PERFORMANCE OF SATELLITE QUANTUM KEY DISTRIBUTION UNDER ATMOSPHERIC TURBULENCE-INDUCED PHASE FLUCTUATIONS

*Nam Nguyen[1], Thang V. Nguyen[2], Ngoc T. Dang[2], Vuong Mai[3]**

[1]*School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, USA*
[2]*Wireless Systems and Applications Lab., Posts and Telecommunications Institute of Technology, Hanoi, Vietnam*
[3]*Bradford-Renduchintala Centre for Space AI, University of Bradford, Bradford, UK*
**v.mai@bradford.ac.uk*

Keywords: FREE-SPACE OPTICS, SATELLITE QUANTUM KEY DISTRIBUTION, ATMOSPHERIC TURBULENCE-INDUCED PHASE FLUCTUATIONS.

Abstract

Satellite FSO/QKD systems employ free-space optical links between satellites and ground stations to achieve long-distance quantum key distribution. However, these systems face challenges from atmospheric turbulence. This paper introduces a theoretical framework to evaluate the influence of phase fluctuations caused by atmospheric turbulence on the system performance. Mathematical expressions for key performance metrics are derived and validated through Monte-Carlo simulations. Using results from the framework, we provide a recommended system setup to fulfil the QKD performance requirements under different atmospheric turbulence conditions.

1. Introduction

Conventional encryption methods relying on classical computational complexities are becoming more susceptible to breaches as computing technologies rapidly advance. Quantum key distribution (QKD) leveraging principles of quantum mechanics presents a robust cryptographic solution to securely distribute secret keys over unsecured communication channels. Although QKD systems using optical fibers are commercially available, their range is currently limited to a few hundred kilometres. Utilizing free-space optical (FSO) links between satellites and ground stations is a promising approach for achieving QKD over long distances. Satellite FSO/QKD systems have the potential to revolutionize secure communications on a global scale [1].

QKD can be classified into two major types: discrete variable (DV) and continuous variable (CV), based on how a quantum bit is encoded. In the former, quantum bits are encoded using discrete states of each photon, such as polarization or phase. The latter allows quantum bits to be encoded using properties of optical waves, such as intensity or phase. DV-QKD requires the utilization of single-photon detectors for quantum bit detection. However, these detectors have low detection efficiency. CV-QKD, on the other hand, employs conventional optical detectors that operate faster and more efficiently. Furthermore, CV-QKD is compatible with standard optical communication technology as it can be implemented using readily available optical components [2]. Coherent detectors can be utilized to implement CV-QKD systems, but one of their limitations is the need for a highly sophisticated phase-stabilized local light [3]. An alternative approach is non-coherent CV-QKD, which employs dual-threshold/direct detection at receivers. This implementation offers a couple of advantages, including simplicity and cost-effectiveness, as it eliminates the need for a phase-stabilized local light [4].

In satellite FSO/QKD systems, atmospheric turbulence presents a significant challenge. It arises from variations in the refractive index of the atmosphere. As a result, atmospheric turbulence leads to fluctuations in both the intensity and phase of optical signals. Extensive research has been conducted to investigate the impact of atmospheric turbulence-induced intensity fluctuations, which are commonly known as fading. However, studies considering phase fluctuations remain limited. This paper introduces a theoretical framework for the performance analysis of satellite FSO/QKD systems, considering atmospheric turbulence-induced phase fluctuations. To the best of our knowledge, this study represents the first attempt to develop such an analytical framework.

Our analytical framework concentrates on satellite FSO/QKD systems utilizing dual-threshold/direct detection that offers a simplified and cost-effective implementation, paving the way for the widespread adoption of QKD on a global scale. We derive mathematical expressions for the quantum bit error rate and probability of sift in the systems, considering various channel factors, including atmospheric turbulence-induced phase fluctuations, and fading, atmospheric attenuation, and geometric spreading loss. We apply a Tatarskii's perturbation approximation theory based on the Rytov's theory to model phase fluctuations and predict its distribution following a Gaussian distribution. To validate the analytical results, we also conduct Monte-Carlo simulations. Based on the obtained results, we provide recommendations for the system setup to meet the QKD performance requirements under various atmospheric turbulence conditions.

https://doi.org/10.1049/icp.2024.0825

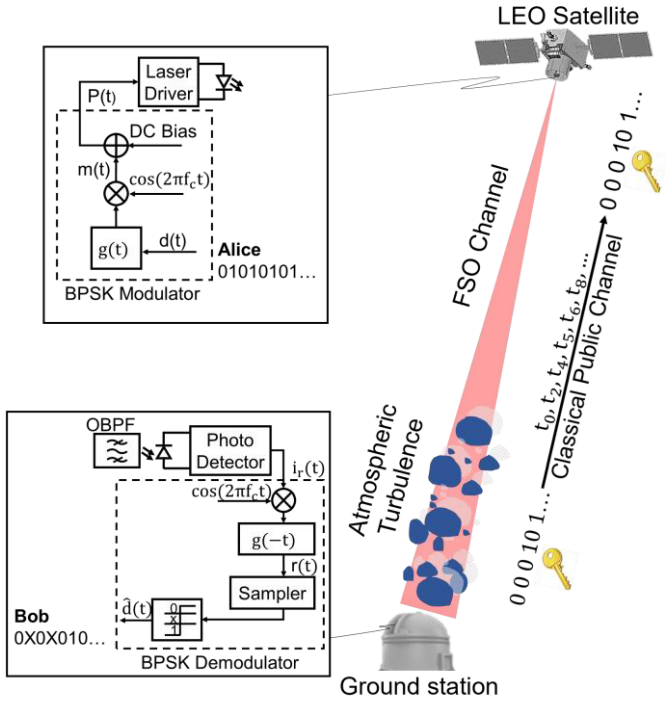

Fig. 1. Block diagram of satellite FSO/QKD system utilizing dual-threshold/direct detection.

2. System Model

The block diagram of satellite FSO/QKD system we consider is illustrated in Fig. 1. In this system, the transmitter (Alice) is located on a low Earth orbit (LEO) satellite, while the receiver (Bob) is positioned at a ground station. To generate signals representing binary random bits "0" or "1", Alice utilizes the subcarrier intensity modulation binary phase shift keying (SIM/BPSK) signalling with a small modulation depth. These signals are then transmitted to Bob over an FSO link. The modulated signals are coherent states that are nonorthogonal to each other, and they function similarly to nonorthogonal bases in the BB84 protocol. The signals are detected using dual-threshold/direct-detection by Bob. Random fluctuations in the received signals over the atmospheric turbulence channel can result in detection outcomes of "0", "X", or "1", where "X" indicates the scenario of incorrect basis selection in the BB84 protocol. Additional information about the FSO/QKD system employing dual-threshold/direct detection can be referenced in [5].

The mathematical models for determining the FSO channel consist of four terms, which are atmospheric attenuation, geometric spreading loss, turbulence-induced fading, and phase fluctuations. The atmospheric attenuation can be calculated based on exponential Beer-Lambert laws. A Gaussian beam profile and a circular detection aperture are assumed to quantify the geometric spreading loss. Hufnagel-Valley model is employed to determine the turbulence profiles in FSO links between satellites and ground stations. Gamma-Gamma distribution is used to model the atmospheric turbulence-induced fading.

The channel coefficient h can be presented as $h=h^l h^t$, where h^l is the channel loss including atmospheric attenuation and geometric spreading loss, and h^t is the atmospheric turbulence-induced fading. The channel coefficient has been intensively studied. For example, details of modelling h^l and h^t can be found in [6]. It is noted that h^t is random variable, and its probability density function (PDF) is denoted as $f_{h^t}(h^t)$.

We can apply Tatarskii's perturbation approximation theory, which is based on Rytov's theory, to develop a model of phase fluctuations [7]. Given the statistical standard deviation of the received signal frequency Δf_{IF}, the phase error is calculated as

$$\Delta\phi(t) = \int_{t}^{t+T_b} 2\pi\Delta f_{IF}(t)dt \tag{1}$$

where T_b is the interval between two successive detections, which can equivalently be interpreted as the bit duration within our system. The phase fluctuations, denoted as $\Delta\phi$, can be modelled following a Gaussian distribution.

$$f_g(\Delta\phi) = \frac{1}{\sqrt{2\pi}\sigma_\phi} e^{\frac{-\Delta_\phi^2}{2\sigma_\phi^2}} \tag{1}$$

where $f_g(\Delta\phi)$ is the PDF of $\Delta\phi$, and σ_ϕ^2 is the variance of the phase error.

$$\sigma_\phi^2 =< \Delta_\phi^2(t) \geq \frac{2\pi\Delta f_{IF}}{f_s} \tag{1}$$

where $f_s=1/T_b=R_b$ is the bit rate.

In following, we focus on deriving mathematical expressions for quantum bit error rate (QBER) and probability of sift (P_{sift}) at Bob's receiver.

QBER represents the percentage of bit errors in the sifted key and can be defined as

$$\text{QBER} = \frac{P_{error}}{P_{sift}} \tag{1}$$

where P_{sift} is the probability that Bob uses the same bases as Alice to detect bits "0" and "1", and P_{error} is the probability that there are erroneous bits in the sifted key, caused by physical-layer impairments and/or Eve's intervention.

$$P_{sift} = P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1) \tag{2}$$

$$P_{error} = P_{A,B}(0,1) + P_{A,B}(1,0) \tag{3}$$

where $P_{A,B}(a,b)$ is the joint probability that Alice sends bit "a" while Bob detects bit "b". These probabilities under the effect

of phase fluctuations and fading induced by atmospheric turbulence can be respectively calculated as

$$P_{A,B}(a,0) = \frac{1}{2}\int_{-\infty}^{\infty}\int_{0}^{\infty} Q\left(\frac{I_a - d_0}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t d_{\Delta\phi} \tag{4}$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_{-\infty}^{\infty}\int_{0}^{\infty} Q\left(\frac{d_1 - I_a}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t d_{\Delta\phi} \tag{5}$$

where $Q(.)$ is the Gaussian Q-function, σ_N is the total noise variance, and I_a is the received current signals for bit "a", d_0 and d_1 are two levels of the dual-threshold which can be selected symmetrically over the "zero" level.

$$\begin{cases} I_0 = -\frac{1}{4} R\bar{g} P_T \delta h^l h^t \cos(\Delta\phi) \\ I_1 = \frac{1}{4} R\bar{g} P_T \delta h^l h^t \cos(\Delta\phi) \end{cases} \tag{6}$$

$$\begin{cases} d_0 = E[I_0] + \varsigma\sqrt{\sigma_N^2} \\ d_1 = E[I_1] + \varsigma\sqrt{\sigma_N^2} \end{cases} \tag{7}$$

where ς is the dual-threshold scale coefficient, $E[I_a]$ is the mean value of I_a, R is the responsivity of the APD, P_T is the peak transmitted power, δ is the intensity modulation depth, $\bar{g}$ is the APD average gain.

It is noted that atmospheric turbulence-induced phase fluctuations and fading are unrelated phenomena. The light intensity experiences irregular changes, while the phase becomes randomized during transmission. Each of these factors has its own distinct distribution. Furthermore, when compared to the high data rates of optical signals (Mbps or Gbps), atmospheric turbulence effects change more gradually. As a result, we can perform a double integration involving the original joint probability and the probability density function of phase fluctuations and fading induced by atmospheric turbulence. This double integration can be regarded as an ergodic process, which can effectively represent the joint probability across all the random changes of light intensity and phase fluctuations [8].

$$\begin{aligned} &P_{A,B}(a,0) \\ &= \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2}\int_{0}^{\infty} Q\left(\frac{I_a - d_0}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t\, d_{\Delta\phi} \\ &+ \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2}\int_{0}^{\infty} Q\left(\frac{I_a - d_0}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t\, d_{\Delta\phi} \end{aligned} \tag{8}$$

$$\begin{aligned} &P_{A,B}(a,1) \\ &= \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2}\int_{0}^{\infty} Q\left(\frac{d_1 - I_a}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t\, d_{\Delta\phi} \\ &+ \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2}\int_{0}^{\infty} Q\left(\frac{d_1 - I_a}{\sigma_N}\right) f_{h^t}(h^t) f_g(\Delta\phi) dh^t\, d_{\Delta\phi} \end{aligned} \tag{9}$$

The closed-form expressions for the joint probability in (8) and (9) could be determined by using the Gaussian-Laguerre quadrature method respectively as follow.

$$\begin{aligned} &P_{A,B}(1,0) \\ &= \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2}\sum_{i=1}^{U}\sum_{l=1}^{V} a_i\, \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \\ &\times Q\left(\frac{\frac{1}{4\xi_i} R\bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi) - d_0}{\sigma_{N-i,l}}\right) f_g(\Delta\phi) d_{\Delta\phi} \\ &+ \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2}\sum_{i=1}^{U}\sum_{l=1}^{V} a_i\, \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \\ &\times Q\left(\frac{\frac{1}{4\xi_i} R\bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi) - d_0}{\sigma_{N-i,l}}\right) f_g(\Delta\phi) d_{\Delta\phi} \end{aligned} \tag{10}$$

$$\begin{aligned} &P_{A,B}(0,0) \\ &= \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2}\sum_{i=1}^{U}\sum_{l=1}^{V} a_i\, \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \\ &\times Q\left(\frac{-\frac{1}{4\xi_i} R\bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi) - d_0}{\sigma_{N-i,l}}\right) f_g(\Delta\phi) d_{\Delta\phi} \\ &+ \sum_{n=-\infty}^{\infty}\int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2}\sum_{i=1}^{U}\sum_{l=1}^{V} a_i\, \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \\ &\times Q\left(\frac{-\frac{1}{4\xi_i} R\bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi) - d_0}{\sigma_{N-i,l}}\right) f_g(\Delta\phi) d_{\Delta\phi} \end{aligned} \tag{11}$$

$$P_{A,B}(1,1) = \sum_{n=-\infty}^{\infty} \int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2} \sum_{i=1}^{U} \sum_{l=1}^{V} a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \times Q\left(\frac{d_1 - \frac{1}{4\xi_i} \mathrm{R} \bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi)}{\sigma_{N-i,l}} \right) f_g(\Delta\phi) d_{\Delta\phi} + \sum_{n=-\infty}^{\infty} \int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2} \sum_{i=1}^{U} \sum_{l=1}^{V} a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \times Q\left(\frac{d_1 - \frac{1}{4\xi_i} \mathrm{R} \bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi)}{\sigma_{N-i,l}} \right) f_g(\Delta\phi) d_{\Delta\phi} \quad (12)$$

$$P_{A,B}(0,1) = \sum_{n=-\infty}^{\infty} \int_{2n\pi-\frac{\pi}{2}}^{2n\pi+\frac{\pi}{2}} \frac{1}{2} \sum_{i=1}^{U} \sum_{l=1}^{V} a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \times Q\left(\frac{d_1 + \frac{1}{4\xi_i} \mathrm{R} \bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi)}{\sigma_{N-i,l}} \right) f_g(\Delta\phi) d_{\Delta\phi} + \sum_{n=-\infty}^{\infty} \int_{2n\pi-\frac{3\pi}{2}}^{2n\pi-\frac{\pi}{2}} \frac{1}{2} \sum_{i=1}^{U} \sum_{l=1}^{V} a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} \times Q\left(\frac{d_1 + \frac{1}{4\xi_i} \mathrm{R} \bar{g} P_T \delta h^l \tau_l \cos(\Delta\phi)}{\sigma_{N-i,l}} \right) f_g(\Delta\phi) d_{\Delta\phi} \quad (13)$$

In the closed-form expressions, the parameters a_i, b_i, and ξ_i correspond to the parameters of a mixture-Gamma distribution. This distribution is used for an effective approximation of Gamma-Gamma distribution. Here, U represents the count of mixture components. The variables v_l and τ_l denote the weight factors and abscissas associated with the Laguerre polynomials, respectively. Additionally, V indicates the number of iterations employed to numerically approximate the Laguerre integration process. It is worth mentioning that adopting U=V=10 yields accurate results for this approximation.

3. Numerical Results

In this section, we provide numerical results based on our theoretical model for quantum bit error rate and probability of sift at Bob's receiver. Furthermore, Monte Carlo simulations are carried out to validate the accuracy of theoretical model. The system parameters and constants used in the analysis are given in Table 1.

Figure 2 illustrates the influence of turbulence-induced phase fluctuations on the overall system performance. We compare the quantum bit error rate and the probability of sift at Bob's receiver across two scenarios: one with phase fluctuations and the other without. These scenarios are evaluated under both weak and strong turbulence conditions. Additionally, we undertake an investigation into the optimization of the setup parameters, specifically focusing on the peak transmitted power and the dual-threshold scale coefficient. To accomplish this, we delve into the relationships between the system performance and the peak transmitted power, as shown in Fig. 2(a), and the dual-threshold scale coefficient, as presented in Fig. 2(b).

Table 1. System parameters and constants

Name	Value
Boltzmann's constant	1.38×10^{-23} W/K/Hz
Planck's constant	6.626×10^{-34}
Electrons charge	1.6×10^{-19} C
Load resistor	1000 Ω
Receiver temperature	300 K
Quantum efficiency	0.62
Ionization factor	0.7 (InGaAS APD)
Amplifier noise figure	2
Attention coefficient	0.43 dB/km
Wavelength	1550 nm
Bit rate	1 Gbps
Zenith angle	50°
Satellite telescope gain	141 dB
Beam divergence angle	52.6 μrad
Ground telescope gain	132 dB
Ground aperture radius	0.31 m
Wind speed	21 m/s
Refractive index structure parameter at the ground level (Weak turbulence)	10^{-17} $m^{-2/3}$
Refractive index structure parameter at the ground level (Strong turbulence)	10^{-12} $m^{-2/3}$

The results highlight that phase fluctuations can cause a considerable reduction in the QKD performance in terms of both QBER and P_{sift}. For instance, to compensate the adverse effects of phase fluctuations and maintain the QBER at the same low level as in the scenario without phase fluctuations, it becomes essential to increase the peak transmitted power by an additional 2.5 dB when the QBER is at 10^{-3}. In the case of a lower QBER, such as 10^{-5}, an additional 5 dB increase is necessary.

For the system design, we can adjust the peak transmitted power and dual-threshold scale coefficient to control QBER and P_{sift}. It is commonly required to achieve a P_{sift} value greater than 10^{-2}, ensuring a satisfactory probability of sifting for Bob to receive information from Alice. At the same time, QBER should be maintained below 10^{-3}, allowing for the feasibility of error-correction codes to correct quantum bit errors. To satisfy these requirements, based on the results in Fig. 2(a), we suggest setting the peak transmitted power >30 dBm under weak turbulence and >32 dBm under strong turbulence in this case. Furthermore, based on the findings presented in Figure

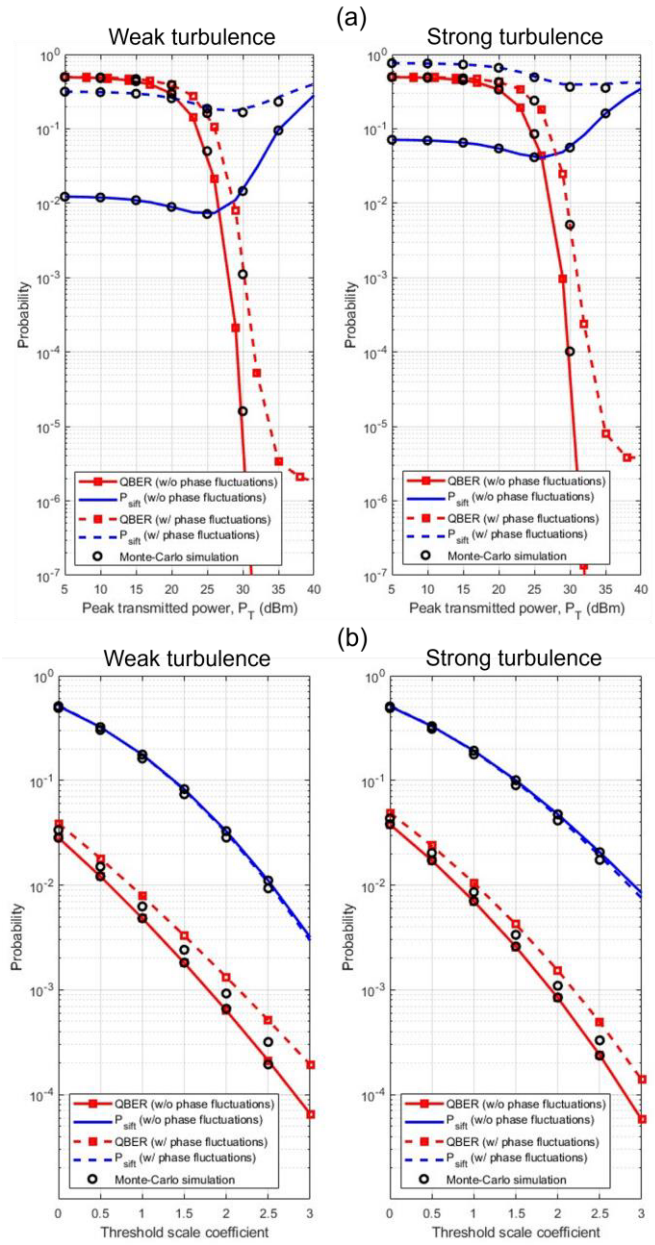

Fig. 2. Quantum bit error rate and probability of sift at Bob's receiver versus (a) peak transmitted power and (b) dual-threshold scale coefficient.

2(b), it is recommended to use a dual-threshold scale coefficient ranging from 2.2 to 2.5 for the system configuration under the condition of weak turbulence. For the scenario involving strong turbulence, the dual-threshold scale coefficient should be set within the range of 2.3 to 2.8.

4. Conclusions

We studied the impact of turbulence-induced phase fluctuations on the performance of a satellite FSO/QKD system that employs dual-threshold direct detection. We formulated the mathematical expressions for the quantum bit error rate and the probability of sift at Bob's receiver. The results confirmed the substantial influence of turbulence-induced phase fluctuations on the system performance. Additionally, we explored the potential for performance enhancement by optimizing the peak transmitted power and the dual-threshold scale coefficient.

Acknowledgements

This research was supported by the Ministry of Information and Communications (Viet Nam) under Grant No. DT.26/23.

References

[1] Liao, S., Cai, W., Liu, W. et al.: 'Satellite-to-ground quantum key distribution', Nature, 2017, 549, p. 43–47.
[2] Hosseinidehaj, N., Babar, Z., Malaney, R. et al.: 'Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook', IEEE Commun. Surv. Tutor., 2019, 21, p. 881–919.
[3] Jain, N., Chin, H., Mani, H. et al.: 'Practical continuous-variable quantum key distribution with composable security'. Nat. Commun., 2022, 13, p. 4740–1–8.
[4] Vu, M., Le, H., Pham, T. et al.: 'Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/direct detection', IEEE Access, 2022, 10, p. 113260–113274.
[5] Trinh, P., Pham, T., Dang, N. et al.: 'Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver', IEEE Access, 2018, 6, pp. 4159–4175.
[6] Nguyen, N., Pham, H., Mai, V. et al.: 'Comprehensive performance analysis of satellite-to-ground FSO/QKD systems using key retransmission', Opt. Eng., 2020, 59, pp. 126102–1–25.
[7] Xie, G., Dang, A., Guo, H.: 'Effects of atmosphere dominated phase fluctuation and intensity scintillation to DPSK system', Proc. IEEE International Conference on Communications, Kyoto, Japan, 2011, pp. 1–6.
[8] Li, M., Li, B., Zhang, X. et al.: 'Investigation of the phase fluctuation effect on the BER performance of DPSK space downlink optical communication system on fluctuation channel', Opt. Commun., 2016, 366, p. 348–252.