Comprehensive performance analysis of satellite-to-ground FSO/QKD systems using key retransmission

Nam D. Nguyen,[a] Hien T. T. Pham,[a] Vuong V. Mai,[b] and Ngoc T. Dang[a,c,*]

[a]Posts and Telecommunications Institute of Technology, Hanoi, Vietnam
[b]Korea Advanced Institute of Science and Technology, School of Electrical Engineering, Daejeon, Republic of Korea
[c]University of Aizu, Computer Communications Laboratory, Aizuwakamatsu, Japan

Abstract. We propose to investigate the performance of a satellite-to-ground quantum key distribution (QKD) system that uses key retransmission as a method for improving the system reliability. We develop analytical frameworks based on two three-dimensional Markov chain models allowing us to comprehensively analyze the proposed system's performance in terms of key loss rate, link utilization, and delay outage rate. Our performance analysis takes into account the physical layer impairments induced by free-space optical channel and receiver noise. Numerical results quantitatively demonstrate that the performance of satellite-to-ground QKD system is significantly improved due to key retransmission. In addition, the appropriate selection of system parameters corresponding to different turbulence conditions to achieve the best performance improvement is also provided. © *2020 Society of Photo-Optical Instrumentation Engineers (SPIE)* [DOI: 10.1117/1.OE.59.12.126102]

Keywords: quantum key distribution; free-space optics; key retransmission; Markov chain model; key loss rate.

Paper 20200670 received Jun. 9, 2020; accepted for publication Nov. 12, 2020; published online Dec. 3, 2020.

1 Introduction

Quantum key distribution (QKD) is a secure method of distributing cryptographic keys between distant parties. QKD systems that are based on optical fiber are commercially available today; however, the achievable distance is limited to a few hundred kilometers.[1] To overcome the limitation in terms of transmission distance, satellite QKD systems are considered as the best solution. A global-scale QKD network based on satellite-to-ground free-space optical (FSO) links to distribute secret encryption keys could meet the emerging and long-term threats to data.[2] Recently, several proof-of-principle experiments for satellite QKD have been performed. In 2015, QKD from space to ground via the in-orbit satellite corner cube retroreflectors was demonstrated.[3] The first quantum science satellite named Micius, which is an LEO satellite orbiting at an altitude of about 500 km, was launched in 2016 by China. This satellite was then used as a trusted relay to distribute secure keys between multiple remote locations in China and Europe.[4]

It is well known that the main factors limiting the performance of satellite-to-ground FSO links are atmospheric turbulence and attenuation, which are induced by the atmospheric channel. Due to these factors, even if there exists no eavesdropper existed, quantum key error rate (QKER) may be very high under strong turbulence. Therefore, designing a reliable QKD protocol could be a crucial issue in the study of satellite-to-ground QKD systems. It is also important to note that, for any designs, they should work within tight constraints of satellite platforms on size, weight, and power. Accordingly, many types of QKD protocols have been proposed. Depending on how the information is encoded, the QKD protocols can be classified into two major types, namely discrete variable (DV) and continuous variable (CV). In DV-QKD systems, the key information is encoded onto the discrete state of each photon that is known as the photon properties including phase and polarization.[5] Then, the encoded photons are propagated over the

*Address all correspondence to Ngoc T. Dang, ngocdt@ptit.edu.vn

0091-3286/2020/$28.00 © 2020 SPIE

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

quantum channel and a single-photon device is used to detect the photons at the receiver. DV-QKD implementation, however, requires using complicated technologies and the expensive cost. On the other hand, with CV-QKD, the key information is encoded relying on the amplitude and/or phase of the light pulse, i.e., the CV of coherent states.[6] It can also be implemented based on subcarrier intensity modulation binary phase-shift keying signaling and direct detection[7,8] and quadrature phase-shift keying (QPSK) using optical carrier.[9] Compared to DV-QKD, the advantage CV-QKD lies in the efficient, high-rate, and cost-effective detection using homodyne/heterodyne receivers as opposed to single-photon counters.[10]

The reduction of QKER could be achieved by the reconciliation process based on forwarding error correction (FEC) techniques. In the well-known Cascade technique, Alice and Bob divide their shifted keys into blocks and exchange the parity of each block. A binary search can be then used to locate and correct the position of errors in the shifted keys.[11] The other well-known technique, Winnow,[12] uses Hamming codes for the calculation of separate syndromes instead of a simple parity-check equation to correct the errors. Also, low-density parity-check codes (LDPC) can be used in the reconciliation process.[13,14] However, the binary search process in the Cascade protocol requires many interactive communications, which slows down the process in practice and not suitable for high-speed QKD applications. Although Winnow requires fewer interactions, the efficiency of this protocol is still far from the Shannon limit. LDPC helps to reduce the number of iterations and improve efficiency. However, LDPC codes are defined by a solid sparse parity-check matrix that requires large computational memory. In all mentioned techniques, highly computational algorithms are needed for optimizing FEC redundancy. These facts would increase the complexity of QKD transceivers significantly.

Another possible solution to provide reliable QKD is the use of key retransmission. In the case of using FEC, it is the receiver (Bob) who corrects errors based on the received redundancy from the sender (Alice) to minimize QKER in the reconciliation process. With the key retransmission scheme, Alice is responsible for error correction by retransmitting unsuccessfully keys received by Bob to ensure QKD reliability. The advantage of key retransmission is that it does not require complex coding algorithms or large interactive communications for error control. However, the feasibility of applying key retransmission for satellite-to-ground QKD systems has not been investigated. To address these issues, the main objective of this study is to carry out a comprehensive performance analysis of the satellite-to-ground QKD system using key retransmission, which is shown in Fig. 1. Satellite plays a role as a flying trusted-node, which holds all keys. Satellite carries out QKD operations with distinct ground stations to establish independent secret keys with each of them. The main contributions of the paper can be summarized as follows:

- First, we carry out the cross-layer design for the satellite-to-ground QKD system using key retransmission. Our considered QKD system is based on QPSK signaling, whose

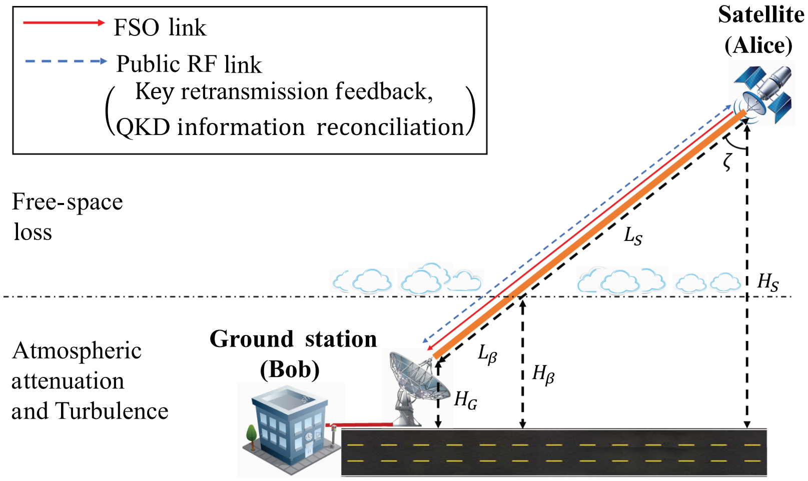

Fig. 1 Satellite-to-ground FSO/QKD system using key retransmission.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

architecture is simple due to the use of optical carrier directly (no RF subcarrier modulator needed). Furthermore, heterodyne detection (HD) receiver is employed for improving the receiver's sensitivity. The key retransmission scheme is implemented at the link layer based on the information about key errors obtained from the physical layer.

- Second, for validating the proposed QKD system, we develop analytical frameworks based on two three-dimensional 3-D Markov chain models allowing us to analyze the key loss rate (KLR), link utilization, and delay outage rate. Our performance analysis takes into consideration the physical layer impairments induced by FSO channels such as the atmospheric attenuation, atmospheric turbulence, and receiver noise. Based on our developed analytical frameworks, the appropriate values of the system's parameters, including the peak transmitted power, the maximum number of retransmissions, and the buffer size, can be determined.

The remainder of this paper is organized as follows. Section 2 describes the architecture of QKD systems using QPSK modulation with an HD receiver and key retransmission scheme. FSO link model is presented in Sec. 3. In Sec. 4, the performance analysis in terms of the KLR, link utilization, and delay outage rate is carried out. Numerical results are demonstrated and discussed in Sec. 5. Finally, the paper is concluded with summarized key points in Sec. 6.

2 QKD System Using QPSK Modulation, HD Receiver, and Key Retransmission

2.1 *Overall System Description*

The block diagram of the QKD system using QPSK modulation with an HD receiver and key retransmission is shown in Fig. 2. Alice's transmitter is located on a satellite while and Bob's

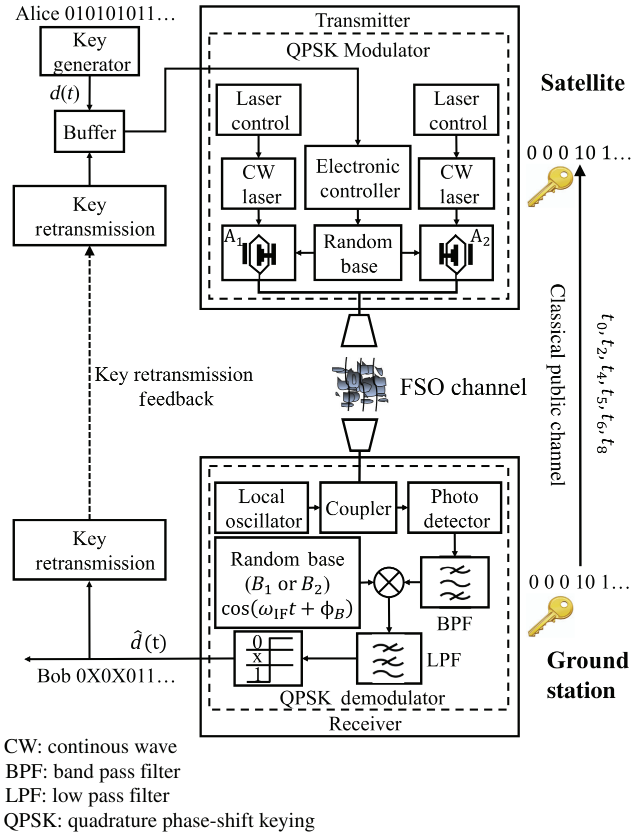

Fig. 2 FSO/QKD system utilizing QPSK modulation/HD receiver and key retransmission.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

Table 1 Alice's encoded states and Bob's decoded states.

Base	Bit	ϕ_1	ϕ_2	ϕ_A	Base	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

receiver is placed on a ground station. Alice sends the secret key to Bob through an FSO channel. In addition, a classical public channel is used for Bob to Alice the time instants he can create binary bits from the detected bits and key retransmission feedback signal.

Alice's random bit sequence $d(t)$ created by the key generator is first queued in a buffer. Then, Alice's buffer forwards the bit sequence at the front of the queue to the transmitter. At 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 the optical carrier generated from the laser. At each MZM, the phase of the optical carrier at each branch is governed by the binary bit ("1" or "0") as shown in Table 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.

The optical signal received by the receiver is combined with a continuous wave (CW) optical field generated by the optical local oscillator (LO). Next, the mixed signal is converted to the electrical current using an avalanche photodetector (APD). The electrical current is then passed through a bandpass filter (BPF) to eliminate the undesired component while the useful components at the intermediate frequency are retained to perform the decoding process. More specifically, the electrical signal from the BPF is multiplied with the reference signal $\cos(2\pi f_{\mathrm{IF}} t + \phi_B)$, where two decoded bases of Bob are randomly chosen by setting the phase ϕ_B of the reference signal. The decoded signal is then filtered by a low-pass filter (LPF) to recover the baseband signal. Finally, a dual-threshold detector is used to decide on bit "1," bit "0" or bit "X" to form $\hat{d}(t)$, which is the estimation of sequence $d(t)$.

2.2 *QPSK-Based QKD Protocol*

The first and best-known QKD protocol (named BB84 protocol) was proposed by Bennett and Brassard in 1984.[15] Using BB84 as a reference model, a new QKD protocol based on QPSK modulation, HD, and dual-threshold has been proposed.[9] The principle of this protocol is summarized in four steps and shown in Table 1.

Step 1: At Alice's transmitter, each binary bit is randomly encoded onto one of two-phase values of optical carrier (ϕ_A), where ϕ_A, the combination of the phase from two branches of MZM, i.e., ϕ_1 and ϕ_2, is calculated as $\phi_A = (\phi_1 + \phi_2)/2$. Four values of the phase ϕ_A known as the phase states of QPSK signaling while two-phase values of optical carrier are corresponding to two bases A_1 or A_2 in the BB84 protocol.

Step 2: To decode the signal obtained from Alice, Bob also randomly sets the value of his phase ϕ_B to one of two bases, including B_1 ($\phi_B = \pi/4$) or B_2 ($\phi_B = -\pi/4$). The mixed signal between the one from Alice and the one generated by Bob forms $\cos(\phi_A - \phi_B)$.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

Alice and Bob choose the same basis when Alice chooses A_y and Bob uses B_y, where $y \in \{1,2\}$. In this case, the electrical current (i) at the output of the detector receives one of two values, i_0 or i_1, which is corresponding to bit "0" or "1." If they choose different basis, the value of i is zero and bit "X" is formed. It is significant to note that bit "X" is discarded. This is also known as the sifting process in BB84 protocol as illustrated in Table 1.

Step 3: In this step, Bob informs Alice the time instants he can create binary bits from the detected signals via a classical public channel. Alice also discards bit values at the time instants that Bob created an unidentified bit, which is 50% on average. The remaining bits in the bit sequence from a new and identical bit sequence shared between Alice and Bob, namely as the sifted key.

Step 4: In practice, Bob's sifted key may contain errors due to channel/detector imperfections or eavesdropping. Similar to the BB84 protocol, to identify and remove the erroneous bits, this step carries out further information reconciliation to create error-free secret key. Nevertheless, instead of using FEC, the key retransmission scheme is employed in our considered QKD system.

2.3 *Key Retransmisson Scheme*

Key retransmission scheme is deployed in the link-layer as shown in Fig. 3 to reduce the KLR. In the link-layer, if the sifted key is received by Bob successfully without errors, Bob sends back a local acknowledgment (ACK) to Alice instantly. Alice then removes this bit sequence from her buffer. If Bob fails to receive the bit sequence, then Alice retransmits the corrupt bit sequence. Denote M as the maximum number of retransmission allowed for each bit sequence. The bit sequence is removed from Alice's 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.

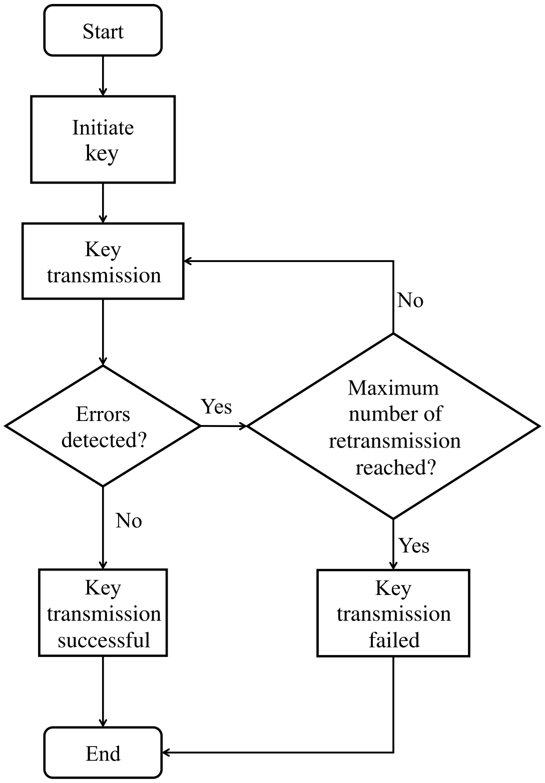

Fig. 3 Key retransmission scheme.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

3 FSO Link Model

3.1 *Atmospheric Channel*

In this section, we present the mathematical models for the atmospheric channel, which composed of three terms including free-space loss (FSL), atmospheric attenuation (h^l), and atmospheric turbulence (h^a). Accordingly, the channel coefficient h_c can be presented as $h_c = \frac{1}{\mathrm{FSL}} h^l h^a$. To calculate the channel coefficient, we define the altitudes of the satellite and the ground station as H_S and H_G, respectively. In addition, the turbulence strength, which is commonly determined by the reflective index structure parameter C_n^2, can be supposed to be zero while the altitude is high enough.[16] Therefore, we use the altitude of H_β as a threshold to determine whether the power loss is dominated by FSL or atmospheric attenuation in the following mathematical models.

3.1.1 *Free-space loss*

Considering the altitudes ranging from H_S to H_β, the FSL is the main factor causing the weakening of the received signal and can be formulated as[16]

$$\mathrm{FSL} = \left(\frac{4\pi L_S}{\lambda}\right)^2, \tag{1}$$

where L_S is the transmission distance in the free-space environment, which can be defined as $L_S = (H_S - H_\beta)/\cos(\zeta)$. ζ is the zenith angle, which is created by the zenith and the propagation direction of optical signal. λ is the operational wavelength

3.1.2 *Atmospheric attenuation*

Atmospheric attenuation is due primarily to absorption and scattering. By selecting the wavelengths coinciding with the transmission windows, absorption attenuation can be negligible. Hence, the channel loss is dominated by Mie scattering and is determined by the Kruse model as[17]

$$h^l = 10^{-A_{\mathrm{sca}}/10}, \tag{2}$$

where A_{sca} is the scattering attenuation, which is calculated in dB as follows:

$$A_{\mathrm{sca}} = 4.343\gamma d = 4.343\left[\frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-\delta(V)}\right]d, \tag{3}$$

where γ (km^{-1}) is the scattering coefficient. d (km) denotes the distance along which the scattering occurs. V (km) is the visibility range. $\delta(V) = 0.585V^{(1/3)}$ for $V < 6$ km, $\delta(V) = 1.3$ for $6 < V < 50$ km, and $\delta(V) = 1.6$ for $V > 50$ km.

- In the case of normal conditions, $d = L_\beta$, where $L_\beta = (H_\beta - H_G)/\cos(\zeta)$ is the transmission distance in atmospheric environment. This is due to the fact that scattering attenuation mainly occurs below the altitude of H_β.
- In fog conditions, Eq. (3) can be used for determining fog attenuation (A_{fog}) using appropriate value of V and $d = \frac{L_{\mathrm{fog}}}{\cos(\zeta)}$, where L_{fog} denotes the fog layer thickness.
- Rainfall is the main factor causing the nonselective scattering. The rain attenuation can be expressed as[17]

$$A_{\mathrm{rain}} = 1.076R_{\mathrm{rain}}^{0.67}\frac{L_{\mathrm{rain}}}{\cos(\zeta)}, \tag{4}$$

where R_{rain} (mm/h) is the rainfall rate. L_{rain} denotes the rain layer thickness.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

- Clouds can be characterized by liquid water contents (LWC), number density (N), and their layer thickness. By dividing the atmosphere into different layers, the cloud visibility range of each layer is estimated as $V_{\text{cloud}} = 1.002(\text{LWC} \times N)^{-0.6473}$. Then, the attenuations in individual cloud layers are predicted in the same way as Eq. (3).

3.1.3 *Atmospheric turbulence*

This is a random phenomenon caused by the pressure of the atmosphere and inhomogeneities in the temperature lead to refractive-index variations along the transmission path. Atmospheric turbulence will bring about the fluctuations of intensity also known as fading, which results in the degradation of the system performance. Since all turbulent regimes from weak to strong are considered in our work, the Gamma–Gamma (GG) distribution model is used to statistically characterize the atmospheric turbulence-induced fading with $h^a > 0$ as[18]

$$f_{h^a}(h^a) = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} (h^a)^{\left(\frac{\alpha+\beta}{2}\right)-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h^a}\right), \tag{5}$$

where $K_{\alpha-\beta}(.)$ is the second kind modified Bessel function of order $(\alpha - \beta)$ and $\Gamma(.)$ denotes the Gamma function defined as $\Gamma(m) = \int_0^\infty t^{m-1} e^{-t} \mathrm{d}t$; $\alpha > 0$ and $\beta > 0$ are the effective numbers of small-scale and large-scale eddies of the turbulent environment, respectively. Assuming a plane wave propagation, α and β can be approximately expressed as[19]

$$\alpha = \left\{ \exp\left[\frac{0.49\sigma_R^2}{(1 + 1.11\sigma_R^{12/5})^{7/6}} \right] - 1 \right\}^{-1}, \tag{6}$$

$$\beta = \left\{ \exp\left[\frac{0.51\sigma_R^2}{(1 + 0.69\sigma_R^{12/5})^{5/6}} \right] - 1 \right\}^{-1}, \tag{7}$$

where σ_R^2 is the Rytov variance. In case of the slant path optical communications in the altitudes ranging from H_β to H_G, σ_R^2 can be expressed as

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

where $k = 2\pi/\lambda$ is the optical wave number. $C_n^2(h)$ stands for the altitude-dependent refractive index structure coefficient. It is widely used to characterize the strength of turbulence. In our work, Hufnagel–Valley (H-V) model is utilized to estimate the turbulence profiles as[20]

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

where h is the height above the ground in meters, w is the root mean squared wind speed in m/s, and $C_n^2(0)$ determines the turbulence strength at the ground level in $m^{-2/3}$ and can be adjusted to fit various site conditions.

3.2 *Quantum Bit Error Rate*

This section presents the mathematical models for our proposed system. Based on these models, the quantum bit error rate can be determined. It is significant to note that we only consider the downlink key transmission from the satellite to the ground station.

At Alice's transmitter, the signal with randomly selected phase states from four different values of ϕ_A can be given as

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

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

where P_T is the peak transmitted power, G_T is the telescope gain of Alice's transmitter, and f_c is the optical carrier frequency. Then, the signal E_T is transmitted over the FSO channel and received at the optical ground station. The received optical signal can be given as follows:

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

where $P_R = G_T P_T h_c(t) G_R = \frac{1}{\mathrm{FSL}} G_T P_T h^l h^a(t) G_R$ is the peak received power at Bob's receiver, where FSL, h^l, and $h^a(t)$ denote the FSL, atmospheric attenuation, and atmospheric turbulence, respectively. G_R is the telescope gain of Bob's receiver. According to HD scheme, the received optical signal is combined with a CW optical field, which is generated by the optical LO. The LO's field is described by a similar expression as

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

where P_{LO} and f_{LO} are the power and the frequency of the LO, respectively. Next, the mixed signal is converted to the photocurrent using the APD and then filtered by a BPF, which only keeps the intermediate frequency component. The decoded bases of Bob are randomly chosen by setting the phase of reference signal $\cos(2\pi f_{\mathrm{IF}} t + \phi_B)$. The decoding process is implemented by multiplying the current at the output of the BPF with the reference one. Therefore, the decoded signal is written as

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

where $f_{\mathrm{IF}} = f_c - f_{\mathrm{LO}}$ is the intermediate frequency. $\Re = \frac{\eta q_e}{\tilde{h} f_c}$ is the primary responsivity of the APD with η is the quantum efficiency, q_e is the electron charge, $\tilde{h}$ is the Planck's constant, f_c is the optical frequency, $\overline{g}$ is the avalanche multiplication factor, and $n(t)$ is the receiver noise. Next, the decoded signal I_{DC} is then passed through the LPF to eliminate the undesired component and obtain the ultimate output current of the coherent receiver (i) depending on the values of ϕ_A and ϕ_B (see Table 1) as follows:

$$i = \overline{g}\Re\sqrt{P_R P_{\mathrm{LO}}}\cos(\phi_A - \phi_B) + n(t) = \begin{cases} i_0 = \overline{g}\Re\sqrt{P_R P_{\mathrm{LO}}} + n(t), \\ 0, \\ i_1 = -\overline{g}\Re\sqrt{P_R P_{\mathrm{LO}}} + n(t), \end{cases} \tag{14}$$

where i_0 and i_1 denote the received current signals for bits "0" and "1," respectively. Figure 4 shows the probability density function (PDF) of Bob's received signals influenced by the FSL, atmospheric attenuation and turbulence channel, and receiver noises, which are symmetric over the "zero" level. 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_0 and d_1 are used to decide on bits "0," and "1," "X" (i.e., no bit created). The decision rule can be described as

$$\text{Decision} = \begin{cases} 1 & \text{if } (i \le d_1) \\ 0 & \text{if } (i \ge d_0) \\ \mathrm{X} & \text{otherwise.} \end{cases} \tag{15}$$

Assuming that the background noise is negligible due to the optical filter, the receiver noise composing of shot noise, dark noise, and thermal noise. They are modeled as additive Gaussian noise (AWGN) with zero-mean. Therefore, $n(t)$ is the zero-mean AWGN with variance as follows:

$$\sigma_n^2 = 2q_e\overline{g}^{2+x}[\Re(P_R + P_{\mathrm{LO}}) + I_d]\Delta f + \frac{4k_B T}{R_L}\Delta f, \tag{16}$$

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

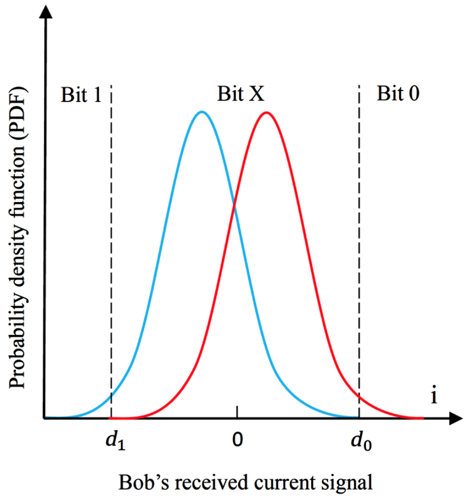

Fig. 4 The PDF of Bob's received signal, where d_0 and d_1 are two levels of the dual thresholds.

where q_e is the electron charge, I_d is the dark current, $\Delta f = R_b/2$ is the receiver's bandwidth, T is the receiver temperature, x is the excess noise factor, k_B is Boltzmann's constant, and R_L is the load resistance. It is worth noting that shot noise is created by both LO power and received optical power. However, P_R is much less than P_{LO} and thus the signal-dependent shot noise is ignored.

In BB84 protocol, the quantum bit error rate QBER reflects the percentage of bit errors in the sift key and can be expressed as[5,21]

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

where P_{sift} and P_{error} are the probabilities of sift and error, respectively. Specifically, P_{sift} is the probability that Bob uses the same bases as Alice to measure the received photons, from which he decodes a sequence of bits called sifted key; P_{error} is the probability that there are several erroneous bits in the sifted key, caused by technical imperfections and/or Eve's intervention.

In our proposed system, P_{sift} denotes the probability that Bob can detect bits "0" and "1" based on the dual-threshold detection. P_{error} corresponds to the probability that Bob wrongly decides bits "0" when Alice sent bits "1" and vice versa. Accordingly, QBER can be formulated as

$$\mathrm{QBER} = \frac{P_{A,B}(0,1) + P_{A,B}(1,0)}{P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1)}, \tag{18}$$

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 calculated as

$$P_{A,B}(a,b) = P_A(a)P_{B|A}(b|a), \tag{19}$$

where $P_A(a) = 1/2$ is the probability that Alice sends bit "0" or bit "1," which is assumed to be equally. $P_{B|A}(b|a)$ is the conditional probability that Alice's bit "a" coincides with Bob's bit "b."

Following the dual-threshold rule, the joint probabilities between Alice and Bob averaged over the FSO channel can be respectively formulated as

$$P_{A,B}(a,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_0 - I_a}{\sigma_n}\right) f_{h^a}(h^a)\mathrm{d}h^a, \tag{20}$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_0^\infty Q\left(\frac{I_a - d_1}{\sigma_n}\right) f_{h^a}(h^a)\mathrm{d}h^a, \tag{21}$$

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

where $Q(.) \cong \frac{1}{\sqrt{2\pi}} \int_0^\infty \exp(-t^2/2)\mathrm{d}t$ is the Gaussian Q-funciton, σ_n^2 is the total noise variance [Eq. (16)], and I_a represents the received current signal without noise for bit "a," which can be expressed as

$$\begin{cases} I_0 = \overline{g}\Re\sqrt{P_R P_{\mathrm{LO}}} = \overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l h^a G_R P_{\mathrm{LO}}}, \\ I_1 = -\overline{g}\Re\sqrt{P_R P_{\mathrm{LO}}} = -\overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l h^a G_R P_{\mathrm{LO}}}. \end{cases} \tag{22}$$

Here, we employ the dual-threshold selections to determine the detection thresholds d_0 and d_1 in Eqs. (20) and (21) as follows:[8]

$$\begin{cases} d_0 = E[i_0] + \varsigma\sqrt{\sigma_n^2}, \\ d_1 = E[i_1] - \varsigma\sqrt{\sigma_n^2}, \end{cases} \tag{23}$$

where ς is the dual-threshold (D-T) scale coefficient. $E[i_0]$ and $E[i_1]$ are the mean value of i_0 and i_1, respectively. Therefore, $E[i_0] = \overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l G_R P_{\mathrm{LO}}}$ and $E[i_1] = -\overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l G_R P_{\mathrm{LO}}}$. We consider $E[h_c] = E[\frac{1}{\mathrm{FSL}} h^l h^a] = E[\frac{1}{\mathrm{FSL}} h^l]$ with $E[h^a] = 1$.

The closed-form expressions for the joint probability in Eqs. (20) and (21) could be determined using the Gaussian–Laguerre quadrature method $\int_0^\infty g(y)\exp(-y)\mathrm{d}y \approx \sum_{l=1}^V \nu_l g(\tau_l)$ respectively as follows:

$$P_{A,B}(a,0) = \frac{1}{2}\sum_{u=1}^{U}\sum_{v=1}^{V} a_u \xi_u^{-b_u} \nu_v \tau_v^{b_u - 1} \times Q\left(\frac{d_0 \mp \overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l \frac{\tau_v}{\xi_u} G_R P_{\mathrm{LO}}}}{\sigma_{n-u,v}}\right), \tag{24}$$

$$P_{A,B}(a,1) = \frac{1}{2}\sum_{u=1}^{U}\sum_{l=1}^{V} a_u \xi_u^{-b_u} \nu_v \tau_v^{b_u - 1} \times Q\left(\frac{\pm\overline{g}\Re\sqrt{\frac{1}{\mathrm{FSL}} G_T P_T h^l \frac{\tau_v}{\xi_u} G_R P_{\mathrm{LO}}} - d_1}{\sigma_{n-u,v}}\right), \tag{25}$$

where

$$d_0 = E[I_0] + \varsigma\sqrt{\sigma_{n-u,v}^2}, \tag{26}$$

and

$$d_1 = E[I_1] - \varsigma\sqrt{\sigma_{n-u,v}^2}, \tag{27}$$

and

$$\sigma_{n-u,v} = \sqrt{2 q_e \overline{g}^{2+x}(\Re P_{\mathrm{LO}} + I_d)\Delta f + \frac{4 k_B T}{R_L}\Delta f}. \tag{28}$$

In the closed-form expressions, a_u, b_u, and ξ_u are the parameters of a mixture-Gamma (MG) distribution estimated to approximate the GG distribution. U is the number of mixture components. ν_v and τ_v are the weight factors and abscissas of the Laguerre polynomials with

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

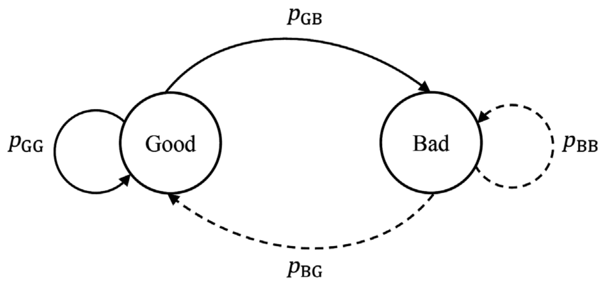

Fig. 5 The link-state transition model.

V is the number of iteration to numerically approximate Laguerre integration.[22] It is noted that $U = V = 10$ gives precise results for this approximation.

3.3 *Link-State Model*

In this section, we propose a two-state Markov model to describe the FSO link-state transition. The model is widely acknowledged as a reasonably accurate and mathematically flexible approach with wireless channels.[23,24] With the two-state model, time is discretized into slots, and the period of each slot is the transmission time of a bit sequence, which is created by Alice's key generator. Therefore, we divide the link into states. Link alternates between a good state (in which all sifted keys are transmitted error-free) and a bad state (in which all transmissions are failed). It is worth noting that the intervals of all link-state are equal to the time of each slot and shorter than the atmospheric turbulence coherent time. Following a geometric distribution, the residence time of each state is shown in Fig. 5.

Next, we consider the QKER, where keys are formed with $l_{\mathrm{bs}}P_{\mathrm{sift}}$ transmitted bits. Without any coding on this key, the key error probability at a given instantaneous QBER from Eq. (18) is given as

$$\mathrm{QKER} = 1 - (1 - \mathrm{QBER})^{l_{\mathrm{bs}}P_{\mathrm{sift}}}, \tag{29}$$

where l_{bs} is the length of a random bit sequence. Thus, the link-state transition probabilities are calculated as

$$\begin{cases} p_{\mathrm{BB}} = \mathrm{QKER}\left(1 - \frac{\tau_{\mathrm{bs}}}{\tau_0}\right), \\ p_{\mathrm{GG}} = (1 - \mathrm{QKER})\left(1 - \frac{\tau_{\mathrm{bs}}}{\tau_0}\right), \\ p_{\mathrm{BG}} = 1 - p_{\mathrm{BB}}, \\ p_{\mathrm{GB}} = 1 - p_{\mathrm{GG}}, \end{cases} \tag{30}$$

where $\tau_{\mathrm{bs}} = \frac{l_{\mathrm{bs}}}{R_b}$ is the transmission time of a bit sequence, which is equivalent to the time of each slot. R_b is the system's bit rate. $\tau_0 = \frac{\sqrt{\lambda L_\beta}}{w}$, is the atmospheric turbulence coherent time defined as the interval of time that the same scintillation coefficient is maintained. λ is the optical wavelength and w is the average wind speed transverse to the propagation direction. $L_\beta = (H_\beta - H_G)\cos(\zeta)$ is the propagation path distance that is equivalent to the transmission distance in the atmospheric environment.[25]

4 Performance Analysis

In this section, the performance parameters considered are KLR, link utilization, and delay outage rate. The KLR is the ratio of lost bit sequences over the bit sequences being sent by Alice's key generator. Link utilization is the number of bit sequences transmitted successfully per τ_{bs}. Delay outage rate is the ratio of received bit sequences with delay jitter exceeding a prescribed threshold.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

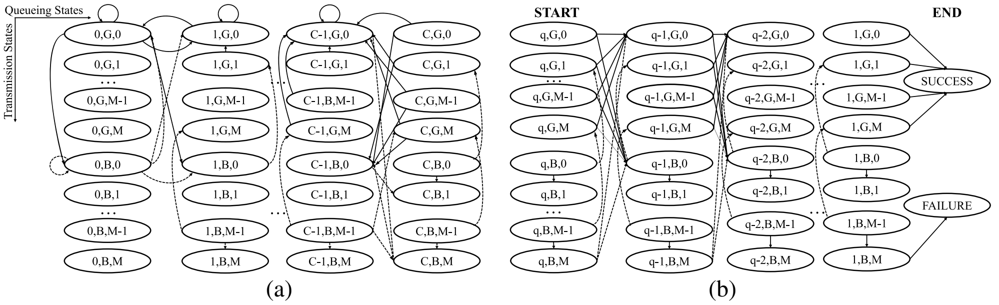

Fig. 6 The states transition probabilities of (a) the QKD queue-associated DTMC and (b) the QKD bit sequence-associated DTMC.

In the analysis, without loss of generality, we list all our operating assumptions.

(1) If Alice's buffer is full, the additional arriving bit sequences will be dropped and will not be recovered by the key retransmission scheme.

(2) An instantaneous and perfect RF uplink channel is assumed. Therefore, Alice's buffer knows whether the transmission was successful or not at the end of each time slot. Bit sequences that were not successfully received are immediately retransmitted in the next time slot to reduce the delay jitter.

(3) The delay jitter of a bit sequence is mainly due to queuing delay in Alice's buffer since the throughput of the FSO link with the key retransmission scheme is highly dynamic, and the FSO link is presumable to be the bottleneck link. Accordingly, the delay outage rate equals the probability that a bit sequence's queuing delay at Alice's buffer exceeds the maximum tolerable delay jitter.

4.1 *Key Loss Rate and Link Utilization*

At Alice's key generator, the bit sequence is created and transmitted to her buffer with the arrival rate of H bit sequences per second. The arrival process of bit sequence at Alice's buffer can be approximated by a stationary Bernoulli process. Therefore, $p_{\mathrm{ar}} = H\tau_{\mathrm{bs}}$ and $p_{\mathrm{no}} = 1 - H\tau_{\mathrm{bs}}$ are the probability of a bit sequence and no bit sequence arrival in a given time slot, correspondingly. Where τ_{bs} is the bit sequence transmission time as above mentioned, i.e., the time of each slot.

Assuming that, during the transmission time of a bit sequence, the link condition remains at its current state. When Alice's buffer is not empty, a bit sequence is forwarded at the beginning of the slot. The bit sequence will be removed at the end of the slot if the transmission is successful.

At the beginning of each slot, a three-dimensional discrete time Markov chains (DTMC) are determined as (n, s, m), i.e., the state space of this DTMC. Where $n \in [0, C]$ is the number of bit sequences in Alice's buffer, $s \in \{G, B\}$ denotes the link-state, and $m \in [0, M]$ represents how many times the currently served bit sequence have been retransmitted. The DTMC is called the QKD queue-associated DTMC. It is noted that states with both $n = 0$ and $m > 1$ are unreachable. The state transition description is shown in Fig. 6(a). Our objective is to generate the state transition probability matrix, i.e., P, of this Markov chain. To do so, we need to compute all possible transition probabilities. In the following, we will discuss how to calculate the transition probability, i.e., $P_{(n,s,m),(k,t,l)}$, from the current state (n, s, m) to the next state (k, t, l).

Link-state can only be either good or bad, i.e., $s \in \{G, B\}$. We proceed the construction of the transition probability by first looking at the good current-state and then consider the bad current-state.

4.1.1 *Good current-state*

- Case 1 (initial state): Alice's buffer is empty, i.e., $n = 0$; thus, the only action is the incoming bit sequence flowing from her key generator to her buffer and no bit sequence is forwarded from her buffer to her transmitter in a given time slot, i.e., $m = 0$ and $l = 0$.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

When no bit sequence arrives at her buffer in this slot, i.e., $k = n$, then

$$\begin{cases} P_{(0,G,0),(0,G,0)} = p_{\text{no}}p_{\text{GG}} = (1 - H\tau_{\text{bs}})p_{\text{GG}}. \\ P_{(0,G,0),(0,B,0)} = p_{\text{no}}p_{\text{GB}} = (1 - H\tau_{\text{bs}})p_{\text{GB}}. \end{cases} \tag{31}$$

Otherwise, when a bit sequence arrives at her buffer in this slot, i.e., $k = n + 1$, then

$$\begin{cases} P_{(0,G,0),(1,G,0)} = p_{\text{ar}}p_{\text{GG}} = H\tau_{\text{bs}}p_{\text{GG}}. \\ P_{(0,G,0),(1,B,0)} = p_{\text{ar}}p_{\text{GB}} = H\tau_{\text{bs}}p_{\text{GB}}. \end{cases} \tag{32}$$

- Case 2: When Alice's buffer size is not full, anymore arriving bit sequences will be queued at her buffer, there is not buffer-overflow. In this case, we consider that her buffer does not overflow, i.e., $n \in [1, C - 1]$ and $m \in [0, M]$. Since the current link-state is good, the currently served bit sequence will be transmitted successfully and removed from her buffer at the end of this slot, i.e., $k = n - 1$. Therefore, at the next state, another bit sequence will be transmitted, i.e., $l = 0$.

When no bit sequence arrives at her buffer in this slot, i.e., $k = n - 1$, then

$$\begin{cases} P_{(n,G,m),(n-1,G,0)} = p_{\text{no}}p_{\text{GG}} = (1 - H\tau_{\text{bs}})p_{\text{GG}}. \\ P_{(n,G,m),(n-1,B,0)} = p_{\text{no}}p_{\text{GB}} = (1 - H\tau_{\text{bs}})p_{\text{GB}}. \end{cases} \tag{33}$$

Otherwise, when a bit sequence arrives at her buffer in this slot, i.e., $k = n$, then

$$\begin{cases} P_{(n,G,m),(n,G,0)} = p_{\text{ar}}p_{\text{GG}} = H\tau_{\text{bs}}p_{\text{GG}}. \\ P_{(n,G,m),(n,B,0)} = p_{\text{ar}}p_{\text{GB}} = H\tau_{\text{bs}}p_{\text{GB}}. \end{cases} \tag{34}$$

- Case 3: When Alice's buffer is full, anymore arriving bit sequences will be discarded at her buffer. In this case, we consider that her buffer is full, i.e., $n = C$ and $m \in [0, M]$. Similarly, the currently served bit sequence will also be transmitted successfully and removed from her buffer at the end of this slot since the current link-state is good, i.e., $k = C - 1$. At the next state, another bit sequence will also be transmitted, i.e., $l = 0$, then

$$\begin{cases} P_{(C,G,m),(C-1,G,0)} = p_{\text{GG}}. \\ P_{(C,G,m),(C-1,B,0)} = p_{\text{GB}}. \end{cases} \tag{35}$$

4.1.2 *Bad current-state*

- Case 4 (initial state): The scenarios in case 4 can be similarly interpreted as in case 1.

When no bit sequence arrives at Alice's buffer in this slot, then

$$\begin{cases} P_{(0,B,0),(0,G,0)} = p_{\text{no}}p_{\text{GG}} = (1 - H\tau_{\text{bs}})p_{\text{BG}}. \\ P_{(0,B,0),(0,B,0)} = p_{\text{no}}p_{\text{GB}} = (1 - H\tau_{\text{bs}})p_{\text{BB}}. \end{cases} \tag{36}$$

Otherwise, when a bit sequence arrives at her buffer in this slot, then

$$\begin{cases} P_{(0,B,0),(1,G,0)} = p_{\text{ar}}p_{\text{GG}} = H\tau_{\text{bs}}p_{\text{BG}}. \\ P_{(0,B,0),(1,B,0)} = p_{\text{ar}}p_{\text{GB}} = H\tau_{\text{bs}}p_{\text{BB}}. \end{cases} \tag{37}$$

- Case 5: In this case, we consider that Alice's buffer does not overflow, i.e., $n \in [1, C - 1]$ and $m \in [0, M - 1]$. Since current link-state is bad, the transmission will be failed thus the currently served bit sequence will be retransmitted in the next time slot, i.e., $l = m + 1$.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

When no bit sequence arrives at her buffer in this slot, i.e., $k = n$, then

$$\begin{cases} P_{(n,B,m),(n,G,m+1)} = p_{\mathrm{no}} p_{\mathrm{BG}} = (1 - H\tau_{\mathrm{bs}}) p_{\mathrm{BG}}. \\ P_{(n,B,m),(n,B,m+1)} = p_{\mathrm{no}} p_{\mathrm{BB}} = (1 - H\tau_{\mathrm{bs}}) p_{\mathrm{BB}}. \end{cases} \tag{38}$$

Otherwise, when a bit sequence arrives at her buffer in this slot, i.e., $k = n + 1$, then

$$\begin{cases} P_{(n,B,m),(n+1,G,m+1)} = p_{\mathrm{ar}} p_{\mathrm{BG}} = H\tau_{\mathrm{bs}} p_{\mathrm{BG}}. \\ P_{(n,B,m),(n+1,B,m+1)} = p_{\mathrm{ar}} p_{\mathrm{BB}} = H\tau_{\mathrm{bs}} p_{\mathrm{BB}}. \end{cases} \tag{39}$$

- Case 6: The bit sequence will be removed from Alice's buffer after M failed attempts. In this case, the number of retransmission reaches M, i.e., $m = M$, and there is no buffer-overflow, i.e., $n \in [1, C - 1]$. Similarly, the transmission will also be failed since link-state is bad, thus the currently served bit sequence will be dropped. At the next state, another bit sequence will be transmitted, i.e., $l = 0$.

When no bit sequence arrives at Alice's buffer in this slot, i.e., $k = n - 1$, then

$$\begin{cases} P_{(n,B,M),(n-1,G,0)} = p_{\mathrm{no}} p_{\mathrm{BG}} = (1 - H\tau_{\mathrm{bs}}) p_{\mathrm{BG}}. \\ P_{(n,B,M),(n-1,B,0)} = p_{\mathrm{no}} p_{\mathrm{BB}} = (1 - H\tau_{\mathrm{bs}}) p_{\mathrm{BB}}. \end{cases} \tag{40}$$

Otherwise, when a bit sequence arrives at her buffer in this slot, i.e., $k = n$, then

$$\begin{cases} P_{(n,B,M),(n,G,0)} = p_{\mathrm{ar}} p_{\mathrm{BG}} = H\tau_{\mathrm{bs}} p_{\mathrm{BG}}. \\ P_{(n,B,M),(n,B,0)} = p_{\mathrm{ar}} p_{\mathrm{BB}} = H\tau_{\mathrm{bs}} p_{\mathrm{BB}}. \end{cases} \tag{41}$$

- Case 7: In this case, we consider that Alice's buffer is full, i.e., $n = C$ and $m \in [0, M - 1]$. Similarly, the currently served bit sequence will also be retransmitted in the next time slot, i.e., $l = m + 1$. The state transition probabilities can be calculated as

$$\begin{cases} P_{(C,B,m),(C,G,m+1)} = p_{\mathrm{BG}}. \\ P_{(C,B,m),(C,B,m+1)} = p_{\mathrm{BB}}. \end{cases} \tag{42}$$

- Case 8: Alice's buffer is full, i.e., $n = C$ and the number of retransmission reaches M, i.e., $m = M$. Similarly, anymore arriving bit sequences will be discarded by her buffer. At the same time, the currently served bit sequence will be dropped and another bit sequence will be transmitted at the next state, i.e., $k = C - 1$ and $l = 0$. The state transition probabilities can be calculated as

$$\begin{cases} P_{(C,B,M),(C-1,G,0)} = p_{\mathrm{BG}}. \\ P_{(C,B,M),(C-1,B,0)} = p_{\mathrm{BB}}. \end{cases} \tag{43}$$

From the transition matrix P, the system performance metrics including KLR and link utilization can be found in closed-form expressions. To do so, we need to solve the steady-state probability of P. Let $(C + 1) \times 2 \times (M + 1)$ be the size of this matrix, i.e., the total number of states of the Markov chain, its steady-state probability vector π can be obtained from the following linear equations as:

$$\begin{cases} \pi^T P = \pi^T \\ \sum_{n=0}^{C} \sum\limits_{s \in B,G} \sum_{m=0}^{M} \pi(n, s, m) = 1, \end{cases} \tag{44}$$

where $\pi = [\pi(n, s, m)]$.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

Using some standard numerical techniques, e.g., Gauss elimination or Jacobi iteration approaches, to solve the aforementioned system of linear equations, we can obtain π, as shown as

$$\pi = [\pi_{(0,G,0)}, \pi_{(1,G,0)}, \dots, \quad \pi_{(C,G,M)}, \pi_{(0,B,0)}, \pi_{(1,B,0)}, \dots, \pi_{(C,B,M)}]. \tag{45}$$

KLR due to the buffer overflow or M failed retransmissions can be determined as follows:

$$\text{KLR} = \sum_{s\in\{B,G\}} \sum_{m=0}^{M} \pi(C,s,m) + \sum_{n=0}^{C-1} \pi(n,B,M). \tag{46}$$

The link utilization, U, can be calculated as

$$U = H(1 - \text{KLR})/C_L, \tag{47}$$

where $C_L = R_b/l_{\text{bs}}$ is the FSO link capacity (bit sequences per second).

4.2 *Delay Performance Analysis*

In this section, we develop another 3-D DTMC to investigate the delay performance. When a bit sequence arrives at Alice's buffer, the queue length (including the target bit sequence) is represented by q. Let (n_D, s_D, m_D) denote the state space of the Markov chain, where $n_D \in [1, q]$, $s_D \in \{B, G\}$, and $m_D \in [0, M]$. Thus, $n_D - 1$ is the number of bit sequences currently being queued in Alice's buffer before the target bit sequence. For instance, if $n_D = q$ and the bit sequence being served is transmitted successfully or discarded by Alice's buffer, $n_D = q - 1$ in the next slot; otherwise, $n_D = q$. Finally, s_D and m_D are the current FSO link-state and how many times the currently served bit sequence being retransmitted, respectively. We divide the time into equal intervals, each spans a one-bit sequence duration τ_{bs}, and the sequence of the states can be described by an embedded Markov chain called a QKD bit sequence-associated DTMC. The state transition trajectories of the QKD bit sequence-associated DTMC are shown in Fig. 6(b). There is an absorbing state at the end of each trajectory, either success or failure, corresponding to the target bit sequence being successfully received by Bob or being discarded after M failed attempts, respectively.

Specially, Table 2 lists the one-step state transition probabilities of the QKD bit sequence-associated DTMC and the j-step transition matrix of the DTMC, P_j equals P_1^j. Therefore, from

Table 2 States transition probabilities of the quantum bit sequence-associated DTMC.

Current state	Next state	Transition probability
(q, G, m)	$(q-1, G, 0)$	p_{GG}
$1 < q \le C$, $0 \le m \le M$	$(q-1, B, 0)$	p_{GB}
$(1, G, m)$ $0 \le m \le M$	Success	1
(q, B, m)	$(q, G, m+1)$	p_{BG}
$1 < q \le C$, $0 \le m < M$	$(q, B, m+1)$	p_{BB}
(q, B, M)	$(q-1, G, 0)$	p_{BG}
$1 < q \le C$	$(q-1, B, 0)$	p_{BB}
$(1, B, m)$	$(1, G, m+1)$	p_{BG}
$0 \le m < M$	$(1, B, m+1)$	p_{BB}
$(1, B, M)$	Failure	1

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

P_j, the probability that the bit sequence is transmitted successfully at the j'th slot after its arrival (defined by $p_{j_{(q,s,m),(\text{success})}}$) can be determined, where (q, s, m) is the initial state associated with the target bit sequence. We can realize that the maximum queuing delay is $[q(M+1)-1]$, if the link-state is in the bad state for $[q(M+1)-1]$ consecutive slots and changes to the good state at the $q(M+1)$'th slot. The minimal queuing delay at Alice's buffer is $q-1$ if the link-state is in the good state for q consecutive slots.

Denote D as the maximum delay jitter that the key transmission requirements can tolerate. Consequently, the conditional probability that the queuing delay of a successfully received bit sequence is larger than D/τ_{bs} slots is calculated as

$$Pr\{t_Q > D/\tau_{\text{bs}} | (q,s,m)\} = \frac{\sum_{j=D/\tau_{\text{bs}}+2}^{q(M+1)} p_{j_{(q,s,m),(\text{success})}}}{\sum_{j=q}^{q(M+1)} p_{j_{(q,s,m),(\text{success})}}}, \tag{48}$$

where t_Q denotes the queuing delay at Alice's buffer.

It is important to note that $(1, G, 1), \ldots, (1, G, M)$ and $(1, B, 1), \ldots, (1, B, M)$ are invalid initial states, and the probability of being in one of these states initially is zero. The probability of the initial state associated with the bit sequence can be determined as the steady-state probability of the QKD queue-associated DTMC normalized by the sum of all possible initial states as follows:

$$Pr\{(q,s,m)\} = \pi(q-1,s,m)/\pi_v, \tag{49}$$

where

$$\pi_v = \sum_{s\in\{B,G\}} \pi(0,s,0) + \sum_{q=2}^{C} \sum_{s\in\{B,G\}} \sum_{m=0}^{M} \pi(q-1,s,m), \tag{50}$$

and $\pi(q-1, s, m)$ has been determined in Sec. 4.1.

From Eqs. (48)–(50), the probability of queuing delay exceeding D/τ_{bs} slots can be expressed as

$$\begin{aligned} Pr\{t_Q > D/\tau_{\text{bs}}\} &= Pr\{t_Q > D/\tau_{\text{bs}} | (q,s,m)\} Pr\{(q,s,m)\} \\ &= \frac{1}{\pi_v} \left[\sum_{s\in\{B,G\}} Pr\{t_Q > D/\tau_{\text{bs}} | (0,s,0)\} \pi(0,s,0) \right. \\ &\quad \left. + \sum_{q=2}^{C} \sum_{s\in\{B,G\}} \sum_{m=0}^{M} Pr\{t_Q > D/\tau_{\text{bs}} | (q-1,s,m)\} \pi(q-1,s,m) \right]. \end{aligned} \tag{51}$$

The KLR consists of both the key drop rate and the key error rate due to buffer overflow and transmission errors, respectively. Although the key drop rate induced by buffer overflow can be reduced due to larger Alice's buffer size (C); however, more delay and delay jitter are introduced. Similarly, a larger M helps to reduce the key error rate and increase the link utilization; nevertheless, it also results in more delay and delays jitter. Hence, the tradeoff between key transmission requirements and system utilization should be considered while choosing the values of C and M. The delay outage probability given by Eq. (51) should be bounded. Therefore, the system parameters C and M can be optimized according to the FSO link-state profile to maximize the link utilization under the key transmission constraint. This will be discussed in detail in the following section.

5 Numerical Results

In this section, we present the numerical results to illustrate the effect of system parameters on the performance of the key retransmission scheme. We also compare our proposed system

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

Table 3 System parameters and constants.

Name	Symbol	Value
Constants and receiver parameters		
Boltzmann constant	k_B	1.38×10^{-23} W/K/Hz
Electrons charge	q_e	1.6×10^{-19} C
Load resistor	R_L	50 Ω
Bit rate	R_b	10 Gbps
Excess noise factor	x	0.8 (InGaAS APD)
Avalanche multiplication factor	$\overline{g}$	10
Responsivity of the APD	$\mathfrak{R}$	0.8
Receiver temperature	T	298 K
Dark current	I_d	3 nA
Channel parameters		
Scattering coefficient (clear air)	γ	0.1 km^{-1}
Wind speed	w	21 m/s
Wavelength	λ	1550 nm
Satellite altitude	H_S	600 km
Ground station height	H_G	5 m
Atmospheric altitude	H_β	20 km
Zenith angle	ζ	50°
Tx telescope gain	G_T	110 dB
Rx telescope gain	G_R	110 dB
Fog visibility	V_{fog}	50 m
Fog layer thickness	L_{fog}	50 m
Rain rate	R_{rain}	50 mm/h
Rain layer thickness	L_{rain}	1000 m
Cloud attenuation	A_{cloud}	34.04813 dB
Link-layer parameters		
Length of bit sequence	l_{bs}	5×10^7 bit
Maximum delay jitter	D	80 ms

(with the key retransmission scheme) and conventional systems (without key retransmission scheme). The system parameters and constants used in the analysis are given in Table 3. For atmospheric turbulence channels, the values of $C_n^2(0) = 5 \times 10^{-15}$ and $C_n^2(0) = 7 \times 10^{-12}$ correspond to the weak and strong turbulence conditions, respectively. In addition, the D-T scale coefficients are fixed at 0.7 for the case of weak turbulence and 1.4 for the case of strong turbulence. These coefficients are chosen so that QBER obtains the low values. Regarding atmospheric attenuation, all figures are obtained for the case of clear air except for Fig. 7, which focuses on the impact of fog, rain, and cloud.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

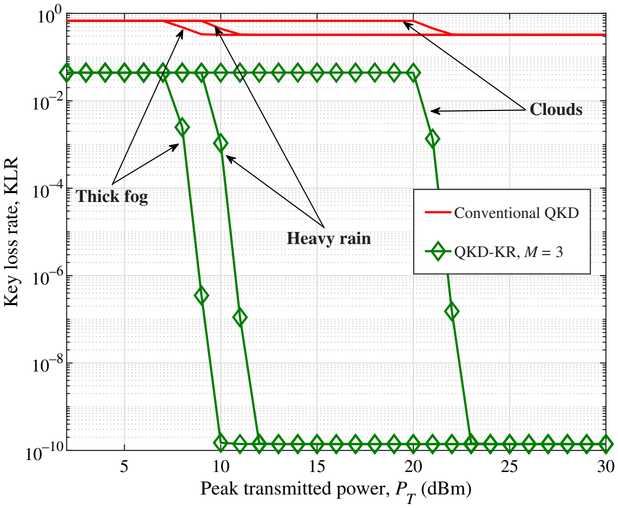

Fig. 7 The KLR for various weather conditions versus peak transmitted power (P_T) under weak turbulence condition with $P_{\mathrm{LO}} = 0$ dBm, $H = 65$ sequence/s, $C = 10$ sequences, $G_T = 110$ dB, and $G_R = 120$ dB.

5.1 *Key Loss Rate*

Figure 7 shows the KLR versus the peak transmitted power (P_T) under different weather conditions and weak turbulence. In this case, Tx and Rx telescope gains are fixed to 110 and 120 dB, respectively. It is clearly seen that the conventional QKD system (i.e., without key retransmission) is severely affected by bad weather conditions such as fog, rain, and cloud. Consequently, the KLR is very high, almost equals to 1 in spite of high transmitted power. Due to key retransmission, the KLR is significantly reduced to nearly 10^{-10} with $M = 3$. We also find that KLR is mostly affected by clouds rather than fog or rain. The transmitted power that is required to satisfy the condition KLR $\leq 10^{-6}$ is 23 dBm for the case of cloud condition, whereas it is 9 dBm for the case of fog condition.

Figure 8 investigates the KLR performance versus peak transmitted power P_T under weak [Fig. 8(a)] and strong [Fig. 8(b)] turbulence conditions. We compare KLR of the QKD system without retransmission and that of the one using the key retransmission (QKD-KR) with the number of retransmission $M = \{1,2,3,4,5,6,7\}$. In Fig. 8(a), without key retransmissions, KLR is relatively high due to the impact of atmospheric turbulence. More specifically, the lowest value of KLR is 3×10^{-1} even with high transmitted power. Due to key retransmissions, the KLR is reduced with the increase of the number of retransmission. For a given KLR, the increase of M also results in the reduction of required transmitted power. This is very useful for the case of strong turbulence shown in Fig. 8(b) because higher transmitted power is required.

To evaluate the advantage of key retransmission, we defined the power gain that is the difference of required peak transmitted power to ensure KLR $= 10^{-6}$. Considering Fig. 8(b), when the number of retransmission increases from 1 to 4, the power gain is 2.5 dB. This is because the large number of retransmission can compensate for the key loss and thus relieve the need in increasing the transmitted power. Nevertheless, the power gain is only 0.2 dB when M increases from 4 to 7. Accordingly, the benefit of using the number of retransmission more than 4 is not significant. Also, retransmission causes the delay, thus M should not be too large.

One of the targets for QKD system design is to control the KLR, e.g., KLR $\leq 10^{-2}$, and thus guarantees the quality of key transmission. Based on this condition, the minimum peak transmitted power can be determined from Fig. 8. For instance, with $M = 3$, we can determine that the minimum transmitted power should be 11 dBm under weak turbulence conditions and 12 dBm under strong turbulence conditions. It is worth noting that the transmitted power should not be larger than a specific value as the KLR reaches the floor.

Figure 9 shows the KLR performance versus arrival rate H with system setting as $P_T = 11$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $C = 10$ bit sequences under (a) weak and (b) strong

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

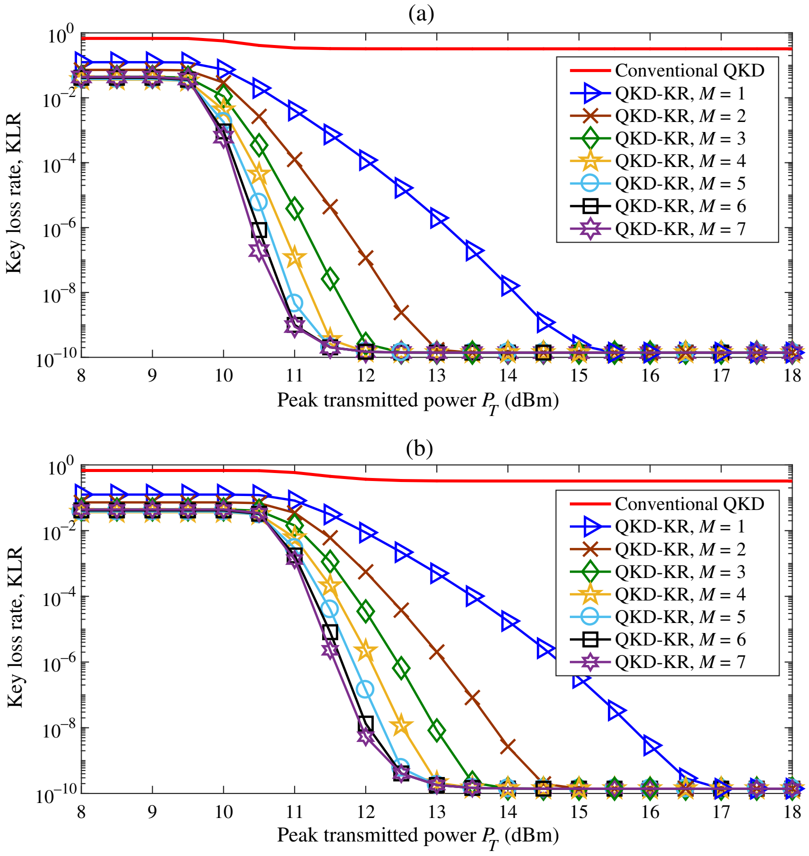

Fig. 8 The KLR versus peak transmitted power (P_T) under (a) weak and (b) strong turbulence conditions with $P_{\mathrm{LO}} = 0$ dBm, $H = 65$ sequence/s, and $C = 10$ sequences.

turbulence conditions. First, we confirm that the KLR reduces due to the use of the key retransmission. Second, the KLR becomes worse when the arrival rate increases. This is because, with a higher arrival rate, the probability of that the Alice's buffer is full increases faster. The additional arriving bit sequences will be dropped when Alice's buffer is full. Consequently, the KLR will be increased because it is governed by both the key error rate and the key drop rate. Third, when the arrival rate reaches a certain level, the use of the key retransmission scheme does not bring the advantage compared to conventional QKD system without key retransmission. Therefore, the utilization of key retransmissions is recommended when $H < 180$ for both turbulence conditions.

Quantitatively, it is clear in Fig. 9 that using the key retransmission scheme improves KLR performance in low arrival rates; however, the performance becomes worse when arrival rate exceeds a certain level. This is due to the fact that, in low arrival-rate region, KLR is mainly governed by PHY transmission errors. Therefore, these errors can be mitigated due to key retransmission. It, however, causes the increase in LINK service time due to a higher number of transmissions needed. Specially, the probability that Alice's buffer is full increases with the traffic intensity and thus it is proportional to the LINK service time and the arrival rate. Consequently, for high arrival rate, the use of key retransmission does not help to reduce the KLR. In addition, the number of key retransmissions (M) should be properly selected. Clearly, a higher value of M results in smaller KLR when H is low; however, this also causes a higher delay and a larger buffer size.

The KLR versus Alice's buffer size C for different turbulence conditions are shown in Fig. 10. With small Alice's buffer size, most bit sequences can be successfully transmitted in M attempts and bit sequences losses are mainly due to buffer overflow. Intuitively, we can see that the KLR improves with an increase in Alice's buffer size. This is because, larger Alice's buffer size can hold more bit sequences in the queue, i.e., the number of bit sequences in Alice's

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

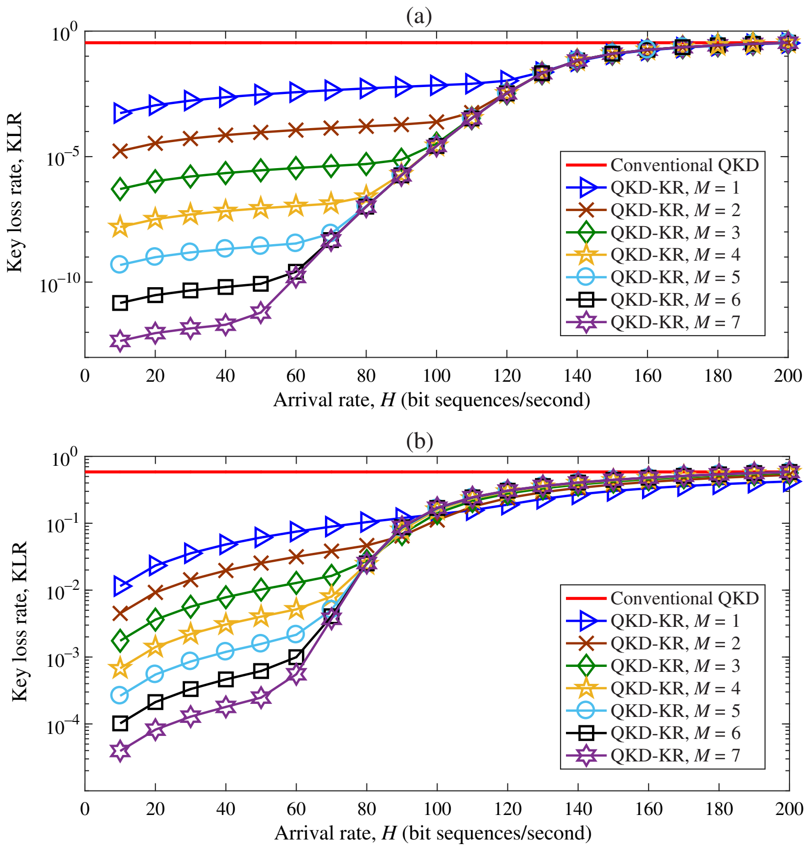

Fig. 9 The KLR versus arrival rate (H) under (a) weak and (b) strong turbulence conditions with $P_T = 11$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $C = 10$ sequences.

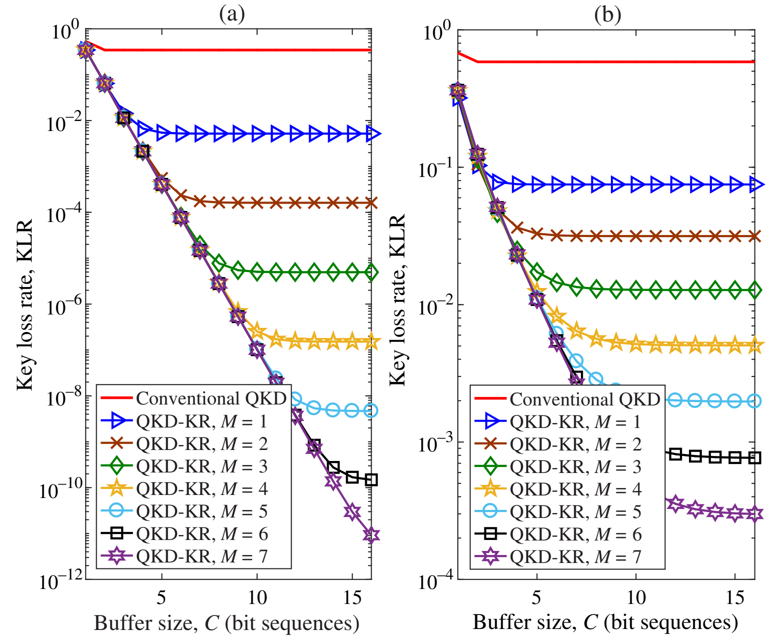

Fig. 10 The KLR versus Alice's buffer size (C) under (a) weak and (b) strong turbulence conditions with $P_T = 11$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $H = 80$ sequence/s.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

buffer waiting to be served can be increased. Consequently, the probability of buffer overflows is smaller. Nevertheless, when Alice's buffer size exceeds a certain level, the KLR reaches the minimum value. In this case, the losses are only those bit sequences being discarded by Alice's buffer when M attempts failed. To keep KLR $\leq 10^{-2}$, we can determine that Alice's buffer size should be >3 under weak turbulence conditions [Fig. 10(a)] and >5 under strong turbulence conditions [Fig. 10(b)].

5.2 *Link Utilization*

This section shows the analytical and numerical results of FSO link utilization, which can also be viewed as normalized flow throughput.

Figure 11 shows the impact of different turbulence conditions on the link utilization U along with the selection of arrival rate H. As can be observed from this figure that the QKD system utilizing key retransmission provides much better link utilization than the one without key retransmission. Again, the cost of using key retransmission can be seen clearly when the arrival rate exceeds a certain level. Because of large arrival rate, the additional traffic induced by the larger number of retransmission (M) leads to higher KLR and thus the link utilization is respectively decreased. Therefore, it is necessary to choose the suitable value of M to get better link utilization. Clearly, higher values of M result in higher link utilization when $H < 100$ for weak turbulence conditions [Fig. 11(a)] and $H < 80$ for strong turbulence conditions [Fig. 11(b)]. Nevertheless, the deference in link utilization for higher values of M is not significant. In the case of large arrival rate, i.e., $H > 100$ or $H > 80$, M should be one.

Figure 12 shows the link utilization U versus Alice's buffer size B with the system setting as $P_T = 10$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $H = 60$ sequence/s under (a) weak and (b) strong turbulence conditions. Intuitively, we also realize that the link utilization of the conventional QKD system is much smaller than the QKD-KR system. Also, the link utilization increases with the Alice's buffer size C as the increase of C helps to solve the problem of buffer overflow. The link utilization, however, reaches the ceiling when C is large enough. In that case, increasing the number of retransmission is a solution to improve the link utilization. However, the gain in link utilization that we obtain is not significant when M increases from 2 to 7. Therefore, we should choose $M = 2$. In addition, the impact of different turbulence conditions on the link

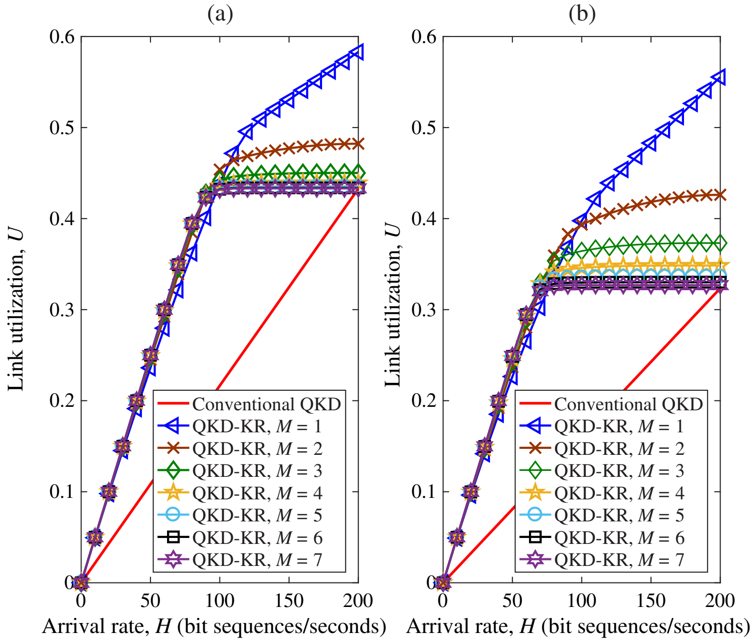

Fig. 11 The link utilization (U) versus arrival rate (H) under (a) weak and (b) strong turbulence conditions with $P_T = 10$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $C = 10$ sequences.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

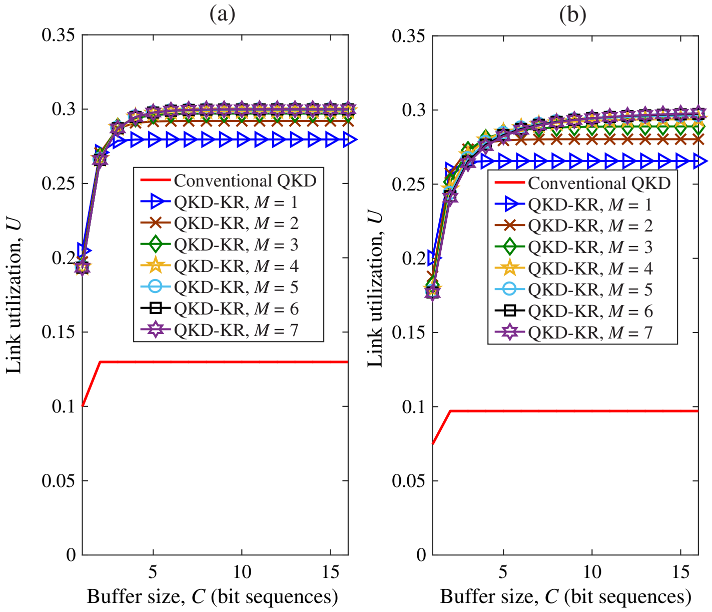

Fig. 12 The link utilization (U) versus Alice's buffer size (C) under (a) weak and (b) strong turbulence conditions with $P_T = 10$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $H = 60$ sequence/s.

utilization is also shown in this figure, clearly. The link utilization is lower under strong turbulence conditions due to larger BER and larger KLR induced.

5.3 *Delay Outage Rate*

In this section, the analytical results of delay outage rates (the ratio of bit sequences with delay jitter t_Q larger than D) are considered. In the conventional QKD system, the queuing delay is negligible since without the key retransmission, the arrival rate is much lower than the FSO link capacity. This leads to the fact that the queue of Alice's buffer does not build up and thus there is no buffer overflow. Consequently, the delay outage rate of the conventional QKD system is zero.

Figure 13 shows the delay outage rate versus arrival rate H under different turbulence conditions, with $P_T = 11$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $C = 10$ bit sequences. We can see that the delay outage rate increases with the arrival rate. This is because the increase of arrival rate leads to the increase of buffer occupancy and queuing delay. Consequently, the ratio of successfully received bit sequences with a delay jitter $t_Q > D$ is large. Nevertheless, the delay decreases when the arrival rate reaches a certain level. For high arrival rates, most of the losses are those bit sequences being discarded due to buffer overflow. The delay outage rate is, therefore, reduced due to the ratio of successfully received bit sequences reduces. However, the link utilization in this case is low. Also, the trade-off of using key retransmission can be seen clearly in Fig. 13.

The delay outage rate versus Alice's buffer size C under weak (a) and strong (b) turbulence conditions are shown in Fig. 14, given $P_T = 11$ dBm, $P_{\mathrm{LO}} = 0$ dBm, and $H = 65$ sequence/s. Basically, for both turbulence conditions, when the buffer size increases, the delay outage rate becomes worse. This is because, in the case of large buffer size, the queue can accommodate more bit sequences while still keeping one for retransmission at the head until they receive successfully key retransmission feedback (ACK) from Bob. This forces the new bit sequences to wait for a long time in the queue, i.e., large queuing delay. With a targeted delay outage rate, e.g., smaller than 10^{-2}, the figure helps to determine the maximum value of buffer size while its minimum value is obtained from Fig. 10. Under weak turbulence conditions, the maximum values of buffer size corresponding to different values of M are trivial while they are much different under strong turbulence conditions. This is due to the fact that strong turbulence conditions cause high KLR and hence key retransmission plays very important role in FSO/QKD systems. Smaller values of M require larger maximum values of buffer size and vice versa.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

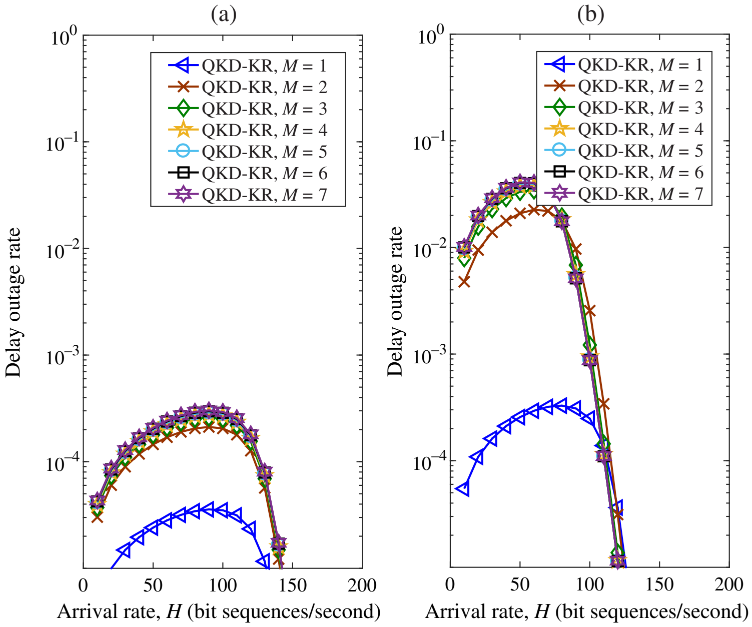

Fig. 13 The delay outage rate versus arrival rate (H) under (a) weak and (b) strong turbulence conditions with $P_T = 11$ dBm, $P_{\text{LO}} = 0$ dBm, and $C = 10$ sequences.

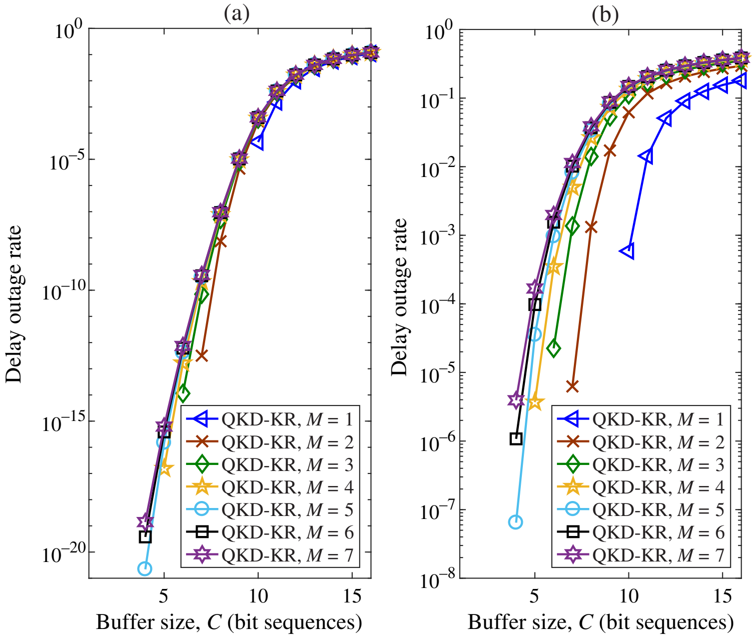

Fig. 14 The delay outage rate versus Alice's buffer size (C) under (a) weak and (b) strong turbulence conditions with $P_T = 11$ dBm, $P_{\text{LO}} = 0$ dBm, and $H = 65$ sequence/s.

6 Conclusions

We did a comprehensive performance analysis of satellite-to-ground FSO/QKD systems using key retransmission under weak and strong turbulence conditions. We also derived the mathematical expressions for the KLR, link utilization, and delay outage rate based on two developed 3-D Markov chain models taking into account the impacts of physical layer impairments. Numerical results showed that key retransmission helps to significantly improve the performance of satellite-to-ground FSO/QKD systems especially under strong turbulence conditions. Key

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

retransmission, however, needs proper setup of the parameters including the number of retransmission and the buffer size depending on the peak transmitted power and the arrival rate to achieve performance improvement with low tradeoff.

Acknowledgments

This research was funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant No. 102.02-2019.08.

References

1. H.-L. Yin et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.* **117**(19), 190501 (2016).
2. N. Hosseinidehai et al., "Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook," *EEE Commun. Surveys Tutor.* **21**(1), 881–919 (2019).
3. G. Vallone et al., "Experimental satellite quantum communications," *Phys. Rev. Lett.* **115**(4), 040502 (2015).
4. S.-K. Liao et al., "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.* **120**(3), 030501 (2018).
5. N. Gisin et al., "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145 (2002).
6. L. B. Samuel and V. L. Peter, "Quantum information with continuous variables," *Rev. Mod. Phys.* **77**, 513 (2005).
7. P. V. Trinh and A. T. Pham, "Design and secrecy performance of novel two-way free-space QKD protocol using standard FSO systems," in *IEEE ICC*, Paris, p. 16 (2017).
8. P. V. Trinh et al., "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. B. Minh et al., "Satellite-based free-space quantum key distribution systems using QPSK modulation and heterodyne detection receiver," in *19th ISCIT*, Ho Chi Minh (2019).
10. F. Laudenbach et al., "Continuous-variable quantum key distribution with Gaussian modulation: the theory of practical implementations," *Adv. Quantum Technol.* **1**, 1800011 (2018).
11. T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol 'Cascade'," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E83-A**(10), 1987–1991 (2000).
12. W. T. Buttler et al., "Fast efficient error reconciliation for quantum cryptography," *Phys. Rev. A* **67**(5), 052303 (2003).
13. A. Thangaraj et al., "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory* **53**(8), 2933–2945 (2007).
14. X. Ai, R. Malaney, and S. X. Ng, "A reconciliation strategy for real-time satellite-based QKD," *IEEE Commun. Lett.* **24**, 1062–1066 (2020).
15. C. H. Bennett and G. Brassard, "Quantum cryptography: publick key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process,* Bangalore, India, pp. 175–179 (1984).
16. H. Hemmati, *Near-Earth Laser Communications*, CRC Press (2009).
17. M. Alzenad et al., "FSO-based vertical Backhaul/Fronthaul framework for 5G+ wireless networks," *IEEE Commun. Mag.* **56**(1), 218–224 (2018).
18. N. A. M. Nor et al., "Investigation of moderate-to-strong turbulence effects on free space optics – a laboratory demonstration," in *13th Int. Conf. Telecommun. (ConTEL)*, Graz, pp. 1–5 (2015).
19. Z. Ghassemlooy et al., "Free-space optical communication using subcarrier modulation in Gamma-Gamma atmospheric turbulence," in *9th ICTON*, Rome, pp. 156–160 (2007).
20. J. Ma et al., "Performance analysis of satellite-to-ground downlink coherent optical communications with spatial diversity over Gamma-Gamma atmospheric turbulence," *Appl. Opt.* **54**(25), 7575–7585 (2015).

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use

21. J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Phys. Rev. A* **67**(2), 022309 (2003).
22. M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions, with Formulas, Graphs, and Mathematical Tables*, 9th ed., Dover, New York (1972).
23. H. Shen, L. Cai, and X. Shen, "Performance analysis of TFRC over wireless link with truncated link-level ARQ," *IEEE Trans. Wireless Commun.* **5**, 1479–1487 (2006).
24. H. S. Wang and N. Moayeri, "Finite-sate Markov channel-A useful model for radio communication channels," *IEEE Trans. Veh. Technol.* **44**(1), 163–171 (1995).
25. A. Navas et al., "Fade statistics of M-turbulent optical links," *J. Wireless Commun. Networking* **2017**, 112 (2017).

Nam D. Nguyen is currently an undergraduate student at the 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 and quantum key distribution.

Hien T. T. Pham received her BE degree from Hanoi University of Transport and Communications in 1999 and her ME and PhD degrees in telecommunication engineering from PTIT in 2005 and 2017, respectively. She has been working at the Department of Wireless Communications of PTIT since 1999. She is currently a senior lecturer at PTIT. Her present research interests are in the area of design and performance evaluation of optical and wireless communication systems.

Vuong V. Mai received his BE degree (Hons.) in electronic telecommunication engineering from PTIT, Vietnam, in 2012, his MS and PhD 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. 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 his BE degree from Hanoi University of Technology, Hanoi, Vietnam, in 1999, and his ME degree from the PTIT, Hanoi, Vietnam, in 2005, both in electronics and telecommunications; and received his PhD in computer science and engineering from the University of Aizu, Aizuwakamatsu, Japan, in 2010. He is currently an associate professor/head at 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. He is a member of IEEE.

Downloaded From: https://www.spiedigitallibrary.org/journals/Optical-Engineering on 10 Jan 2021
Terms of Use: https://www.spiedigitallibrary.org/terms-of-use