Design and Performance of Relay-Assisted Satellite Free-Space Optical Quantum Key Distribution Systems

MINH QUANG VU, (Student Member, IEEE), THANH V. PHAM, (Member, IEEE), NGOC T. DANG, (Member, IEEE), AND ANH T. PHAM, (Senior Member, IEEE)

1Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan
2Posts and Telecommunications Institute of Technology, Hanoi 100000, Vietnam

Corresponding author: Anh T. Pham (pham@u-aizu.ac.jp)

This work was supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant 102.02-2019.08.

ABSTRACT This paper studies the design and performance analysis of relay-assisted satellite free-space optics (FSO) quantum key distribution (QKD) systems for secure vehicular networks. High-altitude platforms (HAPs) equipped with optical amplify-and-forward nodes are used as relay stations. Secrecy performances in terms of quantum bit error rate and ergodic secret-key rate are analytically investigated under the effects of transceiver misalignment, receiver’s velocity variation, receiver noises, and atmospheric turbulence conditions. Based on the analyzed results, the design criteria for the legitimate user are determined so that the security of the considered system could be guaranteed.

INDEX TERMS Atmospheric turbulence, high-altitude platform (HAP), free-space optics (FSO), pointing error, quantum key distribution (QKD), receiver’s velocity variation.

I. INTRODUCTION Information security plays a significant role in communication networks. Traditionally, information privacy is protected mainly by means of cryptographic algorithms performed at the upper layers of the OSI model. The security of those techniques relies on the secrecy of the encryption key, which is shared between two legitimate parties (a.k.a. key distribution) over insecure public channels. In fact, the computational complexity of deriving secrecy key is so overwhelming that the adversary, with current computing power, is almost unable to extract the key in a feasible amount of time. Nonetheless, due to rapid progress in hardware and algorithms, classical key distribution protocols can be compromised in the near future. This indeed urges the need for alternative, more secure key distribution approaches.

Capitalizing on the law of quantum physics, quantum key distribution (QKD) has been considered as a promising method [1], [2]. Depending on how the information is encoded, there are two main kinds of QKD schemes, namely discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). In DV-QKD, the secret key is encoded onto the discrete state (e.g. phase or polarization) of a single photon. DV-QKD can support long-distance key distribution (e.g. up to 421 km over ultralow-loss fibers [3]) at the expense of bulky and expensive single-photon detectors. The CV-QKD, on the other hand, uses continuous variables of the coherent states of weakly amplitude and/or phase-modulated light pulses. Compared to DV-QKD, CV-QKD exhibits a lower implementation complexity as it is compatible with off-the-shelf telecommunication components [4]. As an advantage of this compatibility, a simultaneous CV-QKD and classical communication scheme, where both the bits for classical communication and the cryptographic key are encoded on the same weak coherent pulse and decoded by the same coherent receiver, was proposed and studied in [5], [6]. Recently, this scheme has been experimentally demonstrated over a 25 km single-mode optical fiber by using superposition modulation [7]. CV-QKD also offers higher key generation rates thanks to the use of heterodyne/homodyne detection. This, however, results in a high deployment cost due to the need for a sophisticated phase-stabilized local light. To achieve the QKD function with a simpler setup, intensity modulation
(IM) with dual-threshold/direct detection (DT/DD) has been proposed for fiber CV-QKD systems [8].

While the optical fiber-based QKD has been widely studied with a number of experimental implementations, it can be only used for fixed users. In practice, there are scenarios, such as vehicular networks supporting unmanned aerial vehicles (UAVs) and self-driving vehicles, in which secure users are mostly in mobility. This essentially requires a wireless solution for optical QKD systems. In this regard, free-space optics (FSO) is considered as a promising candidate thanks to its high data-rate, cost-effectiveness, license-free operation, and quick deployment/redemption.

A. RELATED WORKS

FSO/QKD systems have recently gained much interest in terrestrial applications with fixed ground stations [9]–[12] and space communications [13]–[15]. In [9], the feasibility of a 10-km terrestrial FSO/QKD system using BB84 protocol has been demonstrated during the daytime and at night. The potential of free-space links for CV-QKD has also been confirmed through an experiment conducted over a free-space link of 1.6 km [10]. In a recent development, a terrestrial FSO/QKD system over 53 km has been successfully demonstrated [11]. Furthermore, to achieve QKD function with simpler and low-cost implementation, FSO/ CV-QKD systems using DT/DD with subcarrier intensity modulation binary phase-shift keying (SIM/BPSK) have been proposed [12]. The feasibility and reliability of the proposed system have been theoretically confirmed through analyzing the quantum bit error rate (QBER), ergodic secret-key rate, and final key-creation rate.

In the domain of QKD in space communications, several aspects of the feasibility of satellite-based QKD including signal propagation through a turbulence atmosphere, the polarization properties of a satellite-based quantum channel, and the generation rate of secure keys for different configurations and for different protocols have been discussed [13]. In 2016, satellite-based QKD has become a reality with the successful launch of the world’s first quantum satellite, Micius, by China [14]. This satellite is equipped with three payloads, designed and tested to enable a series of space-to-ground-scale quantum experiments including QKD and teleportation. The experimental results obtained during several downlinks from Micius focusing on the performance of the receiving station have been presented in [15]. Satellite-based QKD can enable secure network communications between multiple ground stations if there is an efficient communication scheduling. In [16], a study on how satellite-based QKD can service many ground stations taking into consideration realistic constraints such as geography, operational hour, and weather conditions has been presented. Recently, instead of using fixed ground stations, the world’s first mobile quantum satellite station has been developed in China. The mobile station weighs about 80 kilograms and is small enough to be installed on top of a car [17]. This is a major step towards the commercialization of satellite-based QKD technology.

B. MOTIVATION AND CONTRIBUTIONS

Inheriting the characteristics of FSO, atmospheric conditions, including absorption, scattering, and atmospheric turbulence, are the main factors that significantly limit the transmission distance of FSO/QKD systems. Relaying is thus an appealing solution to extend the operation range. In [18], relay-assisted QKD systems have been initially proposed for fiber-optic DV-QKD systems. Quantum relaying over the FSO channel has been studied for terrestrial transmission, where the authors proposed passive relays equipped with adaptive optics to mitigate the effect of the atmospheric distortion [19]. To expand quantum communications to the global scale, [20] considered several scenarios involving space transmissions among ground stations and satellites, where satellites are relaying nodes. A new architecture for double-layer quantum satellite networks using both geostationary Earth orbit (GEO) and low Earth orbit (LEO) quantum satellite resources to distribute secret keys has been recently proposed in [21]. For such a global scale network, the use of satellites as relays are essential to facilitating the light-of-sight requirement. However, the long-distance between ground stations and satellites is a major challenge, which makes relaying an inevitable solution in reducing the impact of atmospheric impairments.

In this paper, we propose to use high-altitude platforms (HAPs) as relaying stations between LEO satellites (i.e., Alice) and mobile stations (i.e., Bob) in vehicular networks. We also employ the FSO/QKD systems using subcarrier intensity modulation (SIM) binary phase-shift keying (BPSK) with DT/DD scheme. HAPs can be airships, balloons, unmanned or manned aircrafts positioned at the heights of 17 to 25 km. Operating at these altitudes, HAPs exhibit advantageous features of both satellite and terrestrial communications, including large coverage, reasonable operational costs, easy maintenance, and rapid deployment. To reduce the hardware complexity, optical amplify-and-forward relaying is used at HAPs. In [22], the impact of eavesdropper’s location on the ergodic secret-key rate was investigated under moderate-to-strong atmospheric turbulence conditions without pointing error. Due to the mobility nature of the considered system, however, pointing error and variation of users’ velocities are of importance in realistically evaluating the secrecy performances. Therefore, for a thorough analysis, these factors are taken into consideration in this paper. Explicitly, the main contributions of the paper are as follows

- The statistical channel between an LEO satellite (Alice) and a moving ground vehicle is characterized. In our considered system, the ground vehicle can be either a legitimate user (Bob) or an eavesdropper (Eve). The channel is modeled taking into consideration geometric loss, pointing error effects between Alice and HAP as well as between HAP and Bob/Eve over weak-to-strong atmospheric turbulence conditions. Specifically, the pointing error between HAP and Bob caused by
both mechanical errors (e.g. errors in the tracking system or vibration of the transceiver) and variation of user’s velocity is newly derived.

- In addition to the ergodic secret-key rate, the QBER is derived based on the statistical models of Bob’s and Eve’s channel. Extensive numerical results are illustrated to show the effects of transceiver misalignment, Bob’s velocity variation, atmospheric turbulence, receiver noises, and Eve’s location on the considered secrecy performances. We also implement Monte-Carlo (M-C) simulations to verify the accuracy of the analytical derivations.

C. PAPER OUTLINE

The rest of the paper is organized as follows. In Section II, we describe the operation of the DT/DD scheme and the proposed HAP-based relay-assisted satellite IM/DD FSO/CV-QKD system. Statistical channel models for Alice-to-HAP and HAP-to-Bob/Eve links are presented in Section III. Secrecy performances in terms of QBER and ergodic secret key-rate are derived in Section IV. Representative numerical and simulation results are displayed in Section V. Finally, we conclude the paper in Section VI.

II. SYSTEM MODEL

A. QKD SYSTEM USING DT/DD RECEIVER

In the original BB84 protocol for DV-QKD systems, Alice first selects a number of secret bits and encodes them into discrete qubits by randomly using either rectilinear or diagonal basis. These qubits are then transmitted to Bob through a quantum channel. At Bob’s side, as he has no information about the used basis, a random one is therefore used to measure received qubits. If Alice and Bob choose the same basis, the corresponding bit value is read correctly. Otherwise, the received qubit is measured randomly by one of two polarization states of Bob’s selected basis. The corresponding bit from this case is discarded after a sifting step, where Alice and Bob announce their choices of bases for encoding and measurement. The remaining bits after this step is known as the sifted key. In following steps, Alice and Bob perform information reconciliation to identify and remove erroneous bits, and, in the privacy amplification, Alice and Bob use hash functions to produce a new, shorter key in which Eve even has less negligible information. The readers are referred to [23] for more details on the BB84 protocol. In the CV-QKD systems using DT/DD, the BB84 protocol can be imitated by the use of a small modulation depth and the dual-threshold detection [12]. In particular, Alice generates SIM/BPSK modulated signals with a small modulation depth $0 < \delta < 1$ accordingly for binary bits ‘0’ and ‘1’. At the Bob side, he uses an DT/DD receiver, i.e two thresholds $d_0$ and $d_1$ to detect the transmitted bits ‘0’ and ‘1’, respectively, as illustrated in Fig. 1, using the following detection rule

\[
\text{Decision} = \begin{cases} 
0 & \text{if } i \leq d_0, \\
1 & \text{if } i \geq d_1, \\
X & \text{otherwise},
\end{cases} \tag{1}
\]

where $i$ denotes the detected value of the received signal, ‘X’ represents the case that Bob is unable to recover the transmitted bit, which is analogous to the case of wrong basis selection in the original BB84 protocol [12]. Bob then informs Alice of the time instants at which he can decode either bit ‘0’ or ‘1’ from the received signal, i.e. the Bob’s received signal is either higher or lower than $d_1$ or $d_0$, respectively. By doing so, Alice and Bob share an identical bit sequence, which is called the sifted key. Finally, similar to the standard BB84 protocol, information reconciliation and privacy amplification are performed by Alice and Bob over the public channel to correct any errors and to generate necessary secret keys.

It should be noted that Bob can appropriately adjust the value of $d_0$ and $d_1$ so that he can control the sifted-key rate. As the eavesdropper (i.e. Eve) is unable to obtain the knowledge of $d_0$ and $d_1$, it is assumed to use the optimal threshold $d_E = 0$ (as depicted in Fig. 2) to obtain the most information possible from Alice. Nevertheless, due to Alice’s small modulation depth, Eve’s error probability is naturally high. Alice, by adjusting the modulation depth, can also purposely increase Eve’s error probability. As a matter of fact, by reducing $\delta$, Eve’s error region is extended, as seen

![FIGURE 1. The PDF of Bob’s received signal with the DT detection.](image_url)

![FIGURE 2. The PDF of Eve’s received signal with the optimal detection.](image_url)
in Fig. 2). This nevertheless also increases the ‘X’ region in the Bob’s detection, i.e. the sifted-key rate is reduced. In summary, the design of CV-QKD systems using DT/DD involves the selection of δ by Alice and DT levels by Bob taking into consideration the channel conditions and system parameters.

**B. HAP-BASED RELAY-ASSISTED FSO/QKD SYSTEM MODEL**

Fig. 3 presents the block diagram of the proposed HAP-based relay-assisted FSO/QKD system using SIM/BPSK and DT/DD receiver. There are three main parts: an LEO satellite (Alice), a relaying HAP that amplifies and relays the signal, and a legitimate vehicle (Bob) that detects the signal received from HAP to retrieve the quantum keys transmitted from Alice. At the satellite, Alice modulates the data d(t) onto a radio frequency (RF) subcarrier signal using BPSK modulation. The subcarrier signal, m(t), is then used to modulate the intensity of a continuous-wave laser beam to generate the subcarrier intensity modulated (SIM) signal P_s(t) = \frac{P}{2}[1 + \delta m(t)], where P is the peak transmitted power, \delta is the IM depth (0 < \delta < 1), which is necessary to avoid the over modulation. The subcarrier signal m(t) = Ag(t)\cos(2\pi f_c t + b_t \pi), where A is the subcarrier amplitude, g(t) is the rectangular pulse shaping function, f_c is the subcarrier frequency, and b_t \in \{0, 1\} represents bit ‘0’ and bit ‘1’. For the sake of simplicity, the power of m(t) is normalized to unity. At HAP, the received optical signal is passed through an optical bandpass filter (OBPF) to reduce background noise. The filtered signal is amplified by an optical amplifier whose gain G_A. The amplified signal is then relayed to Bob.

At Bob’s side, the received optical signal is also first passed through an OBPF before being converted into an electrical signal by a PIN photodetector. The electrical signal at the output of the photodetector can be expressed as

\[ i_i(t) = \frac{1}{2}Re(P h_{pb}(t) G_A h_i(t) [1 + \delta t m(t)]) + n(t), \]

where Re is the responsivity of the photodetector, h_{pb}(t) is the channel coefficient between LEO satellite and HAP, h_i(t) is the channel coefficient between HAP and Bob, and n(t) is the receiver noise. Assuming that h_{pb}(t) and h_i(t) vary slowly enough, which is practically feasible due to the slow fading nature of FSO channels, the DC term \{Re\}P h_{pb}(t) G_A h_i(t) can be removed. The electrical signal i_i(t) is then demodulated as

\[ r(t) = i_i(t)\cos(2\pi f_c t) \]

\[ = \begin{cases} 
  i_0 = \frac{1}{4}Re(P h_{pb}(t) G_A \delta h_i(t) + n(t)), & P \\
  i_1 = \frac{1}{4}Re(P h_{pb}(t) G_A h_i(t) + n(t)),
\end{cases} \]

where i_0 and i_1 denote the photocurrent for bit ‘0’ and bit ‘1’, respectively. It is assumed that the dark current is negligible, thus the receiver noise consists of shot noise, background noise, and amplified spontaneous emission (ASE) noise generated by the optical amplifier at HAP. They can be well modeled as zero-mean additive white Gaussian noise (AWGN) with variance \sigma_N^2 = \sigma_{sh}^2 + \sigma_{vb}^2 + \sigma_{vb}^2 + \sigma_{th}^2 + \sigma_a^2, where \sigma_{sh}, \sigma_{vb}^2, \sigma_{vb}^2, \sigma_{th}^2, and \sigma_a^2 are the variances of the shot noise, background noise at HAP, background noise at Bob, thermal noise, and ASE noise, respectively. These variances are calculated as \sigma_{sh}^2 = 2qA g \left( \frac{1}{4} P h_{pb} G_A \delta h_i \right) \Delta f, \sigma_{vb}^2 = 2qA g P h_{pb} \Delta f, \sigma_{th}^2 = \frac{4kT \eta}{\lambda^2}, \sigma_a^2 = 2qA g P h_{vb} \Delta f, where P_{hv} = \frac{\Omega_B \pi a_c^2 \Delta \lambda}{\lambda^2} is the background noise power collected at HAP, P_{hv} = \Omega_B \pi a_c^2 \Delta \lambda is the background noise power at Bob, \Omega_v is the Sun’s spectral irradiance from above the atmosphere, \eta is the aperture radius at HAP, \Omega_v is the Sun’s spectral irradiance from above the Earth, \Omega_B is the aperture radius around Bob, \Delta \lambda = \frac{h c}{\nu}, B_0 is the optical bandwidth, \nu is the operating wavelength, c is the speed of light in vacuum. P_a = \frac{h c}{\nu} (n_0 - 1) \Omega B_0 is the ASE noise power, where h is the Planck constant, n_0 is the spontaneous emission factor, F_0 is the amplifier noise figure, \Delta f = R_0 \frac{c}{T} is the efficient bandwidth with R_0 is the system bit rate, T is the receiver temperature in Kelvin degree, and R_0 is the load resistance.

**III. CHANNEL MODELS**

**A. CHANNEL MODEL OF SATELLITE-TO-HAP LINK**

The channel between satellite and HAP is characterized by the geometric spread and pointing error due to misalignment. Consider a Gaussian beam, the normalized spatial distribution of the transmitted intensity at distance L_s from the satellite to HAP is given as

\[ I_{beam}(r_s; L_s) = \frac{2}{\pi W_{L_s}^2} \exp \left( -\frac{2 \|r_s\|^2}{W_{L_s}^2} \right), \]
where \( \rho \) is the radial vector from the satellite’s beam footprint center, \( \| \cdot \| \) is the Euclidean norm, \( L_s = (H_s - H_p) / \cos(\zeta_s) \) with \( H_s \) and \( H_p \) being altitudes of the satellite and HAP, respectively, and \( \zeta_s \) being the zenith angle between them. \( w_{l_s} \) is the beam radius at distance \( L_s \) and can be calculated as \( w_{l_s} = w_{0,s} \left[ 1 + \left( \frac{L_s}{w_{0,s}} \right)^{2} \frac{2}{1/2} \right] \), where \( w_{0,s} \) is the beam waist at the satellite and \( \lambda \) is the wavelength. The channel coefficient with respect to a pointing error \( \eta \) is then given by

\[
h_{ph}(\eta, L_s) = \int_{\lambda h} I_{\text{beam}}(\rho_s - \eta; L_s) \, d\rho_s, \tag{6}
\]

where \( h_{ph}(\cdot) \) denotes the fraction of the power collected by HAP’s receiver, whose area is \( \lambda h \). This integration can be approximated as [24]

\[
h_{ph} \approx A_{oh} \exp \left( -\frac{2h_{t}^2}{w_{l_{oh},eq}^2} \right), \tag{7}
\]

where \( \| \eta \| \) is the radial distance, \( A_{oh} = [\text{erf}(\eta_{h})]^2 \) is the fraction of the collected power at \( \eta_{h} = 0 \) with \( \eta_{h} = \sqrt{2 \lambda h} / \sqrt{2w_{0,s}} \), where \( \lambda h \) is HAP’s receiver radius, and \( w_{l_{oh},eq} = \left( w_{l_{s},eq}^2 w_{l_{t},eq}^2 \right)^{1/2} \) is the equivalent beam radius at distance \( L_s \). Usually, the radial distance \( \eta \) can be modeled by a Rayleigh distribution, whose PDF is given by

\[
f_{\eta_{h}}(\eta_{h}) = \frac{\eta_{h}^2}{\sigma_{s}^2} \exp \left( -\frac{\eta_{h}^2}{2\sigma_{s}^2} \right), \tag{8}
\]

where \( \sigma^2 \) is the jitter variance at HAP. From (7) and (8), the PDF of \( h_{ph} \) is derived as

\[
f_{h_{ph}}(h_{ph}) = \frac{\gamma^2}{A_{oh}^2} h_{ph}^{-2} \exp \left( \frac{-\gamma^2 h_{ph}}{2A_{oh}^2} \right), \tag{9}
\]

where \( \gamma = w_{l_{oh},eq}/2\sigma_{s} \).

### B. CHANNEL MODEL OF HAP-TO-VEHICLE LINK

The HAP-to-vehicle (either Bob or Eve) channel is characterized as \( h_{f} = h_{l} h_{t} h_{p} \), where \( h_{l} \) is the atmospheric attenuation, \( h_{t} \) is the atmospheric turbulence-induced fading, and \( h_{p} \) is the misalignment-induced fading.

#### 1) ATMOSPHERIC ATTENUATION

The atmospheric attenuation is described by the exponential Beer-Lambert’s Law as [26]

\[
h_{l} = \exp(-\xi L_{p}), \tag{10}
\]

in which \( L_{p} = H_{p} / \cos(\zeta_p) \) and \( \zeta_p \) are the distance and the zenith angle between HAP and the vehicle, respectively. \( \xi \) is the attenuation coefficient, which is determined by [27]

\[
\xi(\lambda) = \frac{3.912}{V} \left( \frac{\lambda}{550} \right)^{-q(V)}, [V] = \text{km}, [\lambda] = \text{nm}, \tag{11}
\]

where \( V \) is the atmospheric visibility, whose value depends on the weather condition (e.g. fog, rain, drizzle, clear). Values of \( V \) for typical weather conditions are presented in Table 1. Based on the values of \( V \) with respect to the considered weather condition, the value of the specific atmospheric attenuation visibility coefficient \( q(V) \) can be determined as follows

\[
q(V) = \begin{cases} 
1.6 & V > 50 \text{ km} \\
1.3 & 6 \text{ km} < V < 50 \text{ km} \\
0.585V^{1/3} & V < 6 \text{ km} 
\end{cases} \tag{12}
\]

#### 2) ATMOSPHERIC TURBULENCE-INDUCED FADING

Atmospheric turbulence caused by the variation of the refractive index of the air is one of the main challenges in FSO systems, especially for long link distances. In fact, various statistical models have been proposed to describe the atmospheric turbulence-induced fading [29]. Among them, log-normal and gamma-gamma distributions are the most commonly used ones.

\underline{a: LOG-NORMAL (LN) TURBULENCE MODEL}

For weak turbulence conditions, the turbulence-induced fading coefficient \( h_{t} \) can be accurately modeled by the log-normal distribution as

\[
f_{h_{t}}(h_{t}) = \frac{1}{h_{t}\sigma_{X}\sqrt{8\pi}} \exp \left( \frac{[\ln(h_{t}) + 2\sigma_{X}^2]^2}{8\sigma_{X}^2} \right), \tag{13}
\]

where \( \sigma_{X}^2 \) is the log-amplitude variance, which is given by \( \sigma_{X}^2 = \sigma_{t}^2/4 \) and

\[
\sigma_{t}^2 = 2.25k^{7/6}\sec^{11/6}(\zeta_{p}) \int_{H_{t}}^{H_{p}} \frac{C_{n}^2(h)(h - H_{t})^{5/6} \, dh}{H_{t}}. \tag{14}
\]

where \( \sigma_{t}^2 \) is the scintillation index, which characterizes the turbulence strength, \( k = 2\pi/\lambda \) is the wave number [25], and \( H_{t} \) is the altitude of the vehicle. \( C_{n}^2 \) is the refractive index structure parameter, which is modeled by Hufnagel-Valley (H-V) model as [25]

\[
C_{n}^2(h) = 0.00594 \left( \frac{w}{27} \right)^2 \left( 10^{-5}h \right)^{10} \exp \left( \frac{h}{1000} \right) + 2.7
\]
described by the Gamma-Gamma distribution as

\[ h \text{ at the ground level.} \]

For moderate-to-strong turbulence regimes, \( h \) can be well described by the Gamma-Gamma distribution as

\[ f_h(h) = \frac{2(\alpha \beta)^{(\alpha + \beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} \frac{\alpha + \beta - 1}{h^{\alpha + \beta}} K_{\alpha - \beta}(2\sqrt{\alpha \beta h}), \]

where \( \Gamma(\cdot) \) denotes the Gamma function, \( K_{\alpha - \beta}(\cdot) \) is the modified Bessel function of the second kind of the order \((\alpha - \beta)\), \( \alpha \) and \( \beta \) are the effective numbers of large-scale and small-scale eddies, respectively. They are expressed as [30]

\[ \alpha \equiv \exp \left( \frac{0.49\sigma_R^2}{\left(1 + 1.115\sigma_R^{12/5}\right)^{7/6}} \right) - 1, \]

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

where \( \sigma_R^2 \) is the Rytov variance for slant path and given by \( \sigma_R^2 = \sigma_t^2 \) [30].

**3) MISALIGNMENTS-INDUCED FADING**

**a: MISALIGNMENT BETWEEN HAP AND BOB**

In our considered system, Bob is a moving vehicle (e.g. a self-driving car), whose velocity is practically not always constant. Sudden changes in velocity can result in transceiver misalignments as HAP is not able to keep track Bob over a short period of time. Specifically, as illustrated in Fig. 4, from time \( t_1 \) to \( t_2 \), Bob moves with a constant velocity \( v \), which allows HAP to keep track its movement. From time \( t_2 \) to \( t_2 + \Delta t \) with \( \Delta t \) being a short time interval, Bob’s velocity slightly changes by \( \Delta v \), which causes HAP unable to perfectly point its beam to Bob’s new position. The misalignment distance due to this velocity variation (i.e. the distance from the center of the beam footprint to Bob’s instantaneous location) is determined by \( \Delta s = s_{Bob} - s_{beam} = (v\Delta t + \frac{\Delta v}{2}) - (v\Delta t) = \frac{\Delta v}{2}, \) where \( s_{Bob} \) and \( s_{beam} \) are the displacements of Bob and beam footprint in \( \Delta t \), respectively. In addition to velocity variation, mechanical errors in the tracking system or vibrations of the transceiver also cause the transceiver misalignments. As depicted in Fig. 5, the combined misalignment vector is represented by \( r_B = \frac{\Delta v}{2} + a + b \), where \( \frac{\Delta v}{2} = [0, \frac{\Delta v}{2}], a = [a, 0], \) and \( b = [0, b] \) are the misalignments caused by velocity variation, horizontal, and vertical displacement, respectively. Similar to (7), the fraction of the power collected by Bob’s receiver can be approximated by

\[ h_{pb} \approx A_{0b} \exp \left( -\frac{2r_B^2}{w_{1,h,eq}} \right), \]

where \( A_{0b} = [\text{erf}(v)]^2 \) is the fraction of the collected power at \( r_B = 0 \) with \( v = \frac{\sqrt{\sigma_a \sigma_B}}{\sqrt{\sigma_a^2 + \sigma_B^2}} \), \( \sigma_B \) is the Bob’s receiver radius, \( w_{1,h} \) is the beam radius at distance \( L_h \) from HAP to Bob,
and \( w_{L,\text{eq}} = \left( \frac{\beta^2}{4} \exp(-\nu^2) \right)^{1/2} \) is the equivalent beam radius at distance \( L_h, r_B = \|r_B\| = \sqrt{x_B^2 + y_B^2} \) is the radial distance, where \( x_{r_B} = a \) and \( y_{r_B} = b + \frac{\Delta t \Delta v}{2} \) are the magnitudes of the \( x \)- and \( y \)-component of \( r_B \), respectively. In this paper, we assume that \( a \) and \( b \) follow a zero-mean normal distribution with the same variance \( \sigma_a^2 \). The velocity variation \( \Delta v \) is also assumed to be normally distributed with zero mean and variance \( \sigma_v^2 \). As a result, \( x_{r_B} \sim N(0, \sigma_a^2) \) and \( y_{r_B} \sim N(0, \sigma_v^2) \). The PDF of \( r_B \) is then expressed as

\[
f_{r_B}(r_B) = \frac{r_B \exp \left( -\frac{r_B^2}{2\sigma_h^2} \right)}{\sigma_h^2} \exp \left[ \left( \frac{1}{2\sigma_h^2} - \frac{1}{2\sigma_B^2} \right) \frac{r_B^2}{2} \right] \times I_0 \left( \left( \frac{1}{2\sigma_h^2} - \frac{1}{2\sigma_B^2} \right) \frac{r_B^2}{2} \right), \quad r_B > 0, \tag{20}
\]

where \( \sigma_B^2 = \sigma_h^2 + \frac{(\Delta t \Delta v)^2}{4} \) and \( I_0(\cdot) \) is the modified Bessel function of the first kind. The detailed derivation for (20) is provided in Appendix.

Substituting (19) into (20), the PDF of \( h_B \) is given by

\[
f_{h_B}(h_B) = \frac{w_{L,\text{eq}}^2}{4A_{0h}^2} \frac{h_B^\mu B}{A_{0h}} \times I_0 \left[ \left( \frac{1}{2\sigma_h^2} - \frac{1}{2\sigma_B^2} \right) \frac{w_{L,\text{eq}}^2}{2} \right] \ln \left( h_B / A_{0h} \right), \quad 0 \leq h_B \leq A_{0h}, \tag{21}
\]

where \( \mu_B = \left( \frac{1}{4\sigma_h^2} + \frac{1}{4\sigma_B^2} \right) \frac{w_{L,\text{eq}}^2}{2} - 1 \).

**b: MISALIGNMENT BETWEEN HAP AND EVE**

We consider that Eve is an adversary’s car, which follows Bob (supposed to be at the center of the aligned beam footprint) at a distance \( d_E \). To evaluate the worst-case scenario (i.e. the maximum information Eve can possibly eavesdrop), it is assumed that Eve maintains a constant velocity so that her fraction of collected power is only affected by misalignment due to the vibrations of the transceiver. Displayed in Fig. 6, \( d_E \) is the radial vector from the center of the aligned beam footprint (i.e. \( O \)) and \( r = a + b \) is the radial vector from \( O \) to the center of the misaligned beam footprint (i.e. \( O' \)). Then, the radial vector from Eve to \( O' \) is given by \( r_E = d_E + r \) with the magnitudes of \( x \)- and \( y \)-components are calculated as

\[
x_{r_E} = d_E \cos(\varphi) + x_r = d_E \cos(\varphi) + x_a + x_b = d_E \cos(\varphi) + a,
\]

\[
y_{r_E} = d_E \sin(\varphi) + y_r = d_E \sin(\varphi) + y_a + y_b = d_E \sin(\varphi) + b,
\]

where \( d_E = \|d_E\| \) and \( \varphi \) is the angle form by \( d_E \) and \( Ox \). Similar to the case of Bob, Eve’s fraction of collected power is approximated as

\[
h_{PE} \approx A_{0E} \exp \left[ -\frac{2r_E^2}{w_{L,\text{eq}}^2} \right], \tag{24}
\]

where \( A_{0E} = [\text{erf}(w_E/2)]^2 \) is the fraction of the collected power at \( r_E = 0 \) with \( v_E = \frac{\sqrt{v_a \sigma_a^2}}{\sqrt{w_{L,E}^2}} \), \( a_E \) is the Eve’s receiver radius, and \( w_{L,\text{eq}} = \left( \frac{w_{L,E}^2}{4} \exp(-\nu^2) \right)^{1/2} \) is the equivalent beam radius at distance \( L_h, r_E = \|r_E\| = \sqrt{x_E^2 + y_E^2} \) is the radial distance. As mentioned previously, since \( a \sim N(0, \sigma_a^2) \) and \( b \sim N(0, \sigma_v^2) \), we get \( x_{r_E} \sim N(d_E \cos(\varphi), \sigma_a^2) \) and \( y_{r_E} \sim N(d_E \sin(\varphi), \sigma_v^2) \). As a result, \( r_E \) follows a Rician distribution as [31]

\[
f_{r_E}(r_E) = \frac{r_E}{\sigma_h^2} \exp \left[ -\frac{r_E^2 + d_E^2}{2\sigma_h^2} \right] J_0 \left( \frac{r_E d_E}{\sigma_h^2} \right), \tag{25}
\]

where \( J_0(\cdot) \) is the Bessel function of the first kind. From (24) and (25), the PDF of \( h_{PE} \) is expressed by

\[
f_{h_{PE}}(h_{PE}) = \frac{w_{L,\text{eq}}^2}{4\sigma_h^2} \frac{h_{PE}^\mu E}{A_{0E}} \exp \left[ \frac{-d_E^2}{2\sigma_h^2} \right] \left[ \frac{h_{PE}}{A_{0E}} \right]^\mu E J_0 \left( \frac{d_E h_{PE}}{\sigma_h^2} \right), \quad 0 \leq h_{PE} \leq A_{0E}, \tag{26}
\]

where \( \mu_E = \frac{w_{L,\text{eq}}^2}{4\sigma_h^2} - 1 \).  

**4) STATISTICAL CHANNEL MODELS**

**a: BOB’S STATISTICAL CHANNEL MODEL**

The PDF of Bob’s channel coefficient \( h_B = h_1 h_2 h_{PE} \) can be determined as

\[
f_{h_B}(h_B) = \int f_{h_B|h_1}(h_B|h_1) f_{h_1}(h_1) \, dh_1, \tag{27}
\]

where \( f_{h_B|h_1}(h_B|h_1) \) is the conditional PDF of \( h_B \) given the turbulence state \( h_1 \) and given from (21) as

\[
f_{h_B|h_1}(h_B|h_1) = \frac{1}{h_1 h_1} f_{h_B}^\mu B \left( \frac{h_B}{h_1 h_1} \right) = \frac{w_{L,\text{eq}}^2}{4\sigma_h^2} \frac{h_B^\mu B}{A_{0h}^2} \exp \left[ \frac{-w_{L,\text{eq}}^2}{2\sigma_h^2} \right] \left[ \frac{h_B}{A_{0h} h_1} \right]^\mu B \times I_0 \left( \left( \frac{1}{2\sigma_h^2} - \frac{1}{2\sigma_B^2} \right) \frac{w_{L,\text{eq}}^2}{2} \right) \ln \left( h_B / A_{0h} h_1 \right), \quad 0 \leq h_B \leq A_{0h} h_1. \tag{28}
\]

Substituting (28) into (27), we have

\[
f_{h_B}(h_B) = \frac{w_{L,\text{eq}}^2}{4\sigma_h^2} \frac{h_B^\mu B}{A_{0h}^2} \exp \left[ \frac{-w_{L,\text{eq}}^2}{2\sigma_h^2} \right] \left[ \frac{h_B}{A_{0h} h_1} \right]^\mu B \times I_0 \left( \left( \frac{1}{2\sigma_h^2} - \frac{1}{2\sigma_B^2} \right) \frac{w_{L,\text{eq}}^2}{2} \right) \ln \left( h_B / A_{0h} h_1 \right), \quad 0 \leq h_B \leq A_{0h} h_1. \tag{28}
\]
Assume that bits ‘0’ and ‘1’ are equally likely to be transmitted. These probabilities are determined through the joint probabilities between Alice and Bob as

\[ f_{h_E}(h_E) = \int_{h_{h_E}} f_{h_E|h(h_E|t)} f_{h(h)} dh, \]  

where \( f_{h_E|h(h_E|t)} \) is derived from (26) as

\[ f_{h_E|h(h_E|t)} = \frac{w_{h_{h_E}}^2}{4\sigma^2_{h}(h_AE_{0})}\int \left[ \exp \left( \frac{-d_E^2}{2\sigma^2_{h}} \right) \right] h_{1}^{\mu_{E}} \times h_{-\mu_{E}-1} \int_{h_{h}} d_{E} \left[ \frac{w_{h_{h_E}}^2}{2\sigma^2_{h}} \right] \ln \left( \frac{h_{h}}{h_{h_AE_{0}}(h)} \right), \]

\[ 0 \leq h_{E} \leq A_{h_E}h_{h}. \]  

Plugging (31) into (30), we have

\[ f_{h_E}(h_E) = \frac{w_{h_{h_E}}^2}{4\sigma^2_{h}(h_AE_{0})}\int \left[ \exp \left( \frac{-d_E^2}{2\sigma^2_{h}} \right) \right] h_{1}^{\mu_{E}} \times h_{-\mu_{E}-1} \int_{h_{h}} d_{E} \left[ \frac{w_{h_{h_E}}^2}{2\sigma^2_{h}} \right] \ln \left( \frac{h_{h}}{h_{h_AE_{0}}}(h) \right). \]  

IV. SECRECY PERFORMANCE ANALYSIS
A. QUANTUM BIT ERROR RATE

Analogous to the QBER defined in the conventional BB84 protocol, the QBER of the proposed system can be given as

\[ \text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}}, \]  

where \( P_{\text{sift}} \) is the probability that Bob is able to decode bits using the DT detection while \( P_{\text{error}} \) is the probability that Bob mistakenly detects the transmitted bits. These probabilities are determined through the joint probabilities between Alice and Bob as

\[ P_{\text{sift}} = P_{A,B}(0, 0) + P_{A,B}(0, 1) + P_{A,B}(1, 0) + P_{A,B}(1, 1), \]  

\[ P_{\text{error}} = P_{A,B}(0, 0) + P_{A,B}(1, 0), \]  

where \( P_{A,B}(x,y) \) with \( x, y \in \{0, 1\} \) is the probability that Alice’s set bit ‘x’ coincides with Bob’s decoded bit ‘y’. Assume that bits ‘0’ and ‘1’ are equally likely to be transmitted (i.e. the probabilities that Alice transmits bits ‘0’ and ‘1’ are the same \( P_{A}(x = 0) = P_{A}(x = 1) = \frac{1}{2} \)), the joint probabilities in (34) and (35) averaged over the atmospheric channels are calculated as

\[ P_{A,B}(x, 0) = \frac{1}{2} \int_{0}^{\infty} Q \left( \frac{i_{x} - d_{0}}{\sigma_{N}} \right) f_{h_{all}}(h_{all}) dh_{all}, \]  

\[ P_{A,B}(x, 1) = \frac{1}{2} \int_{0}^{\infty} Q \left( \frac{d_{1} - i_{x}}{\sigma_{N}} \right) f_{h_{all}}(h_{all}) dh_{all}, \]  

where \( x \in \{0, 1\}, i_{0} = -i_{1} = -\frac{1}{4} \gamma_{P_{A}}G_{A} \delta_{h_{all}} = -\frac{1}{4} \gamma_{P_{A}}G_{A} \delta_{h_{B}}B, \) and \( Q(\cdot) \) is the Q-function. \( f_{h_{all}} \) is the PDF of \( h_{all} = h_{p_{h}}h_{B} \) and can be calculated as

\[ f_{h_{all}}(h_{all}) = \frac{y^{2}}{A_{h_{all}}}(h_{all}) \int_{0}^{\infty} h_{B}^{2} f_{h}(h_{B}) dh_{B}. \]  

DT are determined by \( d_{0} = \mathbb{E}[i_{0}] - \xi \sigma_{N} \) and \( d_{1} = \mathbb{E}[i_{1}] + \xi \sigma_{N} \), with \( \xi \) being the DT scale coefficient and \( \mathbb{E}[\cdot] \) being the expectation operator, are the two thresholds at Bob’s receiver. Additionally,

\[ \mathbb{E}[i_{0}] = -\mathbb{E}[i_{1}] = -\frac{1}{4} \gamma_{P_{A}}G_{A} \mathbb{E}[h_{p_{h}}] \mathbb{E}[h_{B}] \]  

\[ = -\frac{1}{4} \gamma_{P_{A}}G_{A} \varphi_{2}^{2} A_{h_{all}}^{0} h_{0} \int_{0}^{\infty} h_{p_{h}} f_{h_{p_{h}}}(h_{p_{h}}) dh_{p_{h}}. \]  

B. ERGODIC SECRET-KEY RATE

To evaluate the physical security of the proposed system, we investigate the ergodic secret-key rate, which is defined as the maximum transmission rate between Alice and Bob at which Alice is not able to decode any information from her received signal. Mathematically, in the case of AWGN channel, it is given by

\[ S = I(A; B) - I(A; E), \]  

where \( I(A; B) \) and \( I(A; E) \) are the mutual information between Alice-Bob and Alice-Eve, respectively. Then, the system is considered as secure if \( S \) is positive [32]. As a result of the DT detection rule defined in (1), the transmission between Alice and Bob can be modeled as a binary erasure channel (BEC), and assuming that bits ‘0’ and ‘1’ are equally likely, \( I(A; B) \) can be given

\[ I(A; B) = p \log_{2}(p) + (1 - p - q) \log_{2}(1 - p - q) \]  

\[ - \frac{p}{2} + \frac{(1 - p - q)}{2} \log_{2} \left[ \frac{p}{2} + \frac{(1 - p - q)}{2} \right] \]  

\[ - \frac{(1 - p - q)}{2} + \frac{p}{2} \log_{2} \left[ \frac{(1 - p - q)}{2} + \frac{p}{2} \right]. \]  

\[ (41) \]
where with $p$ and $q$ being the no-error and erasure probabilities, respectively, Eve, on the other hand, tries to maximize the information obtained from the eavesdropped signal by using the optimal detection threshold $d_E = 0$. The mutual information $I(A; E)$ is then

$$I(A; E) = 1 + P_e \log_2(P_e) + (1 - P_e) \log_2(1 - P_e),$$

where $P_e = P_{A,E}(0, 1) + P_{A,E}(1, 0)$ is Eve’s error probability with $P_{A,E}(0, 1)$ and $P_{A,E}(1, 0)$ being the joint probabilities that Alice’s transmitted bits are detected wrongly by Eve. Averaged over the atmospheric channels, $P_{A,E}(0, 1)$ and $P_{A,E}(1, 0)$ can be expressed as

$$P_{A,E}(0, 1) = P_{A,E}(1, 0) = \frac{1}{2} \int_{0}^{\infty} Q\left(\frac{1}{\sigma_N} (h_E^A G_A \delta h_E^E)\right) f_{h^E}^0(h_{all}^E) dh_{all}^E,$$

where $f_{h^E}^0(h_{all}^E)$ is the PDF of $h_{all}^E = h_{0h} h_E$ and calculated as

$$f_{h^E}^0(h_{all}^E) = \int f_{h^E}^0(h_E) f_{h_E}^0(h_E) dh_E = \frac{\gamma^2}{A_h^2} \left(\frac{h_{all}^E}{A_h}\right)^{-2} - 1 \int_{h_{all}^E}^{\infty} h_{all}^E - \gamma f_{h_E}^0(h_E) dh_E.$$

V. NUMERICAL RESULTS

A. MONTE-CARLO SIMULATION

M-C simulations are implemented to verify the accuracy of the analytical derivations presented in the previous section. In this section, the process of M-C simulation for the proposed system is described in detail.

Figure 7 presents the model of M-C simulation for the proposed system. First, at LEO satellite, a bit sequence $d[n]$ is generated by the block Random bit generator. It is then modulated by using SIM/BPSK modulator. Next, the modulated signal is transmitted to HAP after being multiplied by the fraction of the power collected by HAP’s receiver $h_{0h}$, which is calculated from the generated pointing error vector $r_h$. At the HAP, the signal is multiplied by the optical amplifier gain $G_A$. The amplified signal is then forward to the vehicle. On the HAP-to-vehicle link, the amplified signal is multiplied by the atmospheric attenuation depending on the weather condition setting, the turbulence-induced fading coefficient, and the fraction of the power collected by the vehicle’s receiver $h_{vh}$, respectively.

At the vehicle’s receiver, the background noise, ASE noise, shot noise, and thermal noise generated by the block Generating Gaussian random variables are added into the received signal. Then, the signal is detected to retrieve the bit sequence by using the DT detection rule defined in (1) in the case of Bob and by using the optimal threshold 0 in the case of Eve. The recovered bit sequence $d[n]$ is compared to the original bit sequence $d[n]$ from LEO satellite to calculate $P_{sift}$, $P_{error}$, and QBER in the case of Bob and $P_e$ in the case of Eve.

B. DISCUSSIONS

In this section, representative numerical results are presented to illustrate the secrecy performances of the proposed system. Unless otherwise noted, the system parameters are given in Table 2.

| Name                    | Symbol | Value |
|-------------------------|--------|-------|
| **LEO Satellite (Alice)** |        |       |
| Wavelength              | $\lambda$ | 1550 nm |
| Bit rate                | $R_b$  | 1 Gbps |
| Altitude                | $H_s$  | 300 km |
| Beam waist radius       | $w_{0,h}$ | 5 cm   |
| **Alice-HAP Channel**   |        |       |
| Sun’s spectral irradiance from above the atmosphere | $\Omega_h$ | 0.1 W/cm$^2$ $\mu$m |
| **HAP**                 |        |       |
| Altitude                | $H_p$  | 20 km  |
| Alice-HAP zenith angle  | $\zeta_s$ | 0       |
| Aperture radius         | $a_h$  | 20 cm  |
| Beam waist radius       | $w_{0,h}$ | 0.2 mm |
| ASE parameter           | $n_{sp}$ | 4       |
| Optical bandwidth       | $B_0$  | 250 GHz |
| **HAP-Bob/Eve Channel** |        |       |
| Sun’s spectral irradiance from above the Earth | $\Omega_v$ | 0.0125 W/cm$^2$ $\mu$m |
| Wind speed              | $w$    | 21 m/s |
| Visibility              | $V$    | 30 km  |
| **Bob/Eve**             |        |       |
| Altitude                | $H_v$  | 1.6 m  |
| Aperture radius         | $a_v$  | 5 cm   |
| Optical bandwidth       | $B_v$  | 250 GHz |
| Responsivity            | $R$    | 0.9 A/W |
| Effective noise bandwidth | $\Delta f$ | 0.5 GHz |
| Temperature             | $T$    | 298 K  |
| Load resistor           | $R_L$  | 1 k$\Omega$ |
| Amplifier noise figure  | $F_a$  | 2      |

Firstly, Fig. 8 depicts Eve’s error probability $P_e$ versus HAP’s optical amplifier gain $G_A$ and intensity modulation depth $\delta$ under weak turbulence condition with $d_E = 1$ m and $P = 680$ mW. On one hand, it is observed that when $G_A \leq 25$ dB, $P_e$ is always greater than 0.1 regardless of the value of $\delta$. On the other hand, as $G_A$ increases beyond 25 dB, Alice should choose lower values for $\delta$ to guarantee a sufficiently high $P_e$ (e.g. higher than 0.1). For example, when $G_A = 30$ dB, $\delta \leq 0.4$ should be chosen. However, the choices of $G_A$ and $\delta$ also have an impact on Bob’s error probability (i.e. $P_{error}$), which is illustrated in Fig. 9. As seen from the previous figure that given a value of $G_A$, the intensity modulation should be chosen as small as possible to maximize Eve’s error probability. Small values of $\delta$ nonetheless result in high Bob’s error probabilities. Hence, one should set $G_A$ and $\delta$ appropriately to ensure a good trade-off between Bob’s and
Eve’s error probabilities. For instance, setting $G_A = 30$ dB and $\delta = 0.4$ guarantees that $P_e \approx 0.1$ and Bob’s error probability is $10^{-5}$.

The influences of $\delta$ on Eve’s error performance for different values of Eve-Bob distance and turbulence conditions are shown in Figs. 10 and 11, respectively. In general, $P_e$
decreases in accordance with a decrease in Eve-Bob distance as Eve is closer to the center of the beam footprint. However, $P_e$ can still be set higher than 0.1 by letting $\delta \leq 0.4$ even when the Eve-Bob distance is as small as 1 m. When $\delta \leq 0.4$, it is seen that $P_e \geq 0.1$ can always be achieved under a wide range of turbulence regimes, from weak ($\sigma^2_v = 0.06$), moderate ($\sigma^2_v = 0.55$) to strong conditions ($\sigma^2_v = 1.05$). From these observations, $\delta = 0.4$ is thus chosen for the subsequent results.

In Fig. 12, Bob’s error probability as a function of the DT scale coefficient $\varsigma$ is illustrated under the weak turbulence for different standard deviations $\sigma_v$ of the velocity variation. As the severity of velocity variation-induced pointing error is proportional to $\sigma_v$, $P_{\text{error}}$ worsens when $\sigma_v$ increases. Consider the worst-case scenario where $\sigma_v = 5$ m/s, Figs. 13(a) and (b) depict Bob’s QBER and $P_{\text{sift}}$ versus the DT scale coefficient $\varsigma$ under weak and strong turbulence conditions, respectively. To ensure that Bob receives sufficient information (e.g. to achieve a sifted-key rate at Mbps with typical transmission rate at Gbps of standard FSO systems), the sift probability needs to be at least $10^{-2}$. At the same time, QBER needs to be less than $10^{-3}$ so that errors can be efficiently corrected at Mbps sifted-key rates by error-correction codes. To satisfy these two requirements, $1.6 \leq \varsigma \leq 2.8$ and $1.8 \leq \varsigma \leq 3.8$ should be selected for weak and strong turbulence condition, respectively.

Finally, Figs. 14 and 15 show the ergodic secret-key rate $S$ versus DT scale coefficient $\varsigma$ and Eve-Bob distance for weak and strong turbulence conditions, respectively. We are interested in the minimum Eve-Bob distances where the proposed system is considered as secure (i.e. $S > 0$). With the smallest possible values of $\varsigma$ to guarantee sufficient Bob’s sifted-key rates (i.e. $\varsigma = 1.6$ for weak and $\varsigma = 1.8$ for strong turbulence), it is seen that the minimum Eve-Bob distances are 38 m and 36.25 m for weak and strong turbulence conditions. In other words, a minimum distance of 38 m between Bob and Eve should be maintained to ensure the system is secure over a wide range of turbulence regimes.
VI. CONCLUSION
In this paper, the secrecy performances of HAP-based relay-assisted satellite FSO/QKD systems for secure vehicular networks were analyzed. The effects of transceiver misalignment, Bob’s velocity variation, receiver noises, and atmospheric turbulence conditions were considered for thorough channel modeling. Extensive numerical results were also presented to determine appropriate parameters in terms of intensity modulation depth, HAP’s optical amplifier gain, DT scale coefficient, and minimum Eve-Bob distances for secure communication between Alice and Bob.

APPENDIX
DERIVATION OF THE PDF IN (20)
Since \( x_{\text{rf}} \sim \mathcal{N}(0, \sigma_{\text{h}}^2) \) and \( y_{\text{rb}} \sim \mathcal{N}(0, \bar{\sigma}^2_{\text{h}}) \), we have \( x_{\text{rf}}^2 \sim \text{Gamma} \left( \frac{1}{2}, 2\sigma_{\text{h}}^2 \right) \) and \( y_{\text{rb}}^2 \sim \text{Gamma} \left( \frac{1}{2}, 2\bar{\sigma}^2_{\text{h}} \right) \). For mathematical connivence, denote \( C = x_{\text{rf}}^2 \) and \( D = y_{\text{rb}}^2 \) and let \( f_{C,D}(c,d) \) be the joint PDF of \( C \) and \( D \). Also, let \( C = V \) and \( D = U^2 - V \) (i.e. it is equivalent to \( U = \sqrt{C + D}, V = C \)) be a one-to-one transformation from \((C, D)\) to \((U, V)\). Then, the joint PDF of \( U \) and \( V \) is obtained as
\[
f_{U,V}(u, v) = |J| f_{C,D}(c(u,v), d(u,v)),
\]
where \( J \) is the Jacobian of the transformation, which is defined as
\[
J = \begin{vmatrix}
\frac{\partial c}{\partial u} & \frac{\partial c}{\partial v} \\
\frac{\partial d}{\partial u} & \frac{\partial d}{\partial v}
\end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 2u & -1 \end{vmatrix} = -2u.
\]
Since \( C \) and \( D \) are independent, (45) can be rewritten as
\[
f_{U,V}(u, v) = |J| f_{C,D}(c(u,v), d(u,v)) = 2af_{C}(c(u,v))f_{D}(d(u,v)),
\]
where \( f_{C}(c(u,v)) \) and \( f_{D}(d(u,v)) \) are expressed as
\[
f_{C}(c(u,v)) = v^{-1/2} \exp^{-v/2\sigma_{\text{h}}^2},
\]
\[
f_{D}(d(u,v)) = (2\sigma_{\text{h}}^2)^{1/2} \Gamma(1/2) \exp^{-(u^2-v)^2/2\sigma_{\text{h}}^2}.
\]
Substituting (48), (49) into (47), we have
\[
f_{U,V}(u, v) = \frac{2av^{-1/2}(u^2 - v)^{-1/2} \exp^{-v/2\sigma_{\text{h}}^2}}{(2\sigma_{\text{h}}^2)^{1/2} (2\bar{\sigma}_{\text{h}}^2)^{1/2} \left( \Gamma \left( \frac{1}{2} \right) \right)^2}. \tag{50}
\]
Then, the PDF of \( U \) can be derived from the joint PDF of \( U \) and \( V \) as
\[
f_{U}(u) = \int_{0}^{\infty} f_{U,V}(u, v) dv = \frac{2av^{-1/2}(u^2 - v)^{-1/2} \exp^{-v/2\sigma_{\text{h}}^2}}{(2\sigma_{\text{h}}^2)^{1/2} (2\bar{\sigma}_{\text{h}}^2)^{1/2} \left( \Gamma \left( \frac{1}{2} \right) \right)^2}. \tag{51}
\]
Using [33, (3.383.2)], the PDF of \( U \) (in other words, the PDF of \( r_{\text{rb}} \)) is expressed as
\[
f_{U}(u) = \frac{u\exp \left( \frac{-u^2}{2\sigma_{\text{h}}^2} \right) \exp \left[ \frac{-(1/2) + 1/2}{2\sigma_{\text{h}}^2} u^2 \right]}{(2\sigma_{\text{h}}^2)^{1/2} (2\bar{\sigma}_{\text{h}}^2)^{1/2} \left( \Gamma \left( \frac{1}{2} \right) \right)^2}, \quad u > 0. \tag{52}
\]
REFERENCES
[1] V. Padmanabhi, B. V. Vardhan, and A. V. N. Krishna, “Quantum cryptography and quantum key distribution protocols: A survey,” in Proc. IEEE Int. Conf. Adv. Comput. Sci. (ICACS), Feb. 2016, pp. 556–562.
[2] D. Jin, P. Verma, and S. Kartalopoulos, “Key distribution using dual quantum channels,” in Proc. 4th Int. Conf. Infor. Assurance Secur., Naples, Italy, Sep. 2008, pp. 327–332.
[3] A. Boaron, G. Bosso, D. Rusca, C. Valluzi, C. Autembert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, “Secure quantum key distribution over 421 km of optical fiber,” Phys. Rev. Lett., vol. 121, no. 19, Nov. 2018, Art. no. 190502.
[4] T. Gehring, V. Handchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, “Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks,” Nature Commun., vol. 6, no. 1, Oct. 2015, Art. no. 8795.
[5] B. Qi, “Simultaneous classical communication and quantum key distribution using continuous variables,” Phys. Rev. A, Gen. Phys., vol. 94, no. 4, Oct. 2016, Art. no. 042340.
[6] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, “Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states,” Phys. Rev. A, Gen. Phys., vol. 101, no. 1, Jan. 2020, Art. no. 012343.
[7] R. Kumar, A. Wonfor, R. Penty, T. Spiller, and I. White, “Experimental demonstration of single-shot quantum and classical signal transmission on single wavelength optical pulse,” Sci. Rep., vol. 9, no. 1, Aug. 2019, Art. no. 11190.
[8] T. Ikuta and K. Inoue, “Intensity modulation and direct detection quantum key distribution based on quantum noise,” New J. Phys., vol. 18, no. 1, Jan. 2016, Art. no. 013018.
[9] R. Hughes, J. Nordholt, D. Derkacs, and C. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” New J. Phys., vol. 4, p. 43, Jul. 2002.
[10] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, “Atmospheric continuous-variable quantum communication,” New J. Phys., vol. 16, no. 11, Nov. 2014, Art. no. 113018.
[11] S.-K. Liao et al., “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication,” Nature Photon., vol. 11, no. 8, pp. 509–513, Jul. 2017.
[12] N. Triph, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, “Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver,” IEEE Access, vol. 6, pp. 4159–4175, 2018.
[13] C. Bonato, A. Tomasio, V. Da Deppo, G. Naletto, and P. Villoresi, “Feasibility of satellite quantum key distribution,” New J. Phys., vol. 11, no. 4, Apr. 2009, Art. no. 045017.
[14] J. Khan, B. Heim, A. Neuzner, and C. Marquardt, “Satellite-based QKD,” Opt. Photon. News, vol. 29, pp. 26–33, Feb. 2018.
[15] T. Scheidl et al., “Space-to-ground quantum key distribution,” in Proc. Int. Conf. Space Opt., Chania, Greece, Aug. 2019, Art. no. 111801W.
[16] M. Polnik, L. Mazzarella, M. Di Carlo, D. K. Oi, A. Riccardi, and A. Arulselvan, “Scheduling of space to ground quantum key distribution,” EPJ Quantum Technol., vol. 7, no. 1, p. 7, Jan. 2020.
[17] L. Xin, “China tests portable quantum ground station,” Phys. World, vol. 33, no. 2, p. 8, Feb. 2020.
M. Q. Vu et al.: Design and Performance of Relay-Assisted Satellite Free-Space Optical QKD Systems

[18] H.-J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998.

[19] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.

[20] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, “Long-distance quantum communication with entangled photons using satellites,” *IEEE J. Sel. Topics Quantum Electron.*, vol. 9, no. 6, pp. 1541–1551, Nov. 2003.

[21] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, “Quantum key distribution over double-layer quantum satellite networks,” *IEEE Access*, vol. 8, pp. 16067–16098, 2020.

[22] M. Q. Vu, N. T. Dang, and A. T. Pham, “HAP-aided relaying satellite FSO/QKD systems for secure vehicular networks,” in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–6, doi: 10.1109/VTCSpring.2019.8746381.

[23] C. H. Bennett and G. Brassard, “Quantum cryptography: Public-key distribution and coin tossing,” in *Proc. IEEE Conf. Comput., Syst. Signal Process.*, Bangalore, India, Dec. 1984, pp. 175–179.

[24] A. A. Farid and S. Hranilovic, “Outage capacity optimization for free-space optical links with pointing errors,” *J. Lightw. Technol.*, vol. 25, no. 7, pp. 1702–1710, Jul. 2007.

[25] H. Hemmati, *Near-Earth Laser Communication*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2009.

[26] M. Sharma, D. Chadha, and V. Chandra, “High-altitude platform for free-space optical communication: Performance evaluation and reliability analysis,” *IEEE/OSA J. Opt. Commun. Netw.*, vol. 8, no. 8, pp. 600–609, Aug. 2016.

[27] J. L. Green, B. W. Welch, and R. M. Manning, *Optical Communication Link Atmospheric Attenuation Model*. Washington, DC, USA: National Aeronautics and Space Administration, Feb. 2019. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190001012.pdf

[28] Z. Ghassenmolyo, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling With MATLAB*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2018.

[29] M. A. Khalighi and M. Uysal, “Survey on free space optical communication: A communication theory perspective,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2231–2258, 4th Quart., 2014.

[30] L. C. Andrews, *Laser Beam Propagation Through Random Media*, 2nd ed. Bellingham, WA, USA: SPIE, 2005.

[31] M. K. Simon and M. S. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. New York, NY, USA: Wiley, 2004.

[32] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[34] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.

[35] J. Lightw. Technol., vol. 25, no. 7, pp. 1702–1710, Jul. 2007.

[36] L. C. Andrews, *Laser Beam Propagation Through Random Media*, 2nd ed. Bellingham, WA, USA: SPIE, 2005.

[37] M. K. Simon and M. S. Alouini, *Digital Communication Over Fading Channels*, 2nd ed. New York, NY, USA: Wiley, 2004.

[38] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[40] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.

[41] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.

[42] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.

[43] M. Safari and M. Uysal, “Relay-assisted quantum-key distribution over long atmospheric channels,” *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct. 2009.