Photonic Network Communications
https://doi.org/10.1007/s11107-021-00934-y

ORIGINAL PAPER

Reliability improvement of satellite-based quantum key distribution systems using retransmission scheme

Nam D. Nguyen[1] · Hang T. T. Phan[2] · Hien T. T. Pham[1] · Vuong V. Mai[3] · Ngoc T. Dang[1]

Received: 12 February 2020 / Accepted: 12 May 2021

Abstract

This paper theoretically studies the design and performance analysis of the reliable satellite-based quantum key distribution (QKD) over free-space optics channel. The proposed QKD system is based on the optical quadrature phase-shift keying (QPSK) modulation and the dual-threshold/heterodyne detection (DT/HD) receiver that helps to reduce quantum bit error rate (QBER) and improve the receiver sensitivity. In addition, a key retransmission scheme is also designed to enhance the reliability of the proposed QKD system. Performance of the key transmission is analyzed in terms of QBER and the probability of sifted key, taking into account the impacts of free-space path loss, atmospheric attenuation, beam spreading loss, atmospheric turbulence, and receiver noise. In addition, we newly develop an analytical framework by using the 3-D Markov chain model that allows us to investigate the key loss rate (KLR) performance at the link layer. Numerical results quantitatively show that our proposed satellite-based QKD system can offer significant performance improvement over the conventional ones.

Keywords Quantum key distribution (QKD) · Free-space optics (FSO) · Quadrature phase-shift keying (QPSK) · Quantum bit error rate (QBER) · Key retransmission scheme · Key loss rate (KLR)

1 Introduction

Quantum key distribution (QKD) is considered as the promising solution, which can be obtained unconditional security quantum communications by distributing a secret key used to encrypt and decrypt secure data between legitimate parties (i.e., Alice and Bob) with eavesdropper existed (i.e., Eve). To distribute the secret key, different transmission environments such as optical fiber and free-space optics (FSO) have been studied. Optical fiber-based QKD systems are commercially available; nevertheless, their achievable distance is limited to a few hundred kilometers [1]. Therefore, satellite-based QKD systems, which are offered as the best method for overcoming the limitation of transmission distance, are promising candidates for a global-scale QKD network. Several proof-of-principle experiments in this direction have been performed recently. For instance, the space-to-ground QKD system based on a low Earth orbit (LEO) satellite with corner-cube retroreflectors was implemented in 2015 [2]. The first quantum science satellite named Micius, which is the Chinese satellite-based QKD situated at about 500 km in high-altitude, was launched in 2016. After that, the Micius satellite plays a role as the trusted relay that distributes secret keys between multiple remote places in China and Europe [3]. Those experiments confirmed that the main factor limiting the performance of satellite-based QKD systems is atmospheric turbulence. Due to this factor, even there is no eavesdropper existed, the quantum key error rate (QKER) may be very high under strong turbulence. For this reason, designing a reliable satellite-based QKD system could be a crucial issue.

In general, the reliability of satellite-based QKD systems can be improved by using advanced physical-layer techniques. Accordingly, a number of studies have focused on the methods to efficiently encode the key information, which

✉ Ngoc T. Dang
ngocdt@ptit.edu.vn

Nam D. Nguyen
nguyendinhnam.working@gmail.com

[1] Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

[2] Hanoi University of Industry, Hanoi, Vietnam

[3] School of Electrical Engineering, KAIST, Daejeon, South Korea

Published online: 02 June 2021

are categorized into two types including discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). In DV-QKD systems, discrete states of each photon (i.e., polarization or phase) are used to encrypt key information. Therefore, Bob's receiver needs a single-photon device to detect the transmitted key information [4]. Unfortunately, DV-QKD systems show relatively low key rates. The recent highest secret-key rate of 105.7 Mbps has been demonstrated by using a 37-core fiber [5]. Compared to DV-QKD, CV-QKD has good compatibility with the classical optical communication systems. Joint propagation of a CV-QKD channel and wavelength-division multiplexing transmission of classical data-carrying coherent channels has been experimentally reported [6]. There have been several types of CV-QKD systems, where the key information is encoded relying on the amplitude and/or phase of the light pulse [7], subcarrier intensity modulation/binary phase-shift keying (SIM/BPSK) using radio frequency (RF) subcarrier modulator [8], and quadrature phase-shift keying (QPSK) using optical carrier [9, 10].

Also, the reliability improvement could be achieved by the reconciliation process based on forward error-correction (FEC) techniques. With FEC, Bob's receiver corrects the erroneous bits based on the received redundancy that is added to Alice's transmitted key. Several types of FEC techniques have been proposed to QKD systems such as block code [12], Hamming code [13], and low-density parity-check code (LDPC) [14, 15]. The use of FEC, however, requires highly computational algorithms and large computational memory. In addition, it can only detect and correct a limited number of errors. To improve the ability of error correction, FEC technique requires a large amount of redundant information, which causes a reduction in transmission efficiency.

To further improve the reliability and feasibility of satellite-based QKD systems, advanced techniques in both the physical layer and link layer are proposed to be used in this study. Firstly, advanced techniques in the physical layer consisting of optical QPSK signaling and heterodyne detection (HD) receiver are employed. The optical QPSK signaling is easy to implement as it does not require using RF subcarrier and small modulation depth as SIM/BPSK. In addition, heterodyne detection helps to improve the sensitivity of the receiver; hence, the QBER is reduced. Actually, heterodyne detection has been used in of CV-QKD systems that encode key information on light pulse [16]. We also have proposed a QKD system based on QPSK modulation signaling and DT/HD receiver [10]. However, the impacts of beam spreading loss and atmospheric turbulence are ignored in that work and thus will be considered in this study. Moreover, additional contributions of this study are twofold as follows

- A key retransmission scheme is designed to improve the reliability of satellite-based QKD systems, where Alice is responsible for error correction by retransmitting the keys that Bob received unsuccessfully due to bit errors. The advantage of key retransmission is that both large interactive communications and complex coding algorithms for the error-correction process are not required.
- The mathematical expression for QBER of satellite-based QKD system using QPSK modulation signaling is derived taking into account the impact of the free-space path loss, atmospheric attenuation, beam spreading loss, atmospheric turbulence, and receiver noise. We also newly develop a 3-D Markov chain model allowing us to analyze the key loss rate (KLR).

Numerical results demonstrate that the performance of our proposed satellite-based QKD system is significantly improved compared to conventional ones. Also, the appropriate values of system's parameters such as the dual-threshold (DT) coefficient, the required transmitted power, and the number of retransmission are also determined from the numerical results correspondingly to each turbulence condition.

The organization of the paper's remainder is organized as follows. Section 2 describes the detail of QKD protocol design based on QPSK modulation. The proposed satellite-based QKD system enabling key retransmission with system model and FSO channel model is presented in Sect. 3. The performance analysis for physical layer and link layer is presented in Sects. 4 and 5, respectively. Numerical results are demonstrated and discussed in Sect. 6. Finally, the paper is concluded with summarized key points in Sect. 7.

2 QPSK-based QKD protocol

The first QKD protocol, best-known as BB84, was proposed by Bennett and Brassard [17]. In BB84, Alice and Bob share secret keys by using randomly non-orthogonal quantum states of photons (either diagonal or rectilinear) to encode the signal. BB84 has been widely used as a reference model for designing new QKD protocols. Similarly, our proposed QKD protocol using QPSK signaling and dual-threshold/heterodyne detection (DT/HD) receiver is also implemented based on BB84 [10]. More specifically, bases of Alice and Bob are based on the phase of optical carrier as shown in Table 1, and the principle of our designed protocol is summarized as follows

Step 1: Firstly, in the transmitter, Alice randomly selects her base (either A_1 or A_2) for each binary bit, which is encoded into a phase state of an optical carrier denoted as ϕ_A. $\phi_A = \left(\phi_1 + \phi_2\right)/2$ is formed by combining two phase states (i.e., ϕ_1 and ϕ_2) from branches of Mach–Zehnder modulators (MZMs). Consequently, corresponding to four states

Table 1 Base of Alice and Bob with corresponding carrier's phase

Alice	bit	ϕ_1	ϕ_2	ϕ_A	Bob	ϕ_B	$\phi_A - \phi_B$	I	bit
A_1	0	0	$\pi/2$	$\pi/4$	B_1	$\pi/4$	0	I_0	0
A_1	0	0	$\pi/2$	$\pi/4$	B_2	$-\pi/4$	$\pi/2$	0	X
A_1	1	π	$3\pi/2$	$5\pi/4$	B_1	$\pi/4$	π	I_1	1
A_1	1	π	$3\pi/2$	$5\pi/4$	B_2	$-\pi/4$	$-\pi/2$	0	X
A_2	0	0	$-\pi/2$	$-\pi/4$	B_1	$\pi/4$	$-\pi/2$	0	X
A_2	0	0	$-\pi/2$	$-\pi/4$	B_2	$-\pi/4$	0	I_0	0
A_2	1	π	$\pi/2$	$3\pi/4$	B_1	$\pi/4$	$\pi/2$	0	X
A_2	1	π	$\pi/2$	$3\pi/4$	B_2	$-\pi/4$	π	I_1	1

of photon's polarization in BB84 protocol is four values of ϕ_A also known as four phase states of QPSK signaling.

Step 2: The signal from Alice with phase ϕ_A is combined with the one of Bob with phase ϕ_B to obtain $\cos(\phi_A - \phi_B)$. The value of ϕ_B is randomly chosen between two Bob's bases, either B_1 ($\phi_B = \pi/4$) or B_2 ($\phi_B = -\pi/4$). Alice and Bob choose the same basis if Alice chooses A_i, while Bob uses B_i, where $i \in \{1, 2\}$. Consequently, the electrical current (I) at the output of the detector obtains one of three values, I_0, 0 or I_1, which are corresponding to bits "0," "X," and "1," respectively. It is worth noting that bit "X" is discarded.

Step 3: Through the public channel, time instants when Bob can detect "0" or "1" from the received signals are announced to Alice. On the other hands, Alice immediately eliminates bits corresponding to the time instants when Bob detects "X," which is on average about 50% of the total number of bits. Finally, the remaining bits create a new bit sequence shared between Alice and Bob, which is called ***sifted key***.

Step 4: Due to physical-layer impairments or eavesdropping attacks, the sifted key may consist of errors. To detect and eliminate the erroneous bits, *information reconciliation* process can be deployed by using FEC technique to create final ***secret key***. In this study, instead of using FEC technique, the key retransmission scheme is proposed to be used.

3 Satellite-based QKD system enabling key retransmission

3.1 System description

Figure 1 describes our proposed satellite-based QKD system using QPSK modulation, DT/HD receiver, and key retransmission. The system has two main functions: the transmission of the secret key at the physical layer over the FSO channel and the link-layer key retransmission scheme which aims to improve the system performance. Assuming

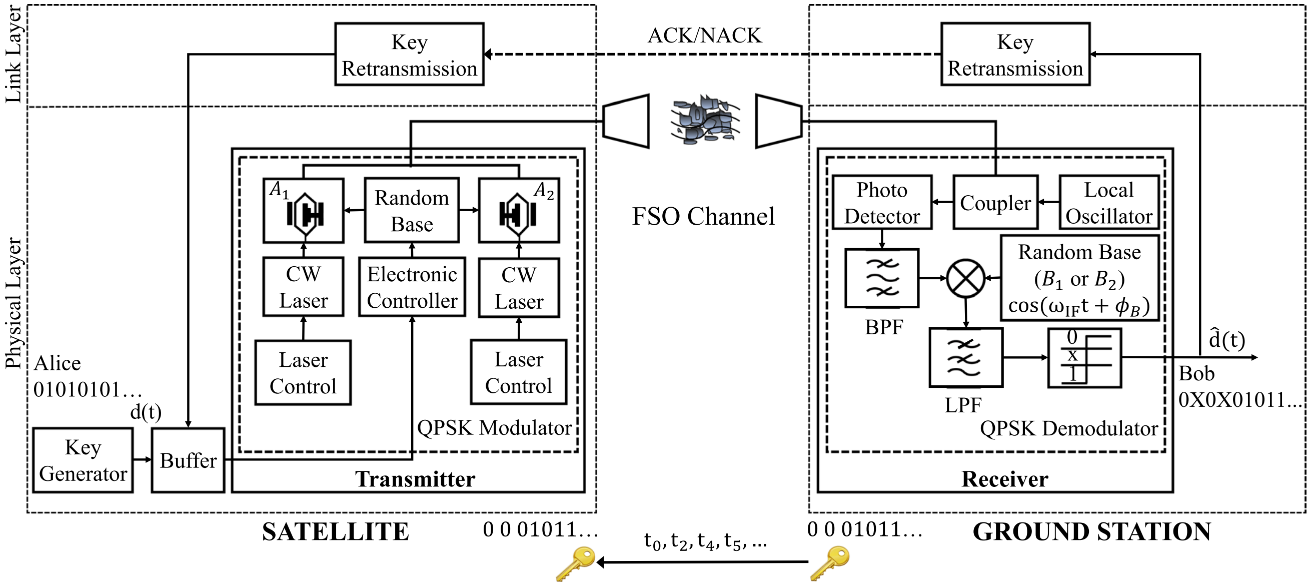


Fig. 1 The proposed satellite-based QKD system using QPSK modulation, DT/HD receiver, and key retransmission

that the transmitter (Alice) is placed at the satellite, while the receiver is located at the ground station (Bob). Secret keys are transmitted from Alice to Bob via a secure FSO channel, while key retransmission feedback from Bob to Alice is sent through a classical public RF channel.

In the transmitter, the electronic controller generates two types of control information depending on the value ("1" or "0") of binary bits from the sequence $d(t)$. The control information is later used to govern the phase of the optical signal outputted from Mach–Zehnder modulators (MZMs). The random base module randomly selects one of two MZMs corresponding to two bases A_1 and A_2 to encode the binary data onto the phase of optical carrier generated from the laser. At each MZM, the phase of optical carrier at each branch is governed by the binary bit ("0" or "1") as shown in Tab. 1. The signal at the output of MZM is the combination of the optical signal from two branches, which forms Alice's phase, ϕ_A.

In the receiver, the received optical signal is combined with a continuous wave (CW) optical field generated by the optical local oscillator (LO). An optical phase-locked loop is used in order to keep the phase matching between the LO and the received signal. The mixed signal is converted to the electrical current thanks to the avalanche photodetector (APD). The electrical signal is then filtered by a bandpass filter (BPF) to eliminate the undesired signal, while the useful component at the intermediate frequency is retained to perform the next processes. Next, the electrical current at the output of the BPF is multiplied with the reference signal $\cos\left(2\pi f_{IF}t + \phi_B\right)$. Two decoded bases of Bob are randomly chosen by setting the phase of reference signal. The decoded signal is then filtered by a low-pass filter (LPF) to recover the baseband signal. Finally, a threshold detector is used to decide on bit "1," bit "0," or bit "X."

3.2 Key retransmission scheme

To reduce the key loss rate, key retransmission scheme is deployed in the link layer. At the satellite, Alice's random bit sequence $d(t)$ created by the key generator is first queued in the buffer. Then, the buffer forwards the bit sequence at the front of the queue to the transmitter. The bit sequence is transmitted over free space optical channel to the receiver, which is located in the ground station. In the link layer, if the sifted key is retrieved by the Bob successfully without errors, Bob sends back a local acknowledgment (i.e., ACK) to Alice instantly. Alice then removes this bit sequence from the buffer. If Bob fails to receive the bit sequence, he sends NACK to Alice and then she retransmits the corrupt bit sequence. Denote M as the maximum number of retransmission allowed for each bit sequence. The bit sequence is removed from the buffer after being received by the Bob successfully, or after M failed attempts. The bit sequences that cannot be obtained by Bob's receiver are those due to buffer overflow and those discarded after M failed attempts.

3.3 Channel model

This section presents the mathematical models for determining the FSO channel that consists of four terms including free-space loss (L_{FS}), atmospheric attenuation (h_a), beam spreading loss (h_l), and atmospheric turbulence-induced fading (h_f). It is worth noting that the impact of atmospheric turbulence is negligible when the altitude is high enough [19]. Therefore, in following mathematical models, the altitude of H_β is used as a threshold to determine whether the power loss is dominated by free-space loss or atmospheric attenuation.

Free-Space Loss: The laser beam is transmitted from the satellite at the altitude of H_S through free-space to the ground station, which is placed at the altitude of H_G. The free-space loss, which is considered for the altitudes ranging from H_S to H_β, can be expressed as [19]

$$L_{FS} = \left(\frac{4\pi D_S}{\lambda}\right)^2, \tag{1}$$

where D_S is the transmission distance in free-space environment, which can be calculated as $D_S = (H_S - H_\beta)/\cos(\zeta)$. ζ denotes the zenith angle, which is determined by the propagation direction and the zenith. λ defines the optical wavelength.

Atmospheric Attenuation: The atmospheric attenuation can be calculated based on exponential Beer–Lambert laws as follows [20]

$$h_a = \exp(-\gamma D_\beta), \tag{2}$$

where γ denotes the weather-based attenuation coefficient. Where D_β is the transmission distance in atmospheric environment, which is determined as $D_\beta = (H_\beta - H_G)/\cos(\zeta)$.

Beam Spreading Loss: At the receiver, a Gaussian beam profile and a circular detection aperture are assumed to quantify the effect of beam spreading. At the distance of $D_{SG} = (H_S - H_G)/\cos(\zeta)$ from Alice to Bob, the normalized spatial distribution of optical intensity can be calculated as [21]

$$I_{\text{beam}}(\boldsymbol{\rho};D_{SG}) = \frac{2}{\pi\omega_D^2}\exp\left(-\frac{2||\boldsymbol{\rho}||^2}{\omega_D^2}\right), \tag{3}$$

where ω_D is the beam waist at the distance D_{SG}. $\boldsymbol{\rho}$ is the radial vector from the center of beam footprint and ||.|| defines the expression of Euclidean norm. The beam spreading loss is quantified by the fraction of power collected by the detector $h_l(.)$. With pointing error $\boldsymbol{r}$, between the centers of the detector and the beam footprint can be determined as

$$h_l(\boldsymbol{r};D_{SG}) = \int_A I_{\text{beam}}(\boldsymbol{\rho} - \boldsymbol{r};D_{SG})\mathrm{d}\boldsymbol{\rho}, \tag{4}$$

where A is the area of Bob's detector. The Gaussian form of $h_l(.)$ is written by [22]

$$h_l(r;D_{SG}) \approx A_0 \exp\left(-\frac{2r^2}{\omega^2_{D_{eq}}}\right), \tag{5}$$

where $\omega^2_{D_{eq}} = \omega^2_D \frac{\sqrt{\pi}\mathrm{erf}(v)}{2v\exp(-v^2)}$ defines the equivalent beam width at the ground station, $A_0 = [\mathrm{erf}(v)]^2$ and $v = \frac{\sqrt{\pi}a}{\sqrt{2}\omega_D}$. a is the radius of the detection aperture at the ground station. A_0 denotes the fraction of collected power at $r = 0$.

Equation (5) is used to determine the optical power obtaining by Bob or an eavesdropper (Eve). In unauthorized receiver attack (URA) scenario, an unauthorized receiver can be placed near Bob (i.e., in the beam footprint) to steal the quantum key. We assume that Bob's detector is located at the beam center (i.e., $r = 0$), while $r = D_{E-B}$ is the distance between Eve and Bob (see Fig. 2). Optical power received by which is conversely proportion to r. At the ground station, the fractions of optical power collected by the detector of Bob and Eve are $h_l(0;D_{SG})$ and $h_l(D_{E-B};D_{SG})$, correspondingly.

Atmospheric Turbulence-Induced Fading: Both weak and strong turbulence conditions are considered in this study; therefore, Gamma–Gamma distribution is used to model the atmospheric turbulence-induced fading h_f, whose PDF with the condition $h_f > 0$ is given as [23]

$$f_{h_f}(h_f) = \frac{2K_{\alpha-\beta}(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)}\left(2\sqrt{\alpha\beta h_f}\right)(h_f)^{\left(\frac{\alpha+\beta}{2}\right)-1}, \tag{6}$$

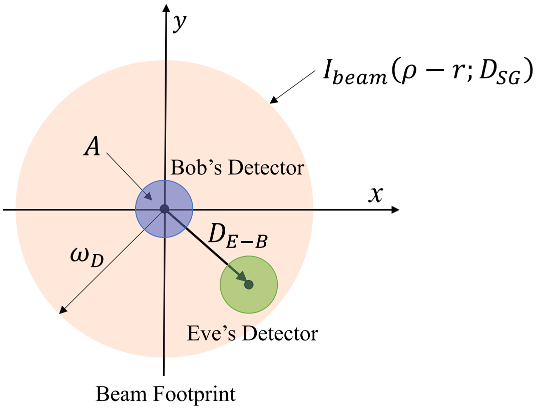


Fig. 2 Beam footprint at the ground and the locations of Bob and Eve

where α and β are the parameters representing the effect of large scale and small scale turbulent eddies, respectively. $K_{\alpha-\beta}(.)$ is the second kind modified Bessel function and order (α-β) and $\Gamma(.)$ represents the Gamma function defined as $\Gamma(m) = \int_0^\infty t^{m-1}e^{-t}dt$. Assuming a plane wave propagation, α and β can be approximately calculated as [24]

$$\begin{cases} \alpha \cong \left[\exp\left(\frac{0.49\sigma_R^2}{\left(1+1.11\sigma_R^{12/5}\right)^{7/6}}\right) - 1\right]^{-1}, \\ \beta \cong \left[\exp\left(\frac{0.51\sigma_R^2}{\left(1+0.69\sigma_R^{12/5}\right)^{5/6}}\right) - 1\right]^{-1}, \end{cases} \tag{7}$$

where σ_R^2 is the Rytov variance and can be express as (when determining the optical communication link at the altitudes ranging from H_β to H_G) [25]

$$\sigma_R^2 = 2.25k^{\frac{7}{6}}\sec(\zeta)^{\frac{11}{6}}\int_{H_G}^{H_\beta} C_n^2(h)(h - H_G)^{\frac{5}{6}}\mathrm{d}h, \tag{8}$$

where $k = 2\pi/\lambda$ defines the wave number in optical field. $C_n^2(h)$ denotes for the altitude-dependent refractive index structure parameter, which characterizes the turbulence strength. Practically, Hufnagel-Valley (H-V) model can be employed to determine the turbulence profiles as follows [25]

$$\begin{aligned} C_n^2(h) =& 0.00594\left(\frac{w}{27}\right)^2\left(10^{-5}h\right)^{10}\exp\left(-\frac{h}{1000}\right) \\ &+ 2.7\times10^{-16}\exp\left(-\frac{h}{1500}\right) + C_n^2(0)\exp\left(-\frac{h}{100}\right), \end{aligned} \tag{9}$$

where w is wind speed, and h is the height above the ground. $C_n^2(0)$, the value of C_n^2 at the ground level, can be adjusted adapting to various conditions at the ground station.

4 Physical-layer performance analysis

4.1 QKD system using QPSK and DT/HD receiver

In this section, the transmission of the downlink from Alice to Bob (or Eve) is analyzed. At Alice's transmitter, the optical signal with phase states selected randomly is written as

$$E_T = \sqrt{P_T G_T}\exp\left[-i(2\pi f_c t + \phi_A)\right], \tag{10}$$

where P_T is the peak transmitted power, f_c is the optical carrier frequency, and G_T is the telescope gain of the transmitter. The signal E_T is transmitted over FSO channel and the signal E_R retrieved at the ground station can be expressed as

$$E_R = \sqrt{P_R}\exp\left[-i(2\pi f_c t + \phi_A)\right], \tag{11}$$

where $P_R = \frac{1}{L_{FS}} G_T P_T h_a h_l h_f(t) G_R$ is the received power at Bob's receiver, where L_{FS}, h_a, h_l, and $h_f(t)$ represent the free-space path loss, atmospheric attenuation, beam spreading loss, and atmospheric turbulence, respectively. G_R is the telescope gain of the receiver. Next, E_R is mixed with a continuous wave optical field, which is created by the optical local oscillator as follows

$$E_{LO} = \sqrt{P_{LO}} \exp[-i(2\pi f_{LO} t)], \tag{12}$$

where P_{LO} and f_{LO} are the power and the frequency of the LO, respectively. The combined signal is converted to the photocurrent by the avalanche photodetector and then filtered by a bandpass filter to eliminate the undesired signal. The bases of Bob are randomly chosen by setting the phase of reference signal $\cos(2\pi f_{IF} t + \phi_B)$. Decoding process is implemented by multiplying the intermediate frequency signal with the reference one. Consequently, the decoded current is given as

$$\begin{aligned} I_{dec} =& 2\bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} \cos(2\pi f_{IF} t + \phi_A) \\ & \times \cos(2\pi f_{IF} t + \phi_B) + n(t), \\ =& \bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} \cos(4\pi f_{IF} t + \phi_A + \phi_B) \\ & + \bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} \cos(\phi_A - \phi_B) + n(t), \end{aligned} \tag{13}$$

where $f_{IF} = f_c - f_{LO}$ is the intermediate frequency. $\mathfrak{R} = \frac{\eta q}{\tilde{h} f_c}$ is the responsivity of the APD with η is the quantum efficiency, q is the electron charge, $\tilde{h}$ is Planck's constant, f_c is the optical frequency, and $\bar{g}$ is avalanche multiplication factor. $n(t)$ is the noise current. The decoded signal I_{dec} is then passed through the low-pass filter to obtain the signal $i(t)$ depending on the values of ϕ_A and ϕ_B (see Table 1) as

$$\begin{aligned} i(t) =& \bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} \cos(\phi_A - \phi_B) + n(t), \\ =& \begin{cases} i_0 = \bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} + n(t), \\ 0, \\ i_1 = -\bar{g}\mathfrak{R}\sqrt{P_R P_{LO}} + n(t), \end{cases} \end{aligned} \tag{14}$$

where i_0 and i_1 represent the received current signals for bits "0" and "1," respectively. We assume that the background noise is negligible thanks to the optical filter, the receiver noise components consist of shot noise, dark noise, and thermal noise, which are modeled as additive Gaussian noise with zero mean. The variance of $n(t)$ is given by

$$\sigma_n^2 = 2q\bar{g}^{2+x}\left[\mathfrak{R}(P_R + P_{LO}) + I_d\right]\Delta f + \frac{4k_B T}{R_L}\Delta f, \tag{15}$$

where q is the electron charge, I_d is the dark current, T is the receiver temperature, x is the excess noise factor, k_B is Boltzmann's constant, R_L is the load resistance, and $\Delta f = R_b/2$ is the receiver's bandwidth, where R_b is the bit rate. It is significant to note that shot noise is created by both received optical power and LO power. However, P_R is much less than P_{LO}, and thus, the signal-dependent shot noise is ignored. Due to the impact of noise, i_0 and i_1 are fluctuated and their probability density functions (PDFs) are shown in Fig. 3. Two peaks of the distribution of the current are corresponding to Alice's bit "0" and bit "1," which overlap with each other. Two thresholds including d_1 and d_0 are used to decide on bits "0," "X," and "1." The decision rule can be expressed as

$$\text{Decision Rule} = \begin{cases} 0 \ \text{ if } \left(i \geq d_0\right) \\ 1 \ \text{ if } \left(i \leq d_1\right) \\ X \ \text{ otherwise.} \end{cases} \tag{16}$$

4.2 Quantum bit error rate

Similar to BB84 protocol, the quantum bit error rate can be defined as [4, 26]

$$\text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}}, \tag{17}$$

where P_{sift} is the probability that Bob uses the same bases as Alice to determine the retrieved photons, from which he decodes a sequence of bits called sifted key; P_{error} is the probability that there are a number of erroneous bits in the sifted key, caused by physical-layer impairments and/or Eve's intervention. These probabilities can be calculated as

$$P_{\text{error}} = P_{A,B}(0,1) + P_{A,B}(1,0), \tag{18}$$

$$P_{sift} = P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1), \tag{19}$$

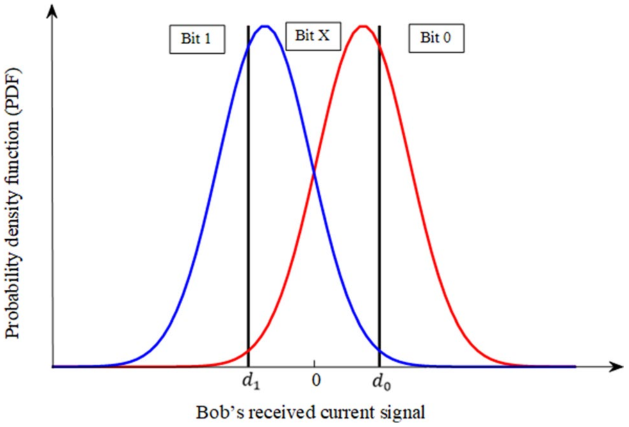


Fig. 3 The PDF of received signal, where d_1 and d_0 are the level of DT detection

where $P_{A,B}(a,b)$ is the joint probability that Alice sends bit "a," while Bob detects bit "b" with $a, b \in \{0,1\}$, and can be expressed as

$$P_{A,B}(a,b) = P_A(a)P_{B|A}(b|a), \tag{20}$$

where $P_A(a) = 1/2$ is the probability that Alice sends bit "0" or bit "1," which is assumed to be equal.

Accordingly, the joint probabilities between Alice and Bob averaged over the fading channel can be respectively calculated as

$$P_{A,B}(a,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_0 - I_a}{\sigma_n}\right) f_{h_f}(h_f)\mathrm{d}h_f, \tag{21}$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_0^\infty Q\left(\frac{I_a - d_1}{\sigma_n}\right) f_{h_f}(h_f)\mathrm{d}h_f, \tag{22}$$

where $P_{A,B}(a,b)$ is the joint probability that Alice sends bit "a," while Bob detects bit "b," with $a,\ b \in \{0,1\}$. $Q(.) \cong \frac{1}{\sqrt{2\pi}}\int_0^\infty \exp(-t^2/2)dt$ is the Gaussian Q-funciton, σ_n^2 is the total noise variance (15), and I_a denotes the received current without noise for bit "a" which can be defined as

$$\begin{cases} I_0 = \bar{g}\Re\sqrt{P_R P_{LO}}, \\ I_1 = -\bar{g}\Re\sqrt{P_R P_{LO}}. \end{cases} \tag{23}$$

To determine the detection thresholds d_0 and d_1, we use the dual-threshold selections as follows [8]

$$d_0 = E[i_0] + \varsigma\sqrt{\sigma_n^2} \quad \textit{and} \quad d_1 = E[i_1] - \varsigma\sqrt{\sigma_n^2}, \tag{24}$$

where ς is the dual-threshold (DT) scale coefficient. As $E[h_f] = 1$, $E[i_a]$, the mean value of i_a, can be expressed as

$$\begin{cases} E[i_0] = \bar{g}\Re\sqrt{\frac{1}{L_{FS}} G_T P_T h_a h_l G_R P_{LO}}, \\ E[i_1] = -\bar{g}\Re\sqrt{\frac{1}{L_{FS}} G_T P_T h_a h_l G_R P_{LO}}. \end{cases} \tag{25}$$

5 Link-layer performance analysis

5.1 Quantum channel-state model

In this section, a two-state Markov model is employed to determine the quantum channel-state transition. This model is known as a logically accurate and flexible with wireless channels [18, 27]. In quantum two-state Markov model, we split time into slots, where a bit sequence created by Alice's key generator is sent. The channel alternates between a bad state and a good state. A state is considered as *good* when all sifted keys are transmitted error-free. On the contrary, if all transmissions are failed, this channel state is *bad*. Figure 4 illustrates the behavior of the proposed quantum channel states based on the geometric distribution.

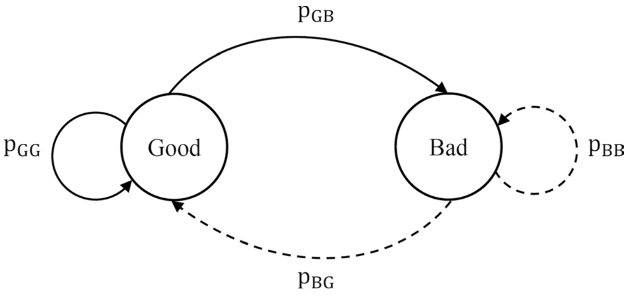


Fig. 4 Quantum channel-state transition model

From Eq. (17), we derive the average quantum key error rate (QKER) as follows

$$\mathrm{QKER} = 1 - (1 - \mathrm{QBER})^{l_{bs}P_{sift}}, \tag{26}$$

where l_{bs} is the length of random bit sequence. Given the QKER, the transition probabilities of channel state are formulated as

$$\begin{cases} p_{BB} = \mathrm{QKER}\left(1 - \frac{\tau_{bs}}{\tau_0}\right), \\ p_{GG} = (1 - \mathrm{QKER})\left(1 - \frac{\tau_{bs}}{\tau_0}\right), \\ p_{BG} = 1 - p_{BB}, \\ p_{GB} = 1 - p_{GG}, \end{cases} \tag{27}$$

where $\tau_{bs} = l_{bs}/R_b$ is the time interval to transmit a bit sequence, i.e., a time slot. R_b is the system's bit rate. $\tau_0 = \sqrt{\lambda D_\beta}/w$ is atmospheric turbulence coherent time, which indicates the time interval in which the turbulence condition is unchanged. w represents the wind speed, and λ denotes the wavelength. D_β is the transmission distance in the atmospheric environment [28].

5.2 Queue-associated DTMC

At the satellite, the bit sequence is generated and inputted to the buffer with the flow throughput H (sequence/second). Stationary Bernoulli process is used to model the arrival process of bit sequence at the buffer. Therefore, $H\tau_{bs}$ and $1 - H\tau_{bs}$ are the probabilities of the events that there is a bit sequence and no bit sequence arriving in each considered time slot, respectively. As mentioned above, τ_{bs} is the duration of a time slot. Assuming that, in each given time slot, the FSO channel keeps stable condition at its current state. When the buffer is not empty, a bit sequence is forwarded to Alice's transmitter at the beginning of time slot. It will be removed at the end of the time slot if this transmission is successful.

At the beginning of each time slot, a three-dimensional discrete-time Markov chain (DTMC) model is determined by (n, s, m), where $n \in [0, C]$ is the number of bit sequences queued at the buffer, $s \in \{B, G\}$ denote the quantum channel state, and $m \in [1, M]$ represents the number of times that the currently-served bit sequence is retransmitted. This type of DTMC is known as the queue-associated DTMC (QA-DTMC). Especially, it is noted that the states which have both parameters $n = 0$ and $m > 1$ are impossible. The transition states of QA-DTMC are demonstrated in Fig. 5 and clearly shown in Table 2.

5.3 Key loss rate

The probability of the steady state of the queue-associated DTMC, which is denoted by $\pi(n, s, m)$, is determined by using the balance equation as follows

$$\begin{cases} \Pi^T P = \Pi^T, \\ \sum_{n=0}^{C} \sum_{s\in\{B,G\}} \sum_{m=0}^{M} \pi(n, s, m) = 1, \end{cases} \tag{28}$$

where $\Pi = [\pi(n, s, m)]$. P is the state transformation probability matrix with the size of $(C + 1) \times 2 \times (M + 1)$ and its elements are shown in the third column of Tab. 2. By using the standard numerical methods including Jacobi iteration or Gauss elimination, the balance equation (28) is solved. Accordingly, Π can be determined as follows

$$\begin{aligned} \Pi =&[\pi(0, G, 0), \pi(1, G, 0), ..., \\ &\pi(C, G, M), \pi(0, B, 0), \pi(1, B, 0), ..., \pi(C, B, M)], \end{aligned} \tag{29}$$

Finally, the key loss rate (KLR) due to M times of failed retransmissions and the buffer overflow can be calculated as

$$\mathrm{KLR} = \sum_{s\in\{B,G\}} \sum_{m=0}^{M} \pi(C, s, m) + \sum_{n=0}^{C-1} \pi(n, B, M). \tag{30}$$

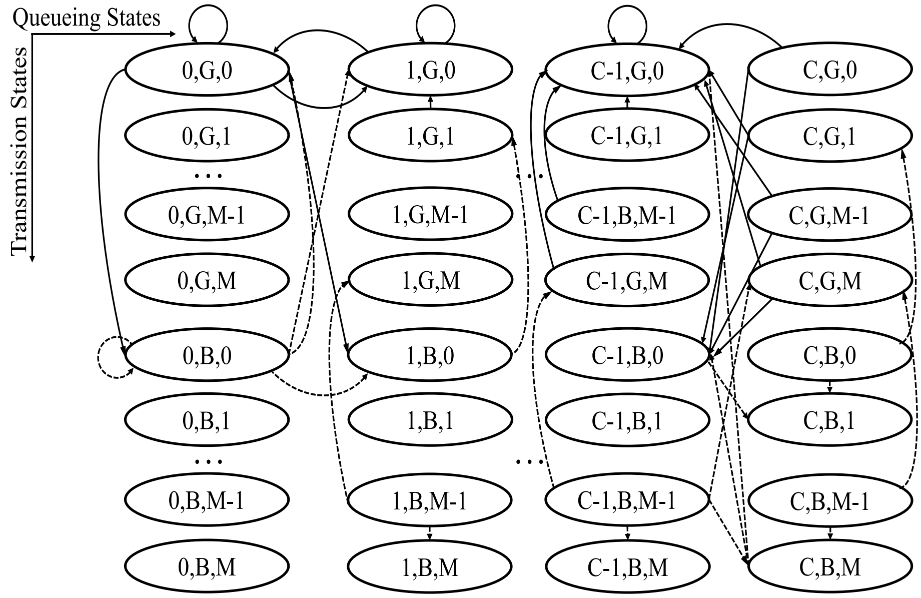


Fig. 5 The state transition of the QA-DTMC

Table 2 State transition probabilities of the QA-DTMC

Current state	Next state	Transformation probability
$(0, B, 0)$	$(1, B, 0)$ $(1, G, 0)$ $(0, B, 0)$ $(0, G, 0)$	$H\tau_{bs}p_{BB}$ $H\tau_{bs}p_{BG}$ $(1 - H\tau_{bs})p_{BB}$ $(1 - H\tau_{bs})p_{BG}$
(n, B, m) $n \in [1, C-1]$ $m \in [0, M-1]$	$(n+1, B, m+1)$ $(n+1, G, m+1)$ $(n, B, m+1)$ $(n, G, m+1)$	$H\tau_{bs}p_{BB}$ $H\tau_{bs}p_{BG}$ $(1 - H\tau_{bs})p_{BB}$ $(1 - H\tau_{bs})p_{BG}$
(n, B, M) $n \in [1, C-1]$	$(n, B, 0)$ $(n, G, 0)$ $(n-1, B, 0)$ $(n-1, G, 0)$	$H\tau_{bs}p_{BB}$ $H\tau_{bs}p_{BG}$ $(1 - H\tau_{bs})p_{BB}$ $(1 - H\tau_{bs})p_{BG}$
(C, B, m) $m \in [0, M-1]$	$(C, B, m+1)$ $(C, G, m+1)$	p_{BB} p_{BG}
(C, B, M)	$(C-1, B, 0)$ $(C-1, G, 0)$	p_{BB} p_{BG}
(0,G,0)	$(1, B, 0)$ $(1, G, 0)$ $(0, B, 0)$ $(0, G, 0)$	$H\tau_{bs}$ p_{GB} $H\tau_{bs}$ p_{GG} $(1 - H\tau_{bs})$ p_{GB} $(1 - H\tau_{bs})$ p_{GG}
(n, G, m) $n \in [1, C-1]$ $m \in [0, M]$	$(n, B, 0)$ $(n, G, 0)$ $(n-1, B, 0)$ $(n-1, G, 0)$	$H\tau_{bs}p_{GB}$ $H\tau_{bs}p_{GG}$ $(1 - H\tau_{bs})p_{GB}$ $(1 - H\tau_{bs})p_{GG}$
(C, G, m) $m \in [0, M]$	$(C-1, B, 0)$ $(C-1, G, 0)$	p_{GB} p_{GG}

6 Numerical results

6.1 Physical-layer performance results

In this section, we determine the criteria for setting up Bob's receiver to guarantee security constraints under the unauthorized receiver attack. The feasibility of our proposed system is also investigated. The constants and key system parameters are summarized in Table 3. The values of $C_n^2(0) = 5 \times 10^{-15}$ and $C_n^2(0) = 7 \times 10^{-12}$ corresponding to the weak and strong turbulence conditions are used for deriving the numerical results.

In Fig. 6, QBER and P_{sift} at Bob's receiver are investigated as the functions of the DT scale coefficient under weak (a) and strong (b) turbulence conditions. The probability that Bob mistakenly detects a bit (i.e., "1" or bit "0") is large if the high DT scale coefficient is used, i.e., the difference between two thresholds d_0 and d_1 is large. Accordingly, P_{error} decreases when the DT scale coefficient increases, and thus, QBER and P_{sift} also reduce. It is important to note that Bob needs to collect enough information from Alice. Therefore, the probability of sifting should be large enough, e.g., $P_{sift} \geq 10^{-2}$ for achieving tens to hundreds Mbps key rate. We also need to keep Bob's QBER small, e.g., QBER$\leq 10^{-3}$, so as to Bob's receiver can feasibly correct the errors in the sifted key using error-correction codes. Based on these requirements of QBER and P_{sift}, we can determine the corresponding range of DT scale coefficient, for instance, $0.7 \leq \varsigma \leq 2.4$ under weak turbulence condition (Fig. 6(a)), and $1.4 \leq \varsigma \leq 2.8$ under strong turbulence condition (Fig. 6(b)). Practically, the receiver can set the DT scale coefficient based on the channel state information calculated by using the pilot signals.

Table 3 Constants and system parameters

Name	Symbol	Value
Constants and receiver parameters		
Electrons charge	q	1.6×10^{-19} C
Boltzmann constant	k_B	1.38×10^{-23} W/K/Hz
Bit rate	R_b	10 Gbps
Load resistor	R_L	50 Ω
Excess noise factor	x	0.8 (InGaAS APD)
Avalanche multiplication factor	$\bar{g}$	10
Responsivity of the APD	$\mathfrak{R}$	0.8
Receiver temperature	T	298 K
Dark current	I_d	3 nA
Channel parameters		
Wavelength	λ	1550 nm
Attenuation coefficient	γ	0.43 dB/km
Wind speed	w	21 m/s
Zenith angle	ζ	50°
Radius of the detection aperture	a	0.31 m
Beam width at ground station	ω_D	50 m
Satellite altitude	H_S	600 km
Ground station height	H_G	5 m
Atmospheric altitude	H_β	20 km
Tx telescope gain	G_T	120 dB
Rx telescope gain	G_R	121 dB
Link-layer parameters		
Flow throughput	H	185 sequence/s
Length of bit sequence	l_{bs}	3×10^6 bit

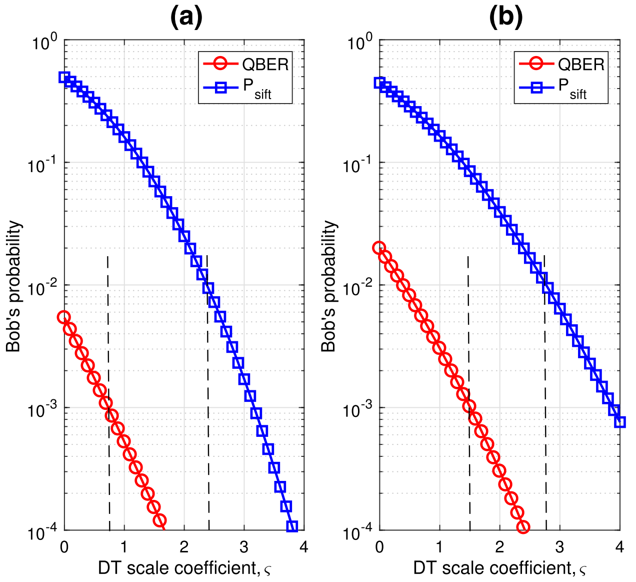


Fig. 6 Bob's QBER and P_{sift} versus the DT scale coefficient (ς), under (a) weak and (b) strong turbulence conditions with $P_T = 25$ dBm and $P_{LO} = 0$ dBm

Figure 7 demonstrates QBER and P_{sift} of Bob as versus the peak transmitted power (P_T) under weak turbulence conditions. For comparison, three types of modulation/detection schemes including optical QPSK-DT/HD, optical QPSK-DT/direct detection (DD), and SIM/BPSK-DT are considered. For all three types of QKD systems, Bob's P_{sift} meets the requirement of $P_{sift} \geq 10^{-2}$. However, the use of heterodyne detection gives an advantage in terms of QBER. More specifically, the QKD system using optical QPSK-DT/HD supports the QBER lower than the ones using optical QPSK-DT/DD and SIM/BPSK-DT. The figure also helps to determine the required transmitted power so as to Bob's QBER satisfies the condition that QBER $\leq 10^{-3}$. In the case of using optical QPSK-DT/HD, the minimum transmitted power is 25 dBm, while it is 45 dBm, i.e., 20 dB larger, for the case of using SIM/BPSK-DT.

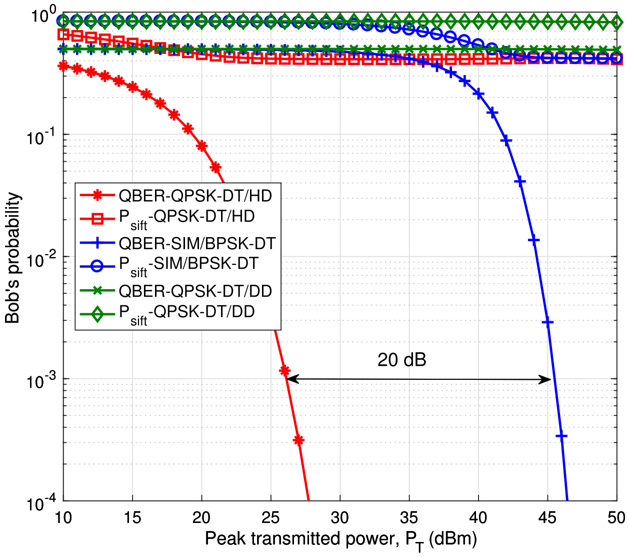


Fig. 7 Bob's QBER and P_{sift} versus the peak transmitted power (P_T) under weak turbulence condition for three cases: QPSK-DT/HD ($\varsigma = 0.7$ and $P_{LO} = 0$ dBm), QPSK-DT/DD ($\varsigma = 0.7$), and SIM/BPSK-DT ($\varsigma = 0.9$)

Figure 8 describes the variation of Bob's QBER with respect to different attenuation coefficients considering some values of the peak transmitted power under strong turbulence condition when the DT scale coefficient is fixed to 1.4, $G_T = 130$ dB, and $G_R = 131$ dB. The weather condition, which is determined via attenuation coefficients, has a clear impact on Bob's QBER. By setting the value of the transmitted power properly, our proposed QKD system can work well under various weather conditions. For instance, when $P_T = 45$ dBm, Bob's QBER $\leq 10^{-3}$ can be guaranteed in very clear conditions ($0 \leq \gamma \leq 0.5$), very light rain, and light mist conditions ($0.5 \leq \gamma \leq 1.53$). However, under haze or medium rain conditions ($1.54 \leq \gamma \leq 2.68$), a larger value of P_T should be set accordingly.

In Fig. 9, Eve's QBER and P_{sift} are investigated versus the Eve-Bob distance (D_{E-B}) under weak (a) and strong (b) turbulence conditions. We consider the worst case of unauthorized receiver attack that Eve uses the same DT scale coefficient as Bob. Clearly, the security constraints for the QKD system are governed by Eve's locations. More specifically, Eve's QBER is small when she is near Bob and thus she can illegally detect the key that Alice sends to Bob. Hence, Eve's QBER should be larger than the minimum value of 10^{-2} so as to she cannot detect the key correctly even with error-correction code. Based on this requirement, the minimum distance between Eve and Bob the guarantee the security is 30 m for both weak and strong turbulence conditions. Eve may reduce her QBER by increasing the DT scale coefficient. This, however, causes the reduction of P_{sift}, i.e., the amount of information she obtains from Alice also decreases.

6.2 Link-layer performance results

The numerical results and discussions related to the key loss rate at Bob's receiver versus the various system parameters are presented in this section. The parameters under consideration

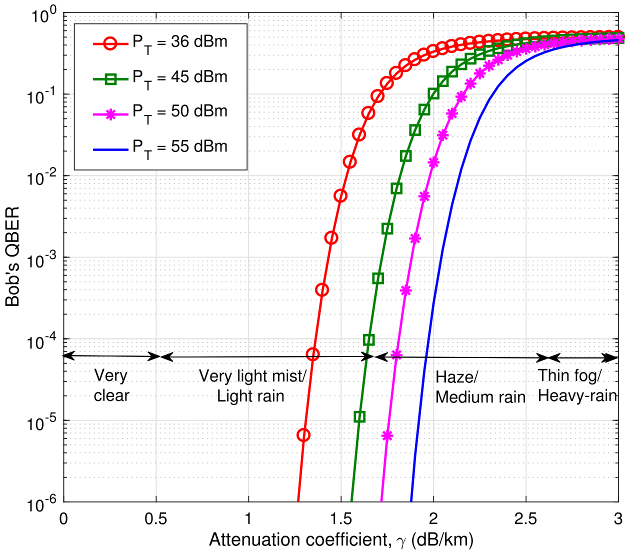


Fig. 8 Bob's QBER versus different attenuation coefficients (γ) under strong turbulence conditions with $P_{LO} = 0$ dBm, $\varsigma = 1.4$, $G_T = 130$ dB, and $G_R = 131$ dB

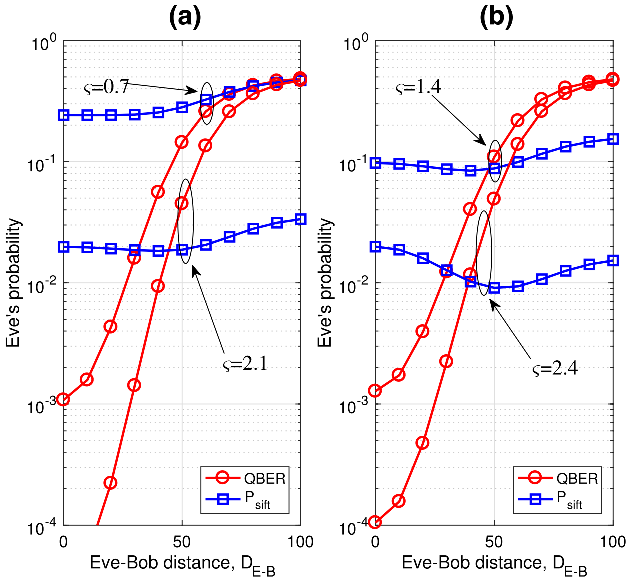


Fig. 9 Eve's QBER and P_{sift} versus the Eve-Bob distance (D_{E-B}) under (a) weak turbulence ($\varsigma = 0.7$ and 2.1), and (b) strong turbulence ($\varsigma = 1.4$ and 2.4) with $P_T = 25$ dBm, $P_{LO} = 0$ dBm

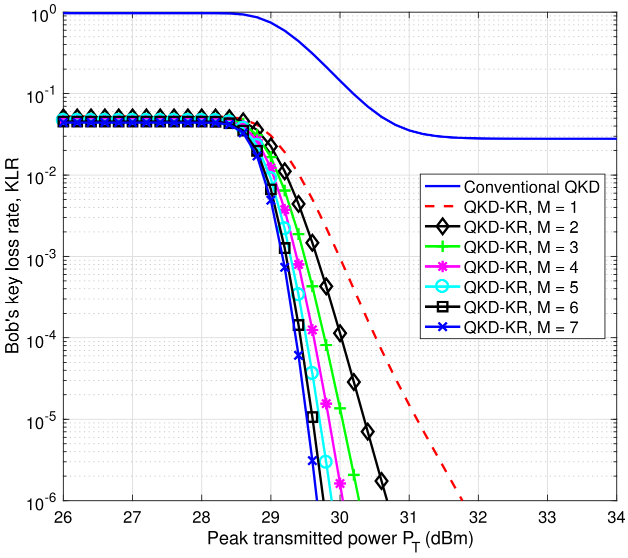


Fig. 10 Bob's key loss rate (KLR) versus the peak transmitted power (P_T) under weak turbulence with $P_{LO} = 0$ dBm and $\varsigma = 0.7$

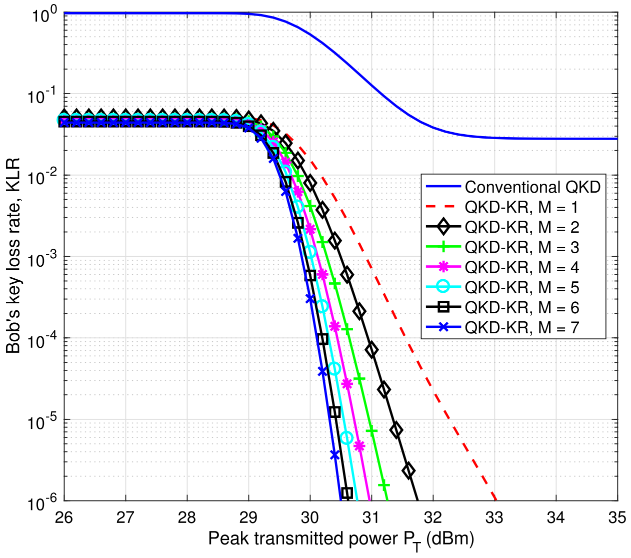


Fig. 11 Bob's key loss rate (KLR) versus the peak transmitted power (P_T) under strong turbulence with $P_{LO} = 0$ dBm and $\varsigma = 1.4$

include the peak transmitted power P_T and the number of retransmission M.

Figure 10 describes Bob's KLR versus the peak transmitted power (P_T) with system setting as $P_{LO} = 0$ dBm, $\varsigma = 0.7$, and $C_n^2(0) = 5 \times 10^{-15}$ for weak turbulence. We compare KLR of QKD system without retransmission (i.e., conventional QKD system) and that of the one enabling key retransmission with the number of retransmission $M = \{1, 2, 3, 4, 5, 6, 7\}$. Without key retransmission, KLR is relatively high because of atmospheric turbulence. More specifically, the lowest value of KLR is 3×10^{-2} even with high transmitted power. The KLR is reduced when the number of retransmission increases. For a given KLR, the increase of M also results in the reduction of the required transmitted power. This is very important for the case of strong turbulence because larger transmitted power is required.

Figure 11 investigates the Bob's KLR versus the peak transmitted power with $P_{LO} = 0$ dBm, $\varsigma = 1.4$, and $C_n^2(0) = 7 \times 10^{-12}$). The figure shows that at KLR $= 10^{-6}$, the power gain is 2 dB when the number of retransmission increases from 1 to 4. This is because the larger number of retransmission can compensate for the key loss due to lower transmitted power. However, the power gain is only 0.5 dB when M increases from 4 to 7. Therefore, the benefit of using the number of retransmission more than 4 is not significant. Also, retransmission causes the delay, thus M should not be properly chosen.

7 Conclusion

We proposed to improve the reliability of satellite-based QKD system using advanced techniques in both physical layer and link layer. We designed the QKD protocol based on QPSK signaling as well as the key retransmission scheme for our proposed QKD system. Also, we derived the mathematical expressions for the quantum bit error rate and key loss rate based on the proposed 3-D Markov chain model. The numerical results proved that our proposed QKD system can work well in both weak and strong turbulence conditions. Besides, it offers considerable performance improvement compared to the conventional systems especially the one without using retransmission scheme. The appropriate values of system's parameters such as the dual-threshold coefficient, the transmitted power, and the number of retransmission were also determined corresponding to each turbulence conditions.

Acknowledgements This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2019.08.

References

1. Yin, H.-L., Chen, T.-Y., Yu, Z.-W., Liu, H., You, L.-X., Zhou, Y.-H., Chen, S.-J., Mao, Y., Huang, M.-Q., Zhang, W.-J., Chen, H., Li, M., Nolan, D., Zhou, F., Jiang, X., Wang, Z., Zhang, Q., Wang, X.-B., Pan, J.-W.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. **117**(19), 190501 (2016)

2. Vallone, G., Bacco, D., Dequal, D., Gaiarin, S., Luceri, V., Bianco, G., Villoresi, P.: Experimental satellite quantum communications. Phys. Rev. Lett. **115**(4), 040502 (2015)
3. Liao, S.-K., et al.: Satellite-relayed intercontinental quantum network. Phys. Rev. Lett. **120**(3), 030501 (2018)
4. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002)
5. Bacco, D., Da Lio, B., Cozzolino, D. et al.: Boosting the secret key rate in a shared quantum and classical fibre communication system. Commun. Phys. **2**(140) (2019)
6. Eriksson, T.A., Hirano, T., Puttnam, B.J. et al.: Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. Commun. Phys. **2**(9) (2019)
7. Samuel, L.B., Peter, V.L.: Quantum information with continuous variables. Rev. Mod. Phys. **77**, 513 (2005)
8. Trinh, P.V., Pham, T.V., Dang, N.T., Nguyen, H.V., Ng, S.X., Pham, A.T.: Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver. IEEE Access **6**, 4159–4175 (2018)
9. Costa e Silva, M.B., Xu, Q., Agnolini, S., Gallion, P., Mendieta, F.J.: Homodyne QPSK detection for quantum key distribution. In: Proceeding optical amplifiers and their applications/coherent optical technologies and applications, Technical Digest (2006)
10. Vu, M.B., Pham, H.T.T., Do, A.T., Phan, H.T.T., Dang, N.T.: Satellite-based free-space quantum key distribution systems using QPSK modulation and heterodyne detection receiver. In: The proceedings of the IEEE 19th international symposium on communications and information technologies (ISCIT: Ho Chi Minh City. Vietnam, Sep. **2019**, 265–270 (2019)
11. Xu, Q., Sabban, M., Gallion, P., Mendieta, F.: Quantum key distribution system using dual-threshold homodyne detection. In: Proceedings of 2008 IEEE international conference on research, innovation and vision for the future in computing and communication technologies, Ho Chi Minh City, pp. 1–8 (2008)
12. Sugimoto, T., Yamazaki, K.: A study on secret key reconciliation protocol "Cascade". IEICE Trans. Fund Electron. Commun. Comput. Sci. **E83-A**(10), 1987–1991 (2000)
13. Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Peterson, C.G.: Fast efficient error reconciliation for quantum cryptography. Phys. Rev. A **67**(5), 052303 (2003)
14. Thangaraj, A., Dihidar, S., Calderbank, A.R., McLaughlin, S.W., Merolla, J.: Applications of LDPC Codes to the Wiretap Channel. IEEE Trans. Inf. Theory **53**(8), 2933–2945 (2007)
15. Ai, X., Malaney, R., Ng, S.X.: Quantum key reconciliation for satellite-based communications: IEEE Glob. Commun. Conf. (GLOBECOM). Abu Dhabi, United Arab Emirates **2018**, 1–6 (2018)
16. Wang, T., et al.: High key rate continuous-variable quantum key distribution with a real local oscillator. Optic. Express **26**(3), 2794–2806 (2018)
17. Bennett, C. H., Brassard, G.: Quantum cryptography: Publick key distribution and coin tossing. In: Proceedings of IEEE international conference on computers systems and signal processing, Bangalore, India, pp. 175–179 (1984)
18. Hong S., Lin C., Xuemin.: Performance analysis of TFRC over wireless link with truncated link-level ARQ. IEEE Trans. Wirel. Commun. (2006)
19. Hemmati, H.: Near-earth laser communications. CRC Press (2009)
20. Sharma, M., Chadha, D., Chandra, V.: High-altitude platform for free-space optical communication: Performance evaluation and reliability analysis. J. Optic. Commun. Netw. **8**(8), 600–609 (2016)
21. Saleh, B.E.A., Teich, M.C.: Fundamentals of Photonics. Wiley, New York (1991)
22. Farid, Ahmed A.: Outage capacity optimization for free-space optical links with pointing errors. J. Lightwave Technol. **25**(7), 1702–1710 (2007)
23. Nor, N.A.M., Fabiyi, E., Abadi, M. M., Tang, X., Ghassemlooy, Z., and Burton, A.: Investigation of moderate-to-strong turbulence effects on free space optics—a laboratory demonstration. In: 2015 13th international conference on telecommunications (ConTEL), Graz, pp. 1–5 (2015)
24. Ghassemlooy, Z., Popoola, W. O., and Leitgeb, E.: Free-Space optical communication using subcarrier modulation in Gamma-Gamma atmospheric turbulence. In: 2007 9th international conference on transparent optical networks, Rome, pp. 156–160 (2007)
25. Ma, J., Li, K., Tan, L., Yu, S., Cao, Y.: Performance analysis of satellite-to-ground downlink coherent optical communications with spatial diversity over Gamma-Gamma atmospheric turbulence. Appl. Optic. **54**(25), 7575–7585 (2015)
26. Shapiro, J.H.: Near-field turbulence effects on quantum-key distribution. Phys. Rev. A **67**(2), Art. no. 022309 (2003)
27. Wang, H.S., Moayeri, N.: Finite-sate Markov channel-A useful model for radio communication channels. IEEE Trans. Vehic. Technol. **44**(1), 163–171 (1995)
28. Navas, A., Balslls, J.M., Vázquez, M., Notario, A., Monroy, I., Olmos, J.J.: Fade statistics of M-turbulent optical links. J. Wirel. Commun. Netw. **2017**, 112 (2017)

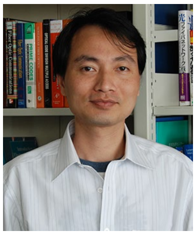
Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Nam D. Nguyen is currently an undergraduate student in Posts and Telecommunications Institute of Technology (PTIT), Vietnam. His research interests include network modeling and performance analysis with a particular emphasis on optical wireless communications.

Hang T. T. Phan received the B.E. degree in Electronics and Telecommunications from the Hanoi University of Science Technology (HUST), Vietnam, in 1999. She received the M.E. degree in Information Technology from HUST in 2005. From 2000 to present, she has been working at Hanoi University of Industry as a lecturer of the Faculty of Electronics Engineering Technology. She is currently working towards PhD. degree in Telecommunication Engineering at Posts and Telecommunications Institute of Technology (PTIT). Vietnam. Her present research interests are in the area of design and performance evaluation of optical and wireless communication systems.

Hien T. T. Pham received the B.E. Degree from Hanoi University of Transport and Communications in 1999; and the M.E. and Ph.D. degrees in Telecommunication Engineering from Posts and Telecommunications Institute of Technology (PTIT) in 2005 and 2017, respectively. From 1999 to present, she has been working at PTIT as a lecturer of the Department of Wireless Communications. Her present research interests are in the area of design and performance evaluation of optical and wireless communication systems.

Vuong V. Mai received the B.E. degree (Hons.) in Electronic Telecommunication Engineering from Posts and Telecommunications Institute of Technology (PTIT), Vietnam, in 2012, the M.S. and Ph.D. degrees in Computer Science and Engineering from the University of Aizu (UoA), Japan, in 2014 and 2017, respectively. In April 2017, he joined the Korea Advanced Institute of Science and Technology (KAIST), Korea, where he is currently a Postdoctoral Fellow with Photonics Systems Research Lab, School of Electrical Engineering. At KAIST, he is involved in a national research project funded by the Agency for Defense Development (ADD). He also works in collaboration with industry partners such as HFR, Inc. through several collaborative R&D projects. He is a member of OSA, IEEE, and IEICE.



Ngoc T. Dang received the B.E. degree from the Hanoi University of Technology, Hanoi, Vietnam in 1999, and the M.E. degree from the Posts and Telecommunications Institute of Technology (PTIT), Hanoi, Vietnam in 2005, both in electronics and telecommunications; and received the Ph.D. degree in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan in 2010. He is currently an Associate Professor/Head with the Department of Wireless Communications at PTIT. He was also an invited researcher at FOTONENSSAT Lab., Universite de Rennes 1, (France) in 2011 and a research fellow at Computer Communications Lab., The University of Aizu (Japan) in 2012, 2013, 2015, and 2017. His current research interests include the area of communication theory with a particular emphasis on modeling, design, and performance evaluation of optical CDMA, RoF, and optical wireless communication systems.