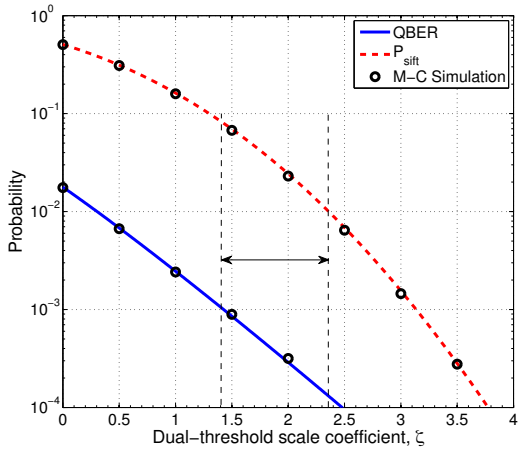

Fig. 7. QBER and Bob's P_{sift} versus ζ. $\delta = 0.4$, $L_{A,B} = 1$ km, $\bar{g} = 10$, $C_n^2 = 10^{-15}$, $P = 0$ dBm.

e is sufficiently high, e.g., $e > 10^{-1}$, the chosen values for δ should be $\delta \leq 0.4$ for all cases. Particularly, under strong turbulence $C_n^2 = 5 \times 10^{-14}$, Eve's error is always higher than 10^{-1} for all values of δ.

Regarding the criteria for receiver design (at Bob), we can control QBER and P_{sift} by adjusting d_0 and d_1 through ζ, as shown in Fig. 7. In this figure, the distance from Alice to Bob is $L_{A,B} = 1$ km. Our target is to control QBER $\leq 10^{-3}$ and $P_{sift} \geq 10^{-2}$ so that the error is small enough while the probability of sift is sufficient for Bob to receive information from Alice. Doing so requires the choice of $1.4 \leq \zeta \leq 2.35$.

With the above design criteria at Alice and Bob, if Eve uses intercept-resend attack, we can guarantee that the probability that Alice and Bob can detect the eavesdrop (i.e. the probability they find disagreement in *Step 3* over the public channel and identify the presence of Eve), given by $P_D = 1 - [(1-e)P_{sift}(1-P_{error})]^n$ with n is the key length, is sufficiently high. For example, when $\delta = 0.4$, $\zeta = 2$,

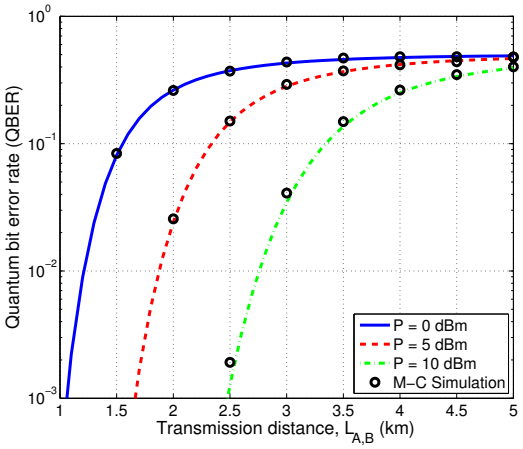

Fig. 8. QBER versus transmission distance $L_{A,B}$. $\delta = 0.4$, $\zeta = 2$, $\bar{g} = 10$, $C_n^2 = 10^{-15}$.

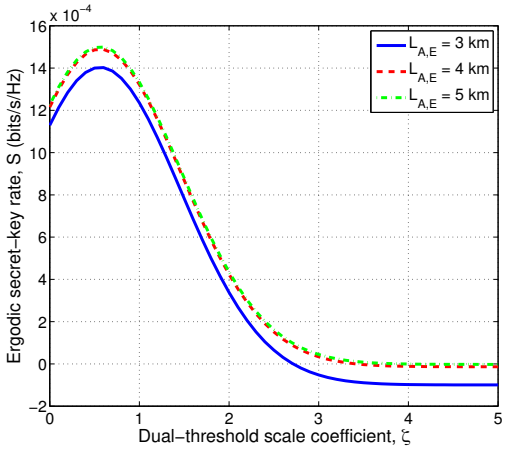

Fig. 9. Ergodic secret-key rate versus ζ. $\delta = 0.4$, $L_{A,B} = 2$ km, $\bar{g} = 10$, $C_n^2 = 10^{-15}$, $P = 0$ dBm.

$C_n^2 = 10^{-15}$ and $n = 7$, we have $P_D = 0.999999999$.

Setting $\zeta = 2$ and with $\delta = 0.4$, the dual thresholds d_0 and d_1 can be determined. Keeping this setting, Fig. 8 investigates the QBER versus $L_{A,B}$ with varying peak transmitted power P. It can be seen that the achievable $L_{A,B}$ at QBER $= 10^{-3}$ can be significantly improved by increasing P, under weak turbulence condition.

Finally, in Fig. 9, we look at another aspect of the performance metric in receiver design by showing the ergodic secret-key rate S versus ζ for different distances from Alice to Eve $L_{A,E}$ (Eve is located further behind Bob). It is seen that there is an optimal DT scale coefficient where the secret-key rate is maximum. Nevertheless, we can only select $1.4 \leq \zeta \leq 2.35$ due to the constraint for receiver design. As a result, to maximize the secret-key rate, it is necessary to select the smallest possible ζ.

VI. Conclusions

We proposed a novel free-space QKD system using SIM/BPSK and DT/DD receiver with an APD. The design criteria for transmitter and receiver, in particular, the modulation depth and the setting for dual-threshold, were comprehensively discussed. The QBER and the ergodic secret-key rate of the proposed system were analytically derived in closed-form expressions, considering the impact of atmospheric channel and receiver noises. Analytical results and M-C simulations confirmed the feasibility of the proposed system.

References

[1] H. P. Yuen, "Security of quantum key distribution, *IEEE Access,* vol. 4, pp. 724–749, Mar. 2016.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.,* pp. 175–179, Bangalore, India, 1984.

[3] N. Gisin et al., "Quantum cryptography" *Rev. Mod. Phys.,* vol. 74, pp. 145–145, 2002.

[4] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.,* vol. 88, 057902, Feb. 2002.

[5] P. Jouguet et al., "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics,* vol. 7, pp. 378–381, 2013.

[6] X. Wang et al., "Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution," *IEEE J. Quantum Electron.,* vol. 51, no. 6, 5200206, Jun. 2015.

[7] D. Huang et al., "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.,* vol. 6, 19201, Jan. 2016.

[8] C. Wang et al., "Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects," *Phys. Rev. A,* vol. 93, no. 2, 022315, 2016.

[9] T. Schmitt-Manderbach et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.,* vol. 98, no. 1, 010504, 2011.

[10] B. Heim et al., "Atmospheric continuous-variable quantum communication," *New J. Phys.,* vol. 16, 113018, 2014.

[11] N. Hosseinidehaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," *In Proc. of the 2015 IEEE Int. Conf. Commun. (ICC),* pp. 7413–7419, Jun. 2015.

[12] X. Sun, I. B. Djordjevic, M. A. Neifeld, "Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels," *IEEE Photon. J.,* vol. 8, no. 3, 7904713, Jun. 2016.

[13] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise," *New J. Phys.,* vol. 18, 013018, Jan. 2016.

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.,* vol. 68, no. 21, pp. 3121–3124, May 1992.

[15] D. A. Luong et al., "Effect of avalanche photodiode and thermal noises on the performance of binary phase-shift keying-subcarrier-intensity modulation/free-space optical systems over turbulence channels," *IET Commun.,* vol. 7, no. 8, pp. 738–744, Mar. 2013.

[16] S. Karp, *Optical channels: fibers, clouds, water and the atmosphere*, Plenum Press, 1988.

[17] P. V. Trinh et al., "All-optical relaying FSO systems using EDFA combined with optical hard-limiter over atmospheric turbulence channels," *IEEE/OSA J. Lightw. Technol.,* vol. 33, no. 19, pp. 4132–4144, Oct. 2015.

[18] H. T. T. Pham et al., "A comprehensive performance analysis of PPM-based FSO systems with APD receiver in atmospheric turbulence," *In Proc. of the 2012 Int. Conf. on Adv. Technol. Commun. (ATC 2012),* pp. 357-361, Oct. 2012.

[19] M. Abramowitz, I. A. Stegun, *Handbook of mathematical functions, with formulas, graphs, and mathematical tables*, 9th edition, Dover, 1972.

[20] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.,* vol. 27, pp. 379–423, 623–656, Jul./Oct. 1948.