Design of Satellite-Based FSO/QKD Systems Using GEO/LEOs for Multiple Wireless Users

Minh Q. Vu, *Student Member, IEEE*, Hoang D. Le, *Member, IEEE*, Thanh V. Pham, *Member, IEEE*, and Anh T. Pham, *Senior Member, IEEE*

***Abstract*—This article proposes the design of a global-scale free-space optics/quantum key distribution (FSO/QKD) network based on a geosynchronous (GEO) satellite as the secret key source and low-Earth orbit (LEO) satellites as relay nodes for multiple legitimate users on the ground. The continuous variable QKD (CV-QKD) protocol with dual-threshold/direct detection (DT/DD) receivers is employed. The system performance is analyzed by considering the spreading loss, atmospheric attenuation, and turbulence. Based on the design criteria for the proposed system, we investigate the feasibility of a case study for the Japan QKD network considering the unauthorized receiver attack (URA) and beam-splitting attack (BSA). In addition, we analyze the secret-key rate performance of the proposed system and perform Monte Carlo simulations to verify analytical results.**

***Index Terms*—Free-space optics, quantum key distribution, entanglement-based scheme, continuous-variable QKD, dual-threshold/direct detection, GEO satellite, LEO satellite, multiple users, atmospheric turbulence, Gaussian beam.**

I. Introduction

THE security of today's communication infrastructure relies on secret key distribution systems based on public-key cryptography. Meanwhile, quantum technology has been advancing rapidly, with significant progress in scaling up quantum processors by Google, IBM, Honeywell, etc. It poses a growing risk to classical public cryptosystems, which could be compromised by quantum algorithms (e.g., Shor's algorithm). Quantum key distribution (QKD), a novel mechanism for secret key agreement between legitimate parties, claims to offer potential mitigation from the public cryptosystem to prepare for threats exposed by quantum computing [2]. Unlike conventional key distribution systems, the security of QKD rests on the laws of quantum mechanics rather than the assumption that a mathematical problem is challenging. By encoding secret information on photons to securely transfer messages of Wiesner in 1983 [3], the first QKD protocol was proposed in 1984 by Bennett and Brassard [4]. Over the past few years, QKD has gained global interest as a unique cybersecurity solution. Many commercial offerings are now available from worldwide vendors, such as Quintessence Labs, Qasky Quantum Science Technology, QuatumnCTek, ID Quantique, SeQureNet [5]. The unique nature of QKD has shown promise for the high-security environment, such as banking, government, and military applications.

While QKD has achieved remarkable progress in the optical fibers [6], [7], [8], and terrestrial free-space optical (FSO) systems [9], [10], [11], [12], it is the FSO/QKD system using satellites that can enable the possibility the global-scale quantum networks for both fixed and wireless users, such as unmanned aerial vehicles (UAV), autonomous vehicles [13]. In 2016, China reached a new milestone when they successfully launched Micius-the world's first quantum communication satellite to orbit [14]. The FSO/QKD payload aboard the satellite generated the cryptographic key pair used by the stations in Vienna and Beijing for the first intercontinental video conference using quantum encryption [15]. The achievement brought us closer to the realization of the global-scale FSO/QKD network. Over the past few years, several experiments on FSO/QKD systems using satellites have been successfully demonstrated [16], [17], [18], [19].

Satellite-based QKD systems can be classified into two different schemes: prepare-and-measure (PM) and entanglement-based (EB) [15] to distribute secret keys between two ground stations (Alice and Bob). In the PM scheme, the satellite establishes two different keys between itself (Charlie) and Alice and Bob, respectively. The satellite, which acts as a single trusted node, combines these two secret keys with a mathematical operation and broadcasts it [20]. In the EB scheme, the trusted source requirement can be relaxed because Alice and Bob, without the involvement of the satellite, can agree on the final secret keys after independently measuring received quantum states [21]. This article focuses on the EB scheme, which is more suitable for implementing a global-scale QKD network.

FSO/QKD systems using low-Earth orbit (LEO) satellites and EB scheme have been proposed in [18], [21], [22]. The LEO satellite benefits from the low channel loss; however, its coverage is limited [18]. The coverage can be extended by multiple LEOs organized into a constellation. Nevertheless, the key relaying/routing in the network of satellites would bring new security concerns. While a geosynchronous satellite (GEO)

Manuscript received 4 July 2023; accepted 9 July 2023. Date of publication 12 July 2023; date of current version 25 July 2023. This work was supported by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant 21K11870. An earlier version of this paper was presented at the 2022 International Conference on Emerging Technologies for Communications (ICETC), Waseda University, Tokyo, Japan, Nov. 2022 [DOI: 10.34385/proc.72.O4-2]. *(Corresponding author: Anh T. Pham.)*

Minh Q. Vu, Hoang D. Le, and Anh T. Pham are with the School of Computer Science and Engineering, The University of Aizu, Aizuwakamatsu 965-8580, Japan (e-mail: quangminhvu95@gmail.com; hoangle@u-aizu.ac.jp; pham@u-aizu.ac.jp).

Thanh V. Pham is with the Department of Mathematical and Systems Engineering, Shizuoka University, Shizuoka 432-8011, Japan (e-mail: pham.van.thanh@shizuoka.ac.jp).

Digital Object Identifier 10.1109/JPHOT.2023.3294723

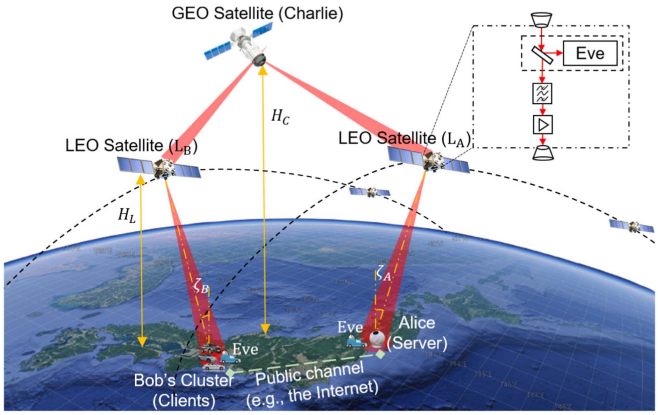


Fig. 1. Proposal of satellite-based FSO/QKD system using GEO and LEO satellites.

satellite with an altitude of 35,786 km can solve the coverage problem, the system suffers from a high path loss and limited key rates. Therefore, combining GEO and LEO satellites becomes a promising solution for the global-scale QKD network.

This article presents a novel satellite-based FSO/QKD system that uses LEO and GEO satellites. We focus on designing a system that can support multiple wireless users, which opens the potential to establish a global-scale QKD network. Based on the design criteria for the proposed system, we investigate the feasibility of a case study for the Japan QKD network using the existing GEO satellite and LEO satellite constellation to provide QKD service for legitimate users in Japan. Furthermore, the secret key performance of the proposed system is studied based on the design criteria of transmitters and receivers considering the unauthorized receiver attack (URA) and beam-splitting attack (BSA). In particular, we aim to design the transmitted signal to prevent URA and propose a simple scheme that allows legitimate users to detect BSA. For all analyses, Monte Carlo simulations are also performed to verify analytical results.

The article is organized as follows. In Section II, we describe the proposed satellite-based FSO/QKD system model using both LEOs and GEO for multiple wireless users, the BBM92 protocol, signal model, and the multiple access scheme. The channel model and system performance analysis are presented in Section III and Section IV, respectively. Section V focuses on the design and analysis of a case study of Japan; in particular, we present the criteria for system design under the URA and BSA and analyze the secret key performance. Finally, the article is concluded in Section VI.

II. System Descriptions

A. System Model

Fig. 1 presents the proposed FSO/QKD system, in which a GEO satellite (Charlie) distributes secret keys to a legitimate server, i.e., Alice and multiple users Bob_i, $i \in \{1, 2 \ldots N\}$, via FSO channels with the help of two LEO satellites for amplifying the signal. LEO satellites relaying Charlie's signals to Alice and Bobs are denoted as L_A and L_B, respectively. We assume that Alice is a server that performs post-processing procedures over the public channel with each user Bob_i to create secret keys between Alice and each user Bob_i. For the sake of simplicity, we use notations "A", "B_i", and "C" for Alice, Bob_i, and Charlie. In addition, H_C, H_L, and H_U denote the altitude of Charlie, LEO satellites, and user $U \in \{A,\ B_i\}$, respectively. The zenith angle is denoted as ζ_U. The elevation angle is given by $(\pi/2 - \zeta_U)$. To inhibit signal blockage by skyscrapers and minimize the effect of atmospheric attenuation and turbulence, the minimum acceptable elevation angle is set to 30° [23].

We consider the scenario in which Eavesdroppers (Eves) can compromise the system by attempting URA or BSA, as shown in Fig. 1. In the former, Eves locate on the ground and try to tap the transmitted signal from LEO satellites by being within the beam footprint near legitimate users, either at Alice or Bob's location. In the case of URA, the countermeasure is to limit the damage by designing and setting appropriate system parameters. In the latter, we assume that Eves have the capability to split a part of the beam at an LEO satellite to perform the BSA. As a portion of the signal is lost, it is possible to detect the presence of BSA. Our strategy is, therefore, to propose a method for BSA detection.

B. Non-Coherent CV-QKD Scheme Inspired by BBM92

In each operating scheme, there are two ways to implement QKD protocol owing to how the key information is encoded, namely discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD) [25]. In EB DV-QKD systems, Alice and Bob each receive one photon from the entangled photon pairs sent from Charlie. The measurement of these received photons requires the use of bulky and expensive single-photon detectors [14]. In comparison with DV-QKD, CV-QKD is a cheaper and easier implementation as it is compatible with standard optical communication technologies. In EB CV-QKD systems, a two-mode entangled state is shared between Alice and Bob. Detection in CV-QKD is realized by high-efficiency coherent detectors (homodyne or heterodyne) [26]. However, the key implementation issue with CV-QKD systems comes from the high-cost coherent detectors due to the requirement for the sophisticated phase-stabilized local light [27]. To simplify CV-QKD systems with low-cost implementation, non-coherent CV-QKD has been proposed for the PM CV-QKD [28], [29], [30]. Recently, we have proposed non-coherent CV-QKD inspired by the BBM92 protocol for EB scheme. This protocol is realized by transmitting subcarrier intensity modulation/binary phase-sift keying (SIM/BPSK) signal and using dual-threshold/direct detection (DT/DD) receivers in [24], [31]. The similarities in the security of the original BBM92 and this protocol and its key features are explained in [24]. We review the implementation of non-coherent CV-QKD inspired by the BBM92 protocol and apply it to the new scenario of this article as follows.

Stage 1: Using the quantum channel (FSO channel)

- *Signal preparation at Charlie:* SIM/BPSK modulated signal is generated representing random binary bits "0" and "1". The value of modulation depth δ $(0 < \delta < 1)$ is chosen to be small enough in order that the transmitted state cannot be fully distinguished.

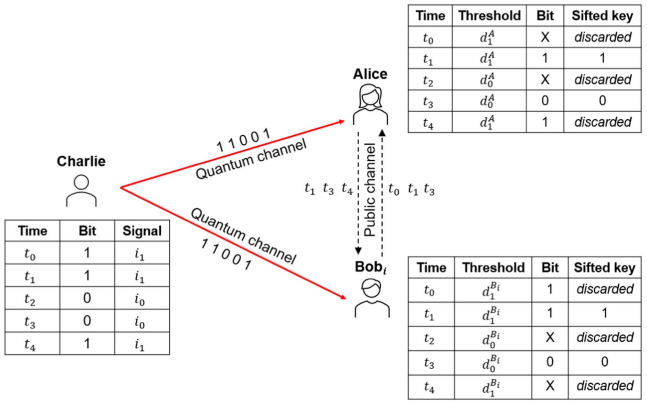


Fig. 2. Example of non-coherent CV-QKD inspired by the BBM92 protocol for EB scheme [24].

- *Signal transmission:* The signal is transmitted simultaneously to both relay satellites, which then amplify and forward the received signal to Alice and Bob$_i$.
- *Detection:* The received signal at Alice and Bob$_i$ is individually detected using their own DT/DD receivers. The two levels of the DT (i.e., d_0^U and d_1^U) at each user are selected symmetrically over the mean signal level.

– If the detected value i_r^U of received current signal at user U is less than d_0^U, the user U detects bit "0".
– If the detected value i_r^U of received current signal at user U is greater than d_1^U, the user U detects bit "1".
– Otherwise, the user U detects bit "X", which specifies the case that either Alice or Bob$_i$ does not detect any bit.

Stage 2: Using the public channel (e.g., the Internet)

- *Sifting process:* Alice and Bob$_i$ notify of the time instants that they were able to create binary bits from received signals. They discard bit values at the time instant that no bit (i.e., bit "X") is detected. Alice and Bob$_i$ then share an identical bit string, i.e., *sifted key*. An example of the detecting and sifting process of this protocol is illustrated in Fig. 2.
- *Post-processing:* Alice and Bob$_i$ perform error correction and privacy amplification to turn the sifted key into a *final shared secret key*.

C. Signal Model

The block diagram of the proposed system is illustrated in Fig. 3. There are four main parts: a GEO satellite (Charlie), LEO satellites as relay nodes, and legitimate users (Alice and Bob$_i$). In the preparation stage, a perfect pre-synchronization realized by using the global positioning system (GPS) between users, LEO satellites, and Charlie is assumed.

At the GEO and LEO Satellites: The raw key data $d(t)$ is modulated onto a radio frequency (RF) subcarrier signal using BPSK scheme prior to modulating the laser irradiance. We denote $P_s(t)$ as the transmitted power of the modulated laser beam. The radiated optical signal is expressed as

$$P_s(t) = \frac{P}{2}\left[1 + \delta m(t)\right], \tag{1}$$

where P is the peak laser power, δ is the intensity modulation depth, and $m(t)$ is the subcarrier signal [24]. It is noted that the two-laser source sending the signal from the GEO satellite to LEO satellites is not a truly entangled one. It was inspired by the BBM92 protocol for EB scheme while the signal from the two-laser source is sent to two LEO satellites simultaneously.

Then, the received signal from the GEO satellite at LEO satellites is passed through an optical band-pass filter (OBPF), amplified optically using erbium-doped fiber amplifiers (EDFA), and forwarded to legitimate users.

At the Legitimate User U: The received optical signal is passed through OBPF, and then detected by a PIN photodetector. The photocurrent i_p^U is given as

$$i_p^U(t) = \frac{1}{2} R_e P G_a h_{\text{e2e}}^U(t)\left[1 + \delta m(t)\right] + n_{\text{e2e}}^U(t), \tag{2}$$

where R_e is the responsivity of the photodetector, G_a is the EDFA gain at the LEO satellite, $h_{\text{e2e}}^U(t)$ is the channel state between Charlie and user U, and $n_{\text{e2e}}^U(t)$ is the receiver noise.

The demodulated signal $r_d^U(t)$ at BPSK demodulator with the DC component filtered out is expressed as

$$r_d^U(t) = \begin{cases} i_0^U = -\frac{1}{4} R_e P \delta G_a h_{\text{e2e}}^U(t) + n_{\text{e2e}}^U(t) \\ i_1^U = \frac{1}{4} R_e P \delta G_a h_{\text{e2e}}^U(t) + n_{\text{e2e}}^U(t) \end{cases}, \tag{3}$$

where $i_r^U, r \in \{0, 1\}$ are the detected signals corresponding to bit "0" and bit "1", respectively.

The receiver noise power at user U, denoted as $(\sigma_N^U)^2$, includes shot noise, background noise, and amplified spontaneous emission (ASE) noise generated by the optical amplifier at the LEO satellite. The formula for $(\sigma_N^U)^2$ is given as

$$(\sigma_N^U)^2 = (\sigma_{\text{sh}}^U)^2 + (\sigma_b^L)^2 + (\sigma_b^U)^2 + (\sigma_a^L)^2 + (\sigma_{\text{th}}^U)^2, \tag{4}$$

where $(\sigma_b^L)^2 = 2qR_e P_b^L h_U \Delta_f$ and $(\sigma_a^L)^2 = 2q\Re P_a^L h_L^U \Delta_f$ are variances of the amplified background noise from the LEO satellite and the ASE noise, respectively. $(\sigma_{\text{sh}}^U)^2 = 2qR_e(\frac{1}{4}P\delta G_a h_{\text{e2e}}^U)\Delta_f$, $(\sigma_b^U)^2 = 2qR_e P_b^U \Delta_f$, $(\sigma_{\text{th}}^U)^2 = \frac{4k_B T}{F_n}\Delta_f$ represent variances of the shot noise, background noise, and thermal noise at user U, respectively. In these formulas, q is the electron charge, k_B is Boltzmann's constant, and h_L^U is the channel state between the LEO satellite and user U. $P_b^L = \Omega_l \pi a_L^2 \Delta\lambda$ is the background noise power collected at the LEO satellite, $P_b^U = \Omega_r \pi a_U^2 \Delta\lambda$ is the background noise power collected at user U's receiver. $\Delta\lambda = \frac{B_0 \lambda^2}{c}$ with c is the speed of light in vacuum. $P_a^L = \frac{hc}{\lambda}(n_{\text{sp}} - 1)G_a B_0$ is the ASE noise power, where h is the Planck constant. $\Delta f = \frac{R_b}{2}$ is the efficient bandwidth. For the remaining notations, they are given in Table. I.

D. Multiple Access Scheme

We consider two methods Charlie can use to transmit the signal to multiple users, called Bob's cluster. In the conventional Time Division Multiplexing Access (TDMA) method, Charlie sends the signal to each user Bob$_i$ within specified time slots. Alice and each user Bob$_i$ receive independent binary bit sequences from Charlie. The key rate will therefore be decreased proportionally to the number of users. To remedy the drawback of TDMA, we exploit the randomness of the fading channels and the DT/DD settings. Specifically, we can let Charlie send

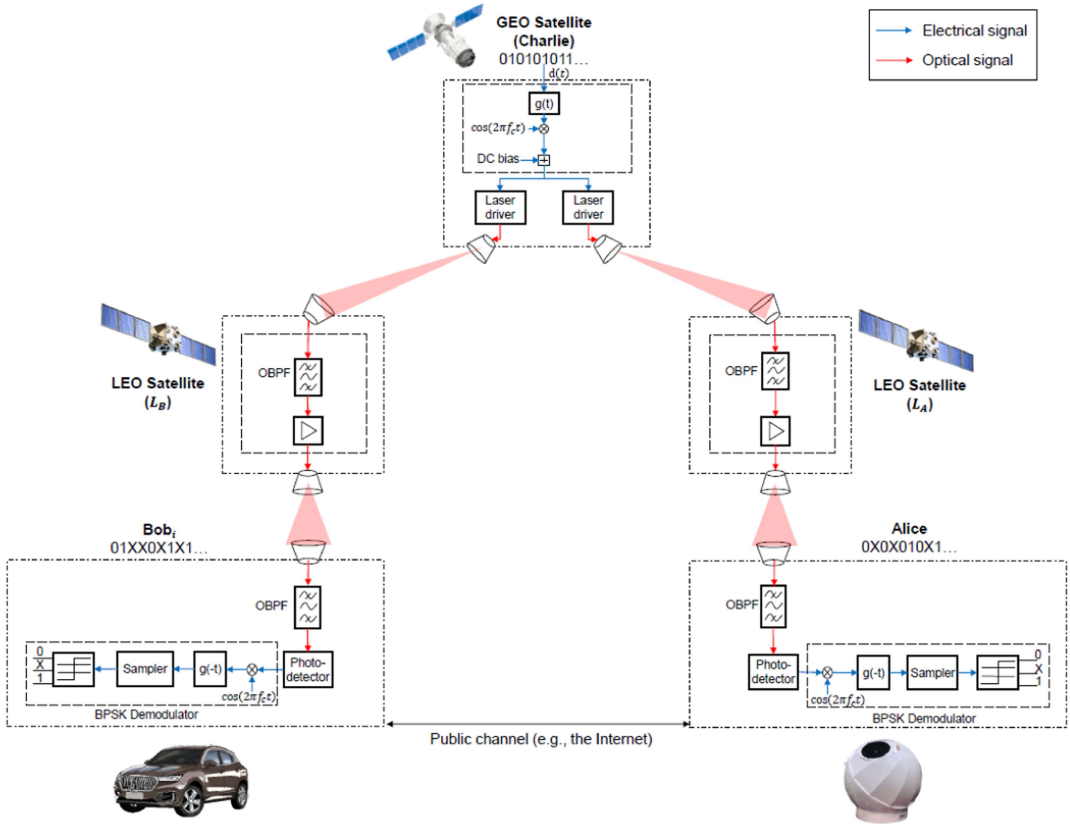


Fig. 3. Block diagram of the proposed satellite-based FSO/QKD system using GEO/LEO satellites.

TABLE I
SYSTEM PARAMETERS

Name	Symbol	Value
GEO Satellite (Charlie)		
Wavelength	λ	1550 nm
Bit rate	R_{b}	1 Gbps
Altitude	H_{C}	35793 km
Divergence angle	θ_C	10 μrad [45]
Transmitted power	P	32 dBm
LEO Satellites (Relay nodes)		
Wavelength	λ	1550 nm
Altitude	H_{L}	550 km
Divergence angle	θ_L	50 μrad
Receiving aperture radius	a_{L}	10 cm
EDFA Gain	G_a	40 dB
ASE Parameter	n_{sp}	5
FSO Channel		
Sun's spectral irradiance from above the atmosphere at 1550 nm	Ω_{l}	0.1 W/cm$^2\cdot\mu$m
Sun's spectral irradiance from above the Earth at 1550 nm	Ω_{r}	0.005 W/cm$^2\cdot\mu$m
Wind speed	w	21 m/s
The refractive index structure parameter at the ground level	$C_n^2(0)$	10^{-15}m$^{-2/3}$
Visibility (Clear weather condition)	V	30 km
Alice/Bob/Eve		
Altitude	H_{U}	2 m
Receiving aperture radius	a_{U}	5 cm
Optical bandwidth	B_0	250 GHz
Responsivity	R_e	0.9 A/W
Effective noise bandwidth	Δf	0.5 GHz
Temperature	T	298 K
Load resistor	R_{L}	1 kΩ
Amplifier noise figure	F_{n}	2

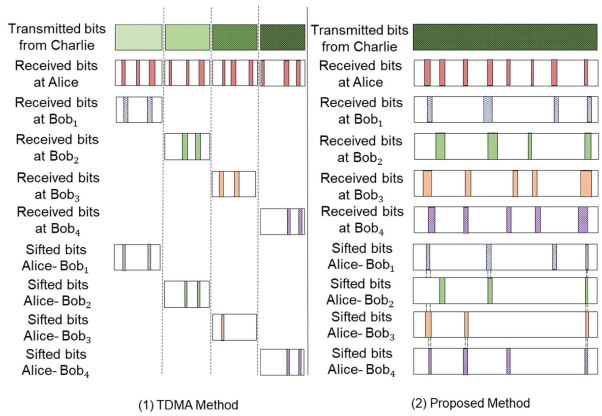


Fig. 4. Conventional TDMA and our proposed approach for the key distribution with $N = 4$.

the same bit sequence to Alice and all users Bob$_i$. As mentioned in Section II-B, only a tiny and random fraction of transmitted bits are detected at each receiver; we expect each pair of Alice and Bob$_i$ to achieve a secret key with a minimum, unknown overlapped with others. This allows a higher achievable key rate while keeping acceptable secrecy between users.

Fig. 4 compares our proposed scheme with the TDMA when Charlie transmits the signal to multiple users. The colored parts of the received bits at Alice and Bob$_i$ illustrate the instants that Alice and Bob$_i$ decoded bits. The blank parts represent the time instants that Alice and Bob$_i$ decoded bit "X" (i.e., no bit is

detected). Sifted bits between Alice and Bob$_i$ are the overlapped parts of the received bits at Alice and Bob$_i$. The knowledge parts of their received bit information from other users Bob$_j$ are aligned by dash lines.

III. Channel Model

The end-to-end channel state between Charlie and user U h^U_{e2e} can be formulated as $h^U_{\text{e2e}} = h^U_G h^U_L$, where h^U_G is the channel state between GEO and LEO satellites, and h^U_L is the channel state between LEO satellites and user U. These channel states are explained in more detail as follows.

A. GEO-to-LEO Channel Model

For the GEO-to-LEO link, the effect of atmospheric is insignificant as the laser signal from the GEO satellite goes through a non-atmospheric region at an altitude above 20 km compared to the sea level [32]. In addition, we assume that a fine tracking system with perfect alignment is equipped [33]. Therefore, it is supposed that the geometric spreading loss of the laser beam is the major impairment for this link. Moreover, the maximum frequency shift in LEO satellite communications is within the capability of the current design for optical satellite communications [32]. Thus, we ignore the Doppler effect in further analysis.

The Gaussian beam model is assumed for the laser beam from the GEO satellite (Charlie (C)). The geometric spreading loss for the position vector from the center of the beam footprint $\boldsymbol{r}$ at LEO satellites is then given by [24]

$$h^U_G = h^U_{g_1}(\boldsymbol{r}; L_C) = \int_{A^Z_r} I_{beam}(\boldsymbol{\rho} - \boldsymbol{r}; L_C)\, d\boldsymbol{\rho}, \tag{5}$$

where $I_{beam}(.)$ is the normalized spatial distribution of the transmitted intensity. $h^U_{g_1}(.)$ denotes the fraction of power collected by each LEO satellite's receiver with the receiving area of $A^Z_r, Z \in \{L_A, L_B\}$. L_C is the distances between Charlie and LEO satellites, which can be derived from two-line element (TLE) sets of the GEO and LEO satellites and the geometric analysis as in [34].

The approximated result of this integration is given as [35]

$$h^U_{g_1}(\boldsymbol{r}; L_C) \approx A^Z_0 \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega^2_{L_C,eq}}\right), \tag{6}$$

where $\|\boldsymbol{r}\|$ is the radial distance from the center of beam footprint, $A^Z_0 = [\text{erf}(\nu_Z)]$ is the fraction of the collected power at $\boldsymbol{r} = 0$ with $\nu_Z = \frac{\sqrt{\pi} a_Z}{\sqrt{2}\omega_{L_C}}$, where a_Z is the radius of Z's receiving telescope aperture, and $\omega^2_{L_C,eq} = (\omega^2_{L_C} \frac{\sqrt{\pi}\text{erf}(\nu_Z)}{2\nu_Z \exp(-\nu^2_Z)})^{1/2}$ is the equivalent beam radius at distance L_C. ω_{L_C} is the beam radius at distance L_C and is given as $\omega_{L_C} = \omega_{0,C}[1 + (\frac{L_C\lambda}{\pi\omega^2_{0,C}})^2]^{1/2}$, where $\omega_{0,C} = \lambda/2\theta_C$ is the beam waist at the transmitter of C, and λ is the operation wavelength. Here, θ_C is the full beam divergence angle determined as $\theta_C = 2.44\lambda/D_G$, where D_G is the diameter of GEO's transmitting telescope aperture [36].

For simplicity's sake, LEO satellites are assumed to be at the center of Charlie's beam footprint. The fraction of collected power at LEO satellites is given as $h^U_{g_1}(0; L_C) \approx A^Z_0$.

B. LEO-to-User Channel Model

For LEO-to-user link, we take into account three major impairments: geometric spreading loss $h^U_{g_2}$, atmospheric attenuation h^U_l, and atmospheric turbulence h^U_a. The composite channel for LEO-to-user link, thus, can be formulated as $h^U_L = h^U_{g_2} h^U_l h^U_a$. These impairments are described as follows

1) Geometric Spreading Loss: : We consider the Gaussian beam model for the laser beam from LEO satellites. With a similar approach in Section III-A, the fraction of power collected by the user U's receiver is approximated as

$$h^U_{g_2}(\boldsymbol{r}; L_Z) \approx A^U_0 \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega^2_{L_Z,eq}}\right), \tag{7}$$

where $L_Z = (H_Z - H_U)/\cos(\zeta_U), Z \in \{L_A, L_B\}$ is the distance between the LEO satellite (L_A or L_B) and user U. H_Z and H_U are altitudes of the LEO satellite and user U, respectively. ζ_U is the zenith angle between the LEO satellite and user U, which can be derived from TLE set of the LEO satellite [37]. $A^U_0 = [\text{erf}(\nu_U)]$ is the fraction of the collected power at $\boldsymbol{r} = 0$ with $\nu_U = \frac{\sqrt{\pi} a_U}{\sqrt{2}\omega_{L_Z}}$ where a_U is the radius of U's receiving telescope aperture. $\omega_{L_Z} = \omega_{0,Z}[1 + (\frac{L_Z\lambda}{\pi\omega^2_{0,Z}})^2]^{1/2}$, where $\omega_{0,Z} = \lambda/2\theta_Z$ is the beam waist at the transmitter of Z, and θ_Z is the full beam divergence angle determined as $\theta_Z = 2.44\lambda/D_U$ with D_U the diameter of user's transmitting telescope aperture [36]. $\omega^2_{L_Z,eq} = (\omega^2_{L_Z} \frac{\sqrt{\pi}\text{erf}(\nu_U)}{2\nu_U \exp(-\nu^2_U)})^{1/2}$ is the equivalent beam radius at distance L_Z. The user U is assumed to be at the center of Charlie's beam footprint. The fraction of collected power at LEO satellites is thus derived as $h^U_{g_2}(0; L_Z) \approx A^U_0$.

2) Atmospheric Attenuation: The attenuation of laser power through the atmosphere is formulated by the exponential Beer-Lambert's law as

$$h^U_l = \exp(-\xi L_U), \tag{8}$$

where $L_U = (H_h - H_U)/\cos(\zeta_U)$ is the propagation distance to user U with the altitude $H_h = 20$ km that the atmospheric attenuation mainly occurs below [13]. ξ is the attenuation coefficient, and determined as [38]

$$\xi(\lambda) = \frac{3.912}{V[\text{km}]}\left(\frac{\lambda[\text{nm}]}{550}\right)^{-q(V)}, \tag{9}$$

where V is the atmospheric visibility. Depending on the weather conditions, the value of V will be changed. The value of the atmospheric attenuation visibility coefficient $q(V)$ is modeled with respect to the value of V as shown in [39].

3) Atmospheric Turbulence-Induced Fading: Atmospheric turbulence causes by inhomogeneities in the temperature and pressure of the atmosphere, which lead to variations of the refractive index along the transmission path [39]. This phenomenon ultimately results in fading of the received optical power, thus leading to system performance degradation. As reported in [32], the turbulence strength for LEO-to-user link is usually weak with the zenith angles being equal to or less than 60° (due to the minimum acceptable elevation angle for satellite tracking being set to 30°). Therefore, the distribution of h^U_a can be modeled as a log-normal distribution that suits the weak turbulence regime.

It can be formulated as [35]

$$f_{h_a^U}(h_a^U) = \frac{1}{\sqrt{8\pi} h_a^U \sigma_X^U} \exp\left(- \frac{\left[\ln(h_a^U) - 2\mu_X^U\right]^2}{8(\sigma_X^U)^2} \right), \quad (10)$$

where $\mu_X^U = -(\sigma_X^U)^2$ and $(\sigma_X^U)^2$ are the mean and variance of log-amplitude fluctuation, respectively. $(\sigma_X^U)^2$ is calculated as [40]

$$(\sigma_X^U)^2 = 0.56\, k^{7/6} \sec^{11/6}(\zeta_U) \int_{H_U}^{H_h} C_n^2(h)\, (h - H_U)^{5/6}\, \mathrm{d}h, \quad (11)$$

where $k = 2\pi/\lambda$ is the wave number, and $\sec(x)$ is the secant function. The refractive index structure parameter $C_n^2(\mathrm{m}^{-2/3})$ can be modeled by Hufnagel-Valley as $C_n^2(\mathrm{m}^{-2/3}) = 0.00594(\frac{w}{27})^2(10^{-5}h)^{10}\exp(-\frac{h}{1000})\exp(-\frac{h}{1500}) + 2.7 \times 10^{-16}\exp(-\frac{h}{1500}) + C_n^2(0)\exp(-\frac{h}{100})$, where w (m/s) is the average wind velocity, h (m) is the height above the ground, and $C_n^2(0)$ is the refractive index structure parameter at the ground level.

IV. Performance Analysis

This section presents the analytical framework to analyze the performance of the proposed system using the non-coherent CV-QKD inspired by the BBM92 protocol for EB scheme. We first derive the sift probability between Alice and an individual Bob in the context of multiple users for both TDMA and the proposed multiple-access method. The quantum bit-error rate (QBER) and the total final key creation rate for all users are then derived.

A. Sift Probabilities

1) Single-User Sift Probability: Sift probability (P_{sift}) between Charlie (the satellite) and a legitimate user U is the probability that the user can decode bits using the DT detection, which is given as

$$P_{\text{sift}}^{C,U} = P_{C,U}(0,0) + P_{C,U}(0,1) + P_{C,U}(1,0) + P_{C,U}(1,1), \quad (12)$$

where $P_{C,U}(x,y)\ (x,y \in \{0,1\}) = P_C(x)P_{U|C}(y|x)$ is the joint probability that bit "x" sent by Charlie coincides with the decoded bit "y" of user U. $P_C(x)$ is the probability that Charlie sends bit "x". Bits "0" and "1" are assumed equally likely to be transmitted; thus, $P_C(x) = \frac{1}{2}$. $P_{U|C}(y|x)$ is the conditional probability that Charlie transmits bit "x" when user U detects bit "y" and calculated as [41]

$$P_{U|C}(0|x) = \int_0^\infty Q\left(\frac{i_x^U - d_0^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \quad (13)$$

$$P_{U|C}(1|x) = \int_0^\infty Q\left(\frac{d_1^U - i_x^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \quad (14)$$

where $i_0^U = -i_1^U = -\frac{1}{4}R_e P G_a \delta h_{\text{e2e}}^U$ are the received current signals for bit "0" and bit "1", respectively. $Q(\cdot)$ is the Q-function. Two thresholds d_0^U and d_1^U at the receiver of user U are determined by

$$d_0^U = \mathbb{E}[i_0^U] - \varsigma_U \sigma_N^U, \quad (15)$$

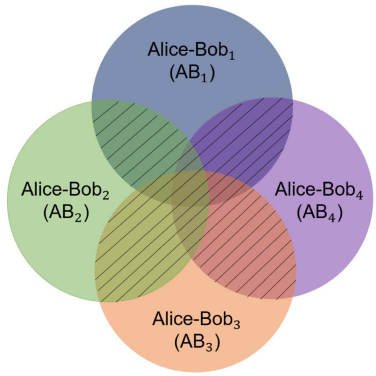


Fig. 5. Visualization for the relationship of sift probabilities between Alice and Bob$_i$, $i \in \{1,2,3,4\}$. The overlapping region is marked by diagonal stripes.

$$d_1^U = \mathbb{E}[i_1^U] + \varsigma_U \sigma_N^U, \quad (16)$$

where ς_U is the DT scale coefficient of user U and $\mathbb{E}[\cdot]$ is the expectation operator. Hence, $\mathbb{E}[i_0^U] = -\frac{1}{4}R_e P G_a \delta h_g^U h_l^U$ and $\mathbb{E}[i_1^U] = \frac{1}{4}R_e P G_a \delta h_g^U h_l^U$, where $h_g^U = h_{g1}^U h_{g2}^U$ and $\mathbb{E}[h_{\text{e2e}}^U] = \mathbb{E}[h_g^U h_l^U h_a^U] = h_g^U h_l^U$ with $\mathbb{E}[h_a^U] = 1$ as the mean irradiance is normalized to unity.

2) Multiple-User Sift Probability:

a) TDMA method: P_{sift} between two legitimate users, namely Alice and Bob$_i$, is the probability that both users can decode a bit sent by Charlie using the DT detection receiver. This probability can be derived as

$$P_{AB_i}^{\text{sift}} = P_{AB_i}(0,0) + P_{AB_i}(0,1) + P_{AB_i}(1,0) + P_{AB_i}(1,1), \quad (17)$$

where $P_{AB_i}(x,y)$ with $x,y \in \{0,1\}$ is the probability that Alice's detected bit "x" coincides with Bob$_i$'s detected bit "y". The probability $P_{AB_i}(x,y)$ is computed as

$$P_{AB_i}(x,y) = P_C(x)P_{A|C}(x|x)P_{B_i|C}(y|x) + P_C(y)P_{A|C}(x|y)P_{B_i|C}(y|y). \quad (18)$$

b) Proposed method: In our proposed method, as Charlie sends the same bit sequence to Alice and all users Bob$_i$, there is a possibility that two or more Bobs can detect the same bit, which is called the *mutual sift probability*. Fig. 5 illustrates the relationship between the sifted bits of four pairs of users Alice-Bob$_i$ (AB_i). To guarantee mutually secret keys, Alice and Bob$_i$ need to exclude sifting bits overlapping with other users. The sift probability between Alice and Bob$_i$ is thus determined as follows

$$P_{AB_i}^{\text{sift-excl}} = P(AB_i) - \varepsilon P(AB_i)_{\text{excl}}, \quad (19)$$

where $P(AB_i)_{\text{excl}}$ is the mutual sift probability with other users Bob$_j$. The exclusion ratio coefficient, $0 \le \varepsilon \le 1$, determines the exclusion ratio of mutual bits; when $\varepsilon = 1$, all mutual bits are excluded. $P(AB_i)_{\text{excl}}$ can be calculated as

$$P(AB_i)_{\text{excl}} = \sum_{1 \le j \le N} P(AB_i \cap AB_j)$$

$$- \sum_{1\le j\le k\le N} P(AB_i \cap AB_j \cap AB_k) + \ldots + (-1)^N P\left(\bigcap_{i=1}^{N} AB_i\right), \quad (20)$$

where $P(AB_i \cap AB_j)$ is denoted for the mutual sift probability between two pairs, AB_i and AB_j. This mutual sift probability $P(AB_i \cap AB_j)$ is expressed as follows

$$\begin{aligned} P(AB_i \cap AB_j) &= P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(0,0,1) \\ &+ P_{AB_iB_j}(0,1,0) + P_{AB_iB_j}(0,1,1) + P_{AB_iB_j}(1,0,0) \\ &+ P_{AB_iB_j}(1,0,1) + P_{AB_iB_j}(1,1,0) + P_{AB_iB_j}(1,1,1), \end{aligned} \quad (21)$$

where $P_{AB_iB_j}(x,y,z)$ with $x,y,z \in \{0,1\}$ is the probability that Alice's detected bit "x" coincides with Bob$_i$'s detected bit "y" and Bob$_j$'s detected bit "z". The probability $P_{AB_iB_j}(x,y,z)$ is then computed as

$$\begin{aligned} P_{AB_iB_j}(x,y,z) &= P_C(x)P_{A|C}(x|x)P_{B_i|C}(y|x)P_{B_j|C}(z|x) \\ &+ P_C(y)P_{A|C}(x|y)P_{B_i|C}(y|y)P_{B_j|C}(z|y). \end{aligned} \quad (22)$$

We assume that bit "0" and bit "1" are equally likely, i.e., $P_C(0) = P_C(1) = 1/2$. DT threshold is set so that the error conditional probabilities $P_{A|C}(y|x)$, $P_{B_i|C}(y|x)$, and $P_{B_j|C}(y|x)$, $x \neq y, x, y \in \{0,1\}$ are small enough to neglect (e.g., below 10^{-6}).

In addition, two levels of DT at receivers are selected symmetrically over "zero" level. Thus, the symmetrical conditional probabilities are equal. We also assume that all users Bob$_i$ are on a circle whose radius is the distance from Bob$_i$ to the center of the beam footprint. The conditional probabilities of B_i given C are the same for all users Bob$_i$. As a consequence, (21) can be rewritten as

$$\begin{aligned} P(AB_i \cap AB_j) &\approx P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(1,1,1) \\ &= P_{A|C}(0|0)\left[P_{B_i|C}(0|0)\right]^2. \end{aligned} \quad (23)$$

From (23), we can simplify (20) as follows

$$P(AB_i)_{\text{excl}} \approx \sum_{k=0}^{N-2} (-1)^k C_{N-1}^{k+1} P_{A|C}(0|0)\left[P_{B_i|C}(0|0)\right]^{k+2}, \quad (24)$$

where N is the number of users and C_{N-1}^{k+1} is the number of combinations of $k+1$ users from a set with $N-1$ users.

B. Quantum Bit Error Rates

Quantum bit error rate (QBER) is used to reflect the bit error rate in the sifted key. QBER of the proposed system is formulated as [24]

$$\text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}}. \quad (25)$$

Depending on calculating QBER between Charlie and the legitimate user or QBER between two legitimate users, P_{error} is determined differently as follows

1) QBER Between Charlie and the Legitimate User:

$$P_{\text{error}} = P_{C,U}(0,1) + P_{C,U}(1,0), \quad (26)$$

where P_{error} is the probability that the transmitted bit from Charlie and the received bit at user U are not the same.

2) QBER Between Two Legitimate Users:

$$P_{\text{error}} = P_{AB_i}(0,1) + P_{AB_i}(1,0), \quad (27)$$

where P_{error} is the probability that the received bits at Alice and Bob$_i$ are not the same.

An approximate expression for QBER can be obtained by plugging the conditional probabilities' approximations in (30) into (12), (17), (25), (26), and (27).

C. Final-Key Creation Rate for Multiple Users

From the information-theoretical viewpoint, we denote the mutual information $I(A;B_i)$, $I(A;E_1)$, $I(B_i;E_2)$, and $I(E_1;E_2)$ are defined as the estimation of the amount of information shared between Alice and Bob$_i$, Alice and Eve$_1$ (Eve$_1$ located near Alice), Bob$_i$ and Eve$_2$ (Eve$_2$ located near Bob$_i$), and Eve$_1$ and Eve$_2$, respectively. All of them can be determined by

$$I(Y;Z) = \sum_{y,z\in\{0,X,1\}} P_{YZ}(y,z)\log_2\left[\frac{P_{YZ}(y,z)}{P_Y(y)P_Z(z)}\right], \quad (28)$$

where $P_{YZ}(y,z)$ with $Y,Z \in \{A, B_i, E_1, E_2\}$ is the probability that Y's detected bit "y" coincides with Z's detected bit "z". $P_Y(y)$, $P_Z(z)$ are probabilities that Y and Z detected bit "y" and bit "z", respectively. In case of $I(A;B_i)$, in the proposed method, $P_{AB_i}(0,0)$ and $P_{AB_i}(1,1)$ needs to exclude respectively the probability $\frac{1}{2}\varepsilon P(AB_i)_{\text{excl}}$ that other users Bob$_j$ also detect the same bit values with user Bob$_i$. In the TDMA method, there is not any effect on $I(A;B_i)$.

After error correction and privacy amplification to exclude the amount of information leaked to Eve$_1$ and Eve$_2$ from the key information shared between Alice and user Bob$_i$ at Bob's cluster, the useful bit rate, namely *final key-creation rate*, is calculated as

$$R_i^f = R_i^s\left[\alpha I(A;B_i) - \max(I(A;E_1), I(B_i;E_2), I(E_1;E_2))\right], \quad (29)$$

where R_i^s is the sifted-key rate, i.e., the length of the raw key that can be produced per unit of time that contains the sifting factor. In case of the TDMA method, $R_i^s = P_{AB_i}^{\text{sift}}\frac{R_b}{N}$. In case of the proposed method, $R_i^s = P_{AB_i}^{\text{sift-excl}}R_b$. R_b is the system bit rate. α accounts for error correction efficiency in post-processing procedures. In this article, we assume perfect error correction efficiency, i.e., $\alpha = 1$, as an upper bound evaluation of the system performance [28].

The *total final key-creation rate* of N users on Bob's cluster is expressed as $R_\Sigma^f = \sum_{i=1}^N R_i^f$.

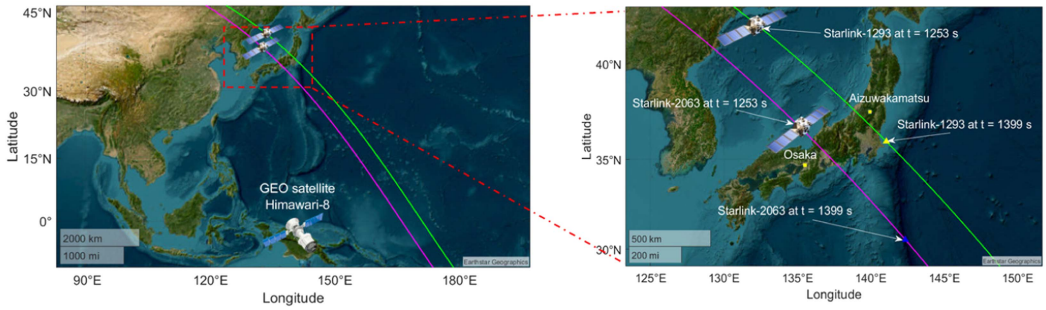


Fig. 6. Position of GEO satellite on the Earth's surface and ground traces of LEO satellites over Japan observed from 16:09:00 UTC+9 2021/12/23.

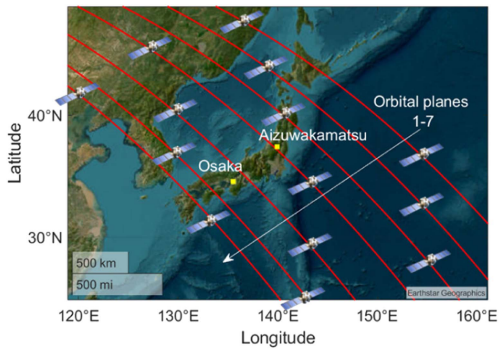


Fig. 7. Seven orbital planes of Starlink satellite constellation over Japan.

V. Design and Analysis: A Case Study of Japan

In this section, we investigate the feasibility of the proposed FSO/QKD systems using GEO and LEO satellites. In particular, a case study of the QKD network for Japan is examined.

A. System Configuration and Satellite Selections

We assume that the server Alice is in Aizuwakamatsu City (longitude: 139.93899°E; latitude: 37.52266°N; elevation: 209.093 m), and the user's cluster Bobs is in Osaka City (longitude: 135.51983°E; latitude: 34.68305°N; elevation: 155.448 m), which is about 500 km southwest of Alice's location. Himawari-8, a Japanese GEO weather satellite operated by the Japan Meteorological Agency [42], is employed as Charlie. Due to the capability of 24/7 global coverage, Starlink satellites are chosen to be the relay nodes [43]. Illustrations of Himawari-8's position and orbits of two Starlink satellites (Starlink-1293 and Starlink-2063) over Japan on December 23rd, 2021 are calculated from the available TLE data in [44] and displayed in Fig. 6. All satellites are supposed to be equipped with optical devices necessary for the proposed system shown in Fig. 3.

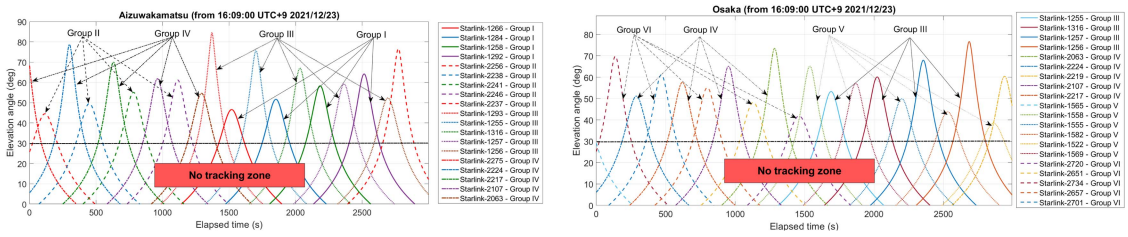
There are seven orbital planes of the Starlink satellite constellation from northwest to southwest of Japan, as shown in Fig. 7. Each plane composes of a group of LEO satellites that fly across Japan alternately. For the sake of clarity, each group is numbered by the orbital plane order at the time of observation. To realize the proposed system, it is required that there exist two LEO satellites that are simultaneously within the required elevation angle with their respective users at any given time. This requirement is verified by Fig. 8(a) and 8(b), which show the evolutions of the elevation angle of satellites in Group I to VI respective to users located in Aizuwakamatsu City and Osaka City during a 3000-second period from 16:09:00 UTC+9 Dec. 23, 2021. For example, during the elapsed time from 1000 to 1200 seconds, Starlink-1293 of group III and Starlink-2063 of group IV are within the required elevation angle with users in Aizuwkamatsu City and Osaka City, respectively. Without loss of generality, in the following analyses, these two satellites are chosen as the relay nodes to forward signals from Charlie to Alice and Bobs.

The parameters used in the analysis, unless otherwise noted, are listed in Table I. Monte Carlo simulations are also provided to validate the correctness of analytical results, and a good match is confirmed. The details of the simulation are as follows. At each second in the elapsed time, we generate 10^7 random binary bits. Also, using parameters given in Table I, we generate 10^7 independent channel states between GEO and LEO satellites h_G^U and between LEO satellite and user h_L^U. The simulation is performed as a discrete event for each bit. Then, we calculate the received current signal for each bit at user U and detect the received bit by comparing it with two thresholds d_0^U and d_1^U. The simulation runs repeatedly 100 times (i.e., the bit rate is 1 Gbps as the given system bit rate). We aggregate the number of received bits "0", "1", and "X".

B. Transmitter Design

We first investigate the design criteria for Charlie's transmitter to maintain the security of the proposed system under URAs. In such attacks, Eves on the ground try to locate their receivers within the beam footprint of the transmitted signal (at the distance of d_{E} m from the footprint center). To prevent URAs, a small modulation depth δ should be set so that Eve would suffer from a high error rate (e.g., $P_{\mathrm{error}}^{\mathrm{E}} > 0.1$) when she tries to decode the received signal using the optimal threshold $d_{\mathrm{t}}^{\mathrm{E}} = 0$[1]. Fig. 9 illustrates the error probabilities at Eves as a function of δ for different values of d_{E}. We consider the worst-case scenario where the relay satellites are closest to legitimate users (i.e., the zenith angle is 0 degrees). In this case, Eve can eavesdrop on the maximum possible information. As seen from the figure, the values of δ should be less than 0.7 to guarantee that $P_{\mathrm{error}}^{\mathrm{E}} > 0.1$ in all chosen values of d_{E}. It is important to note that higher values of δ may lead to a lower key rate and higher

[1] $P_{\mathrm{error}}^{\mathrm{E}}$ can be derived in the similar way as in [24].



(a) Aizuwakamatsu City **(b)** Osaka City

Fig. 8. Illustration of the visibility of Starlink's LEO satellites in two different cities of Japan.

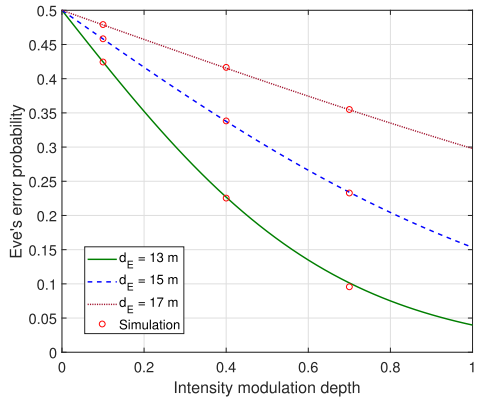


Fig. 9. Eve's error probability versus intensity modulation depth.

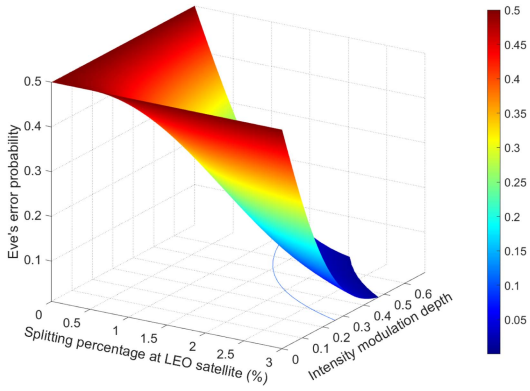


Fig. 10. Eve's error probability versus the intensity modulation depth and splitting percentage at LEO satellites.

QBER [46]. Therefore, we set $\delta = 0.5$ for Charlie's transmitter in the analysis. Also, in this figure, the analytical results closely follow the simulated ones, confirming the model's correctness and analysis.

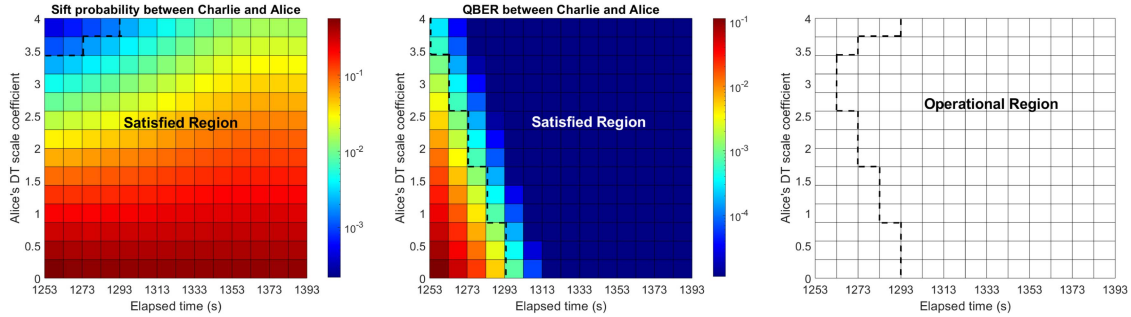
In addition, we consider the case that LEO satellites are attacked by BSA. Fig. 10 shows Eve's error probability versus the modulation depth and the splitting percentage of the signal received at LEO satellites for different modulation depths δ. It is observed that if δ is decreased, Eve needs a more significant amount of the received power at LEO satellites to reduce its error probability. With our transmitter settings (transmitted power, modulation depth, etc.), it is seen that Eve needs at least 1.5% of splitting power to gain an acceptable BER (less than 10%). This minimum splitting percentage is used in further analysis as the lower bound on the performance of BSA detection.

C. Receiver Design

The secrecy performance of the proposed system is significantly influenced by the selection of the dual threshold, which is in turn determined by the DT scale coefficient ς_U. In this section, systematic selections of ς_U for Alice and Bobs are studied.

1) Alice's Receiver Design: Firstly, the selection of ς_A should satisfy two requirements: (i) the sift probability is above 10^{-3} to achieve sifted-key rates at Mbps with Gbps transmission rates of FSO communications; (ii) QBER is kept below 10^{-3} so that the error can be corrected efficiently at Mbps of sifted-key rates by error-correcting code. From Fig. 11(a), (b), and (c), we can determine the range of ς_A values to satisfy two conditions with the sift probability and QBER. For this purpose, Fig. 11(a), 11(b), and 11(c) show the values of ς_U satisfying (i), (ii), and both during the communicable period between Starlink-1293 and Alice. It is seen that from the elapsed time of 1293 s, any value between 0 and 4 can be chosen for ς_A.

In addition to the above requirements, Alice should be able to detect BSA attacks. It can be done by comparing the difference in the sift probability between Charlie and Alice $P_{\text{sift}}^{C,A}$ in the case of BSA and no BSA. The larger the difference is, the more likely a BSA is detected. As shown in Fig. 12, this difference increases as ς_A decreases. The question is how much difference would be enough to detect BSAs with high accuracy. To answer this, we first simulate in Fig. 13 the value of $P_{\text{sift}}^{C,A}$ during the first 10-second period assuming that the transmission rate is 1 Gbps. The time resolution is set to 10^{-2}. Assume that BSAs with the power splitting percentage (SP) of 1.5% happen with a probability of 0.01 (i.e., 1% of the simulation time). Since 10^7 bits are transmitted at each time instance, $P_{\text{sift}}^{C,A}$ is simulated as the average of 10^7 independently random values given in (12). Thus, according to the central limit theorem [47], $P_{\text{sift}}^{C,A}$ at each time instance can be well approximated by a normal random variable with the standard deviation denoted as σ_{sd}. When a BSA happens, $P_{\text{sift}}^{C,A}$ decreases, resulting in an increase in its deviation (i.e., the difference between $P_{\text{sift}}^{C,A}$ and its mean value). An attack event can then be detected if the deviation of $P_{\text{sift}}^{C,A}$ exceeds a properly chosen threshold d_{BSA}, which is determined in what follows. Firstly, we define the following events. A false alarm is an event that the deviation of $P_{\text{sift}}^{C,A}$ exceeds the threshold yet no actual BSA is conducted. A missed



(a) $P_{\text{sift}} \geq 10^{-3}$ **(b)** QBER$\leq 10^{-3}$ **(c)** $P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$

Fig. 11. P_{sift} and QBER between Charlie and Alice versus Alice's DT scale coefficient and the elapsed time.

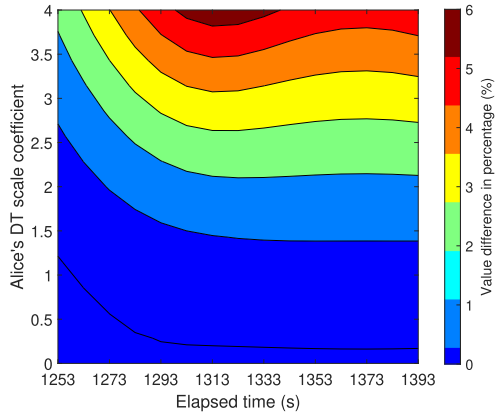


Fig. 12. Difference in the sift probability between Alice and Charlie in the case that no BSA and BSA are performed by L_A, SP $= 1.5$ %.

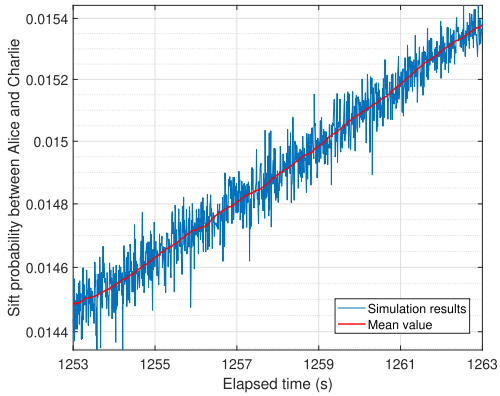


Fig. 13. Simulation results of the sift probability between Alice and Charlie under 1% chance of BSA with SP $= 1.5\%$.

BSA event is an actual BSA that can not be detected due to the low deviation of $P_{\text{sift}}^{C,A}$ compared with the threshold d_{BSA}. A probable BSA event is an event that is either a false alarm or an actual BSA. To prevent frequent false alarms (which may interrupt the communication session), $d_{\text{BSA}} \geq 2\sigma_{\text{sd}}$ is considered. A visualization of these events is displayed in Fig. 14 for the case that $d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$. For different settings of d_{BSA} and differences in $P_{\text{sift}}^{C,A}$ between BSA and no BSA, the numbers of actual BSA events, probable BSA events, false alarms, and correct BSA detections are tabulated in Table II. Here, it can be seen that increasing d_{BSA} results in higher percentages of

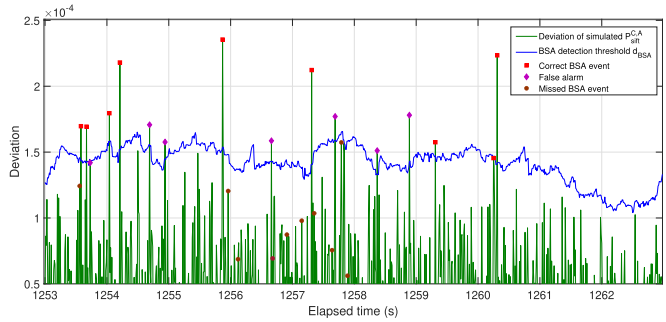


Fig. 14. BSA detection by comparing the deviation of simulated $P_{\text{sift}}^{C,A}$ with the threshold $d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$.

correct attack detection and lower percentages of false alarms. Specifically, when the difference in $P_{\text{sift}}^{C,A}$ between BSA and no BSA is higher than 2% (corresponding to $\varsigma \geq 2.5$ as shown in Fig. 12), the percentages of correct detection (w.r.t both No. actual BSA and probable BSA events) can be made to 100% by choosing $d_{\text{BSA}} = 3\sigma_{\text{sd}}$. Together with the requirements of the sift probability and QBER described above, ς_A should satisfy that $2.5 \leq \varsigma_A \leq 4$. Nonetheless, according to Fig. 11(a), as ς_A increases, the sift probability decreases. Since high values of the sift probability are preferable, $\varsigma_A = 2.5$ is chosen for our design.

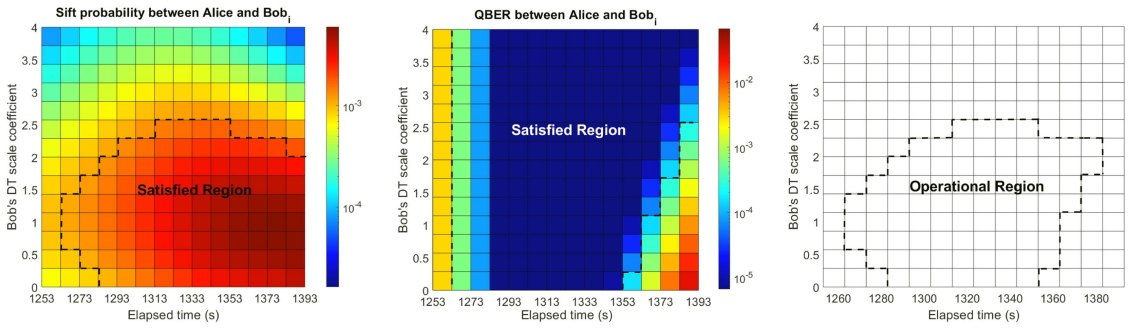
2) Bobs' Receiver Design: To ensure that each user Bob$_i$ can operate properly even if he excludes all key information that other users can be known when applying the proposed system, we assume that $\varepsilon = 1$. Similar to Alice's receiver design, the requirements for selecting ς_{B_i} should satisfy: (i) the sift probability between Alice and Bob$_i$ is higher than 10^{-3}, and (ii) the QBER between them is lower than 10^{-3}. Observing from Fig. 15(a), 15(b), and 15(c), any value of ς_{B_i} between 0 and 2.5 satisfies these requirements. In addition, regarding the detection of BSAs, to achieve a higher 2% difference in the sift probability between Charlie and Bob$_i$ between no BSA and BSA (performed by L_B with SP $= 1.5\%$), ς_{B_i} should be at least 2.25 as shown in Fig. 16. Therefore, $\varsigma_{B_i} = 2.25$ is chosen to maximize the sift probability between Alice and Bob$_i$.

D. Secret-Key Performance

In this section, we investigate the secret-key performance of the proposed system in terms of the total final-key creation rates of all users. The number of users at Bob's cluster is $N = 4$. We

TABLE II
SIMULATION RESULTS OF BSA DETECTION

Difference in $P_{\text{sift}}^{C,A}$ between no BSA and BSA	No. of actual BSA events	No. of probable BSA events	No. of correct BSA events	Percentage of correct detection (w.r.t No. of actual BSA events)	Percentage of correct detection (w.r.t No. of probable BSA events)	No. of false alarms	Percentage of false alarms (w.r.t No. of probable BSA events)
$d_{\text{BSA}} = 2\sigma_{\text{sd}}$							
1.1%-1.5%	19	21	13	68.42%	61.9%	8	31.9%
1.5%-1.8%	15	20	9	60%	45%	11	55%
1.8%-2%	12	24	12	100%	50%	12	50%
2%-2.4%	14	16	14	100%	87.5%	2	12.5%
$d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$							
1.1%-1.5%	19	16	9	47.37%	56.25%	7	43.75%
1.5%-1.8%	15	12	8	53.33%	66.67%	4	33.33%
1.8%-2%	12	17	12	100%	70.59%	5	29.41%
2%-2.4%	14	15	14	100%	93.33%	1	0.67%
$d_{\text{BSA}} = 2.5\sigma_{\text{sd}}$							
1.1%-1.5%	19	11	8	42.1%	72.73%	3	27.27%
1.5%-1.8%	15	7	6	40%	85.71%	1	14.29%
1.8%-2%	12	11	10	83.33%	90.91%	1	9.09%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 2.75\sigma_{\text{sd}}$							
1.1%-1.5%	19	5	4	21.05%	80%	1	20%
1.5%-1.8%	15	6	6	40%	100%	0	0%
1.8%-2%	12	9	9	75%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 3\sigma_{\text{sd}}$							
1.1%-1.5%	19	4	4	21.05%	100%	0	0%
1.5%-1.8%	15	5	5	33.33%	100%	0	0%
1.8%-2%	12	7	7	58.33%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%



(a) $P_{\text{sift}} \geq 10^{-3}$ **(b)** QBER$\leq 10^{-3}$ **(c)** $P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$

Fig. 15. P_{sift} and QBER between Alice and Bob$_i$ versus Bob$_i$'s DT scale coefficient and the elapsed time.

assume that there are two eavesdroppers performing URAs at Alice's and Bob cluster's locations as depicted in Fig. 1. The eavesdroppers are assumed to be located 26 meters away from the legitimate users. Under the design of Alice's and Bob$_i$'s receiver presented in the previous sections, Fig. 17 illustrates the total final-key creation rates of all users $R_{\sum}^{f}$ versus the exclusion ratio coefficient ε at different elapsed time instances that Charlie transmits the signal to the relays. It is observed that $R_{\sum}^{f}$ of the TDMA method is nearly three times lower than that of the proposed system. To ensure that different secret keys are generated for users (i.e., no mutual sift probabilities among 4 users), Bob$_i$ can keep 0% of the overlapped permission (i.e., $\varepsilon = 1$). $R_{\sum}^{f}$ can increase if Bob$_i$ allows a larger percentage of the overlapped permission among all users. For example, at the elapsed time $t = 1328$ s, $R_{\sum}^{f}$ increases by 7% if Bob$_i$ keeps 50% of the overlapped permission (i.e., $\varepsilon = 0.5$) when he is in a trusted network. However, this also increases the knowledge of key information among users, resulting in reduced security of the proposed system if the trust relationship among all users is broken.

Finally, Fig. 18 investigates $R_{\sum}^{f}$ with respect to the number of users at Bob's cluster at the elapsed time $t = 1323$ s. In addition to $\varsigma_{B_i} = 2.25$ chosen from the previous section, we also examine other lower values of ς_{B_i} in the operational region of ς_{B_i}. In the case of TDMA, it can be seen that $R_{\sum}^{f}$ keeps unchanged when the number of users increases. In the proposed method,

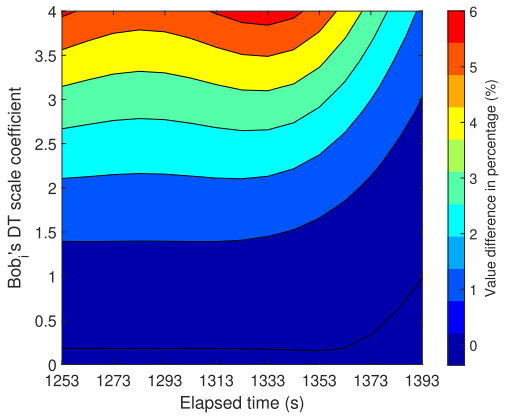


Fig. 16. Value difference in the sift probability between Alice and Bob$_i$ in the case that no BSA and BSA is performed by L_B, SP = 1.5 %.

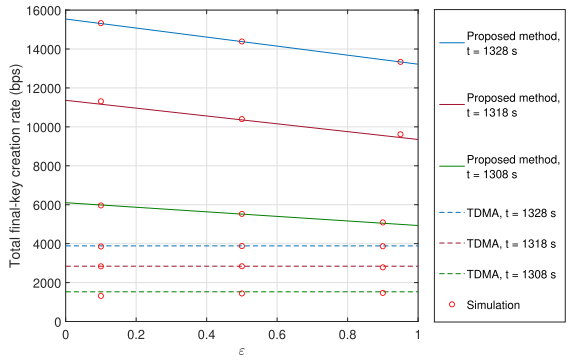


Fig. 17. Total final-key creation rate versus the exclusion ratio coefficient with $N = 4$: Proposed method versus TDMA method.

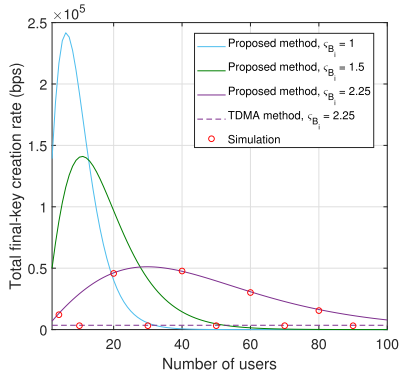


Fig. 18. Total final-key creation rate versus the number of users at Bob's cluster.

for each value of ς_{B_i}, there exist an optimal number of users that maximizes $R^f_{\sum}$. For example, the optimal number of users is about 30 when $\varsigma_{B_i} = 2.25$. As ς_{B_i} decreases, the sift probability between Alice and Bob$_i$ increases as shown in Fig. 15(c), leading to an increase in $R^f_{\sum}$ at the optimal number of users.

VI. Conclusion

We presented a novel design framework for a global-scale FSO/QKD network based on a GEO satellite as the secret key source and LEO satellites as relay nodes for multiple wireless users. The non-coherent CV-QKD protocol inspired by the BBM92 protocol for EB scheme was employed. The system performance was analyzed, considering the spreading loss, atmospheric attenuation, and turbulence. Based on the design criteria for the proposed system, we investigated the case study for the Japan QKD network, taking into consideration the two prevalent attacks of URA and BSA. We proposed a multiple-access method to improve the total secret key performance. We also proposed a simple yet effective BSA detection method based on the statistical observation of sift probability by legitimate users. The numerical and simulation results confirmed the feasibility of implementing the FSO/QKD system.

Appendix A

Approximate Expressions for (13) and (14)

By using the Gauss-Hermite quadrature, approximate expressions for (13) and (14) can be obtained. Specifically, (13) and (14) can be written in the form $\int_{-\infty}^{\infty} g(y)\exp(-y^2)\mathrm{d}y$ by making a change of variable $y = \frac{\ln(h_a^U)+(\sigma_X^U)^2}{\sqrt{8\pi}h_a^U\sigma_X^U}$, where $g(y)$ is a function of the variable y [46]. Next, this integral is approximated using the Gauss-Hermite quadrature as [39]

$$\int_{-\infty}^{\infty} g(y)\exp(-y^2)\mathrm{d}y \approx \sum_{i=1}^{n} \omega_i g(x_i), \tag{30}$$

where n is the order of approximation, while ω_i and x_i are weight factors and zeros of the Hermite polynomial, respectively. Notably, the Gauss-Hermite used for (13) and–(14) quickly converges to the exact-form expressions for a finite value of n, i.e., $n = 20$ terms.

Appendix B

Proof of the Equation (20)

$P^{\text{sift-excl}}_{AB_i}$ can be written in the form of set theory as

$$P^{\text{sift-excl}}_{AB_i} = P(AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C), \quad \text{with } i \in \{1, \ldots, N\}, \tag{31}$$

where $(AB_j)^C, j \neq i$ is the complement of (AB_j).

Proposition 1: For every $N \geq 2$, the sift probability between Alice and Bob$_i$ in the proposed system is calculated as

$$P^{\text{sift-excl}}_{AB_i} = P(AB_i) - \sum_{1\leq j\leq N} P(AB_i \cap AB_j) + \sum_{1\leq j\leq k\leq N} P(AB_i \cap AB_j \cap AB_k) + \ldots - (-1)^N P\left(\bigcap_{i=1}^{N} AB_i\right). \tag{32}$$

Proof: We give a proof by induction on N.

Base Case: Show that the statement holds for $N = 2$. It is easy to calculate and verify the result $P_{AB_i}^{\text{sift-excl}}$ for $N = 2$ as

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} &= P\left(AB_i \cap (AB_1)^C \cap (AB_2)^C\right) \\ &= P(AB_i) - P(AB_1 \cap AB_2) \quad \text{with} \quad i \in \{1, 2\}. \end{aligned} \tag{33}$$

Induction Step: Suppose that the equation is true for N, we show it for $N + 1$. We have

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} &= P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C \\ &\quad \cap (AB_{N+1})^C) \\ &= P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C) \\ &\quad - P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C \\ &\quad \cap (AB_{N+1})) \\ &= S_1 - S_2. \end{aligned} \tag{34}$$

The first term, which is denoted as S_1, has been supposed to be true and has been written as

$$\begin{aligned} S_1 = P(AB_i) &- \sum_{1 \le j \le N} P(AB_i \cap AB_j) \\ &+ \sum_{1 \le j \le k \le N} P(AB_i \cap AB_j \cap AB_k) + \ldots \\ &- (-1)^N P\left(\bigcap_{i=1}^{N} AB_i\right). \end{aligned} \tag{35}$$

The second term, which is denoted as S_2, has been developed as follows

$$\begin{aligned} S_2 &= P\left(\, AB_i \cap AB_{N+1} \cap \left[\, (AB_1)^C \cap (AB_2)^C \right.\right. \\ &\quad \left.\left. \ldots \cap (AB_N)^C\right]\right) \\ &= P(AB_i \cap AB_{N+1}) \\ &\quad - P\left[(AB_i \cap AB_{N+1} \cap AB_1) \cup \right. \\ &\quad \times (AB_i \cap AB_{N+1} \cap AB_2) \\ &\quad \left. \ldots \cup (AB_i \cap AB_{N+1} \cap AB_N)\right]. \end{aligned} \tag{36}$$

Applying the inclusion-exclusion principle [48] for the second term of S_2, it is continued to calculate as

$$\begin{aligned} S_2 &= P\left(AB_i \cap AB_{N+1}\right) \\ &\quad - \sum_{1 \le j \le N} P\left(AB_i \cap AB_{N+1} \cap AB_j\right) \\ &\quad + \sum_{1 \le j \le k \le N} P\left(AB_i \cap AB_{N+1} \cap AB_j \cap AB_k\right) - \ldots \\ &\quad - (-1)^{N+1} P\left(\bigcap_{i=1}^{N+1} AB_i\right). \end{aligned} \tag{37}$$

Combining S_1 and S_2, the equation for $N + 1$ user is given as

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} = P(AB_i) &- \sum_{1 \le j \le N+1} P(AB_i \cap AB_j) \\ &+ \sum_{1 \le j \le k \le N+1} P(AB_i \cap AB_j \cap AB_k) \ldots \\ &- (-1)^N P\left(\bigcap_{i=1}^{N} AB_i\right) + (-1)^{N+1} P\left(\bigcap_{i=1}^{N+1} AB_i\right) \end{aligned} \tag{38}$$

The equation for $N + 1$ also holds true, establishing the induction step. The equation (20) has been proved successfully.

Conclusion: Since both the base case and the induction step have been proved as true by mathematical induction, the equation to calculate $P_{AB_i}^{\text{sift-excl}}$ holds for every number of N.

REFERENCES

[1] M. Q. Vu, H. D. Le, and A. T. Pham, "A proposal of satellite-based FSO/QKD system for multiple wireless users," in *Proc. Int. Conf. Emerg. Technol. Commun.*, 2022, pp. 1–4, doi: 10.34385/proc.72.O4-2.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Modern Phys.*, vol. 92, May 2020, Art. no. 025002.

[3] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, Jan. 1983.

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

[5] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," in *Proc. IEEE Conf. Technol. Homeland Secur.*, 2012, pp. 156–161.

[6] D. Rosenberg et al., "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, Jan. 2007, Art. no. 010503.

[7] A. Boaron et al., "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, Nov. 2018, Art. no. 190502.

[8] B.-X. Wang et al., "Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber," *Opt. Exp.*, vol. 28, no. 9, pp. 12558–12565, Apr. 2020.

[9] Y.-H. Gong et al., "Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror," *Opt. Exp.*, vol. 26, no. 15, pp. 18897–18905, Jul. 2018.

[10] Y. Cao et al., "Entanglement-based quantum key distribution with biased basis choice via free space," *Opt. Exp.*, vol. 21, no. 22, pp. 27260–27268, Nov. 2013.

[11] S.-K. Liao et al., "Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab," *Chin. Phys. Lett.*, vol. 34, no. 9, Aug. 2017, Art. no. 090302.

[12] W. He, S. Guha, J. H. Shapiro, and B. A. Bash, "Performance analysis of free-space quantum key distribution using multiple spatial modes," *Opt. Exp.*, vol. 29, no. 13, pp. 19305–19318, Jun. 2021.

[13] R. Bedington, J. Mantilla, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, Jul. 2017, Art. no. 30.

[14] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Rev. Modern Phys.*, vol. 94, Jul. 2022, Art. no. 035001. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.94.035001

[15] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-based QKD," *Opt. Photon. News*, vol. 11, pp. 26–33, Feb. 2018.

[16] E. Kerstel et al., "Nanobob: A CubeSat mission concept for quantum communication experiments in an uplink configuration," *EPJ Quantum Technol.*, vol. 5, no. 6, Jun. 2018, doi: 10.1140/epjqt/s40507-018-0070-7.

[17] H. Takenaka et al., "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photon.*, vol. 11, no. 8, pp. 502–508, 2017.

[18] R. Bedington et al., "Nanosatellite experiments to enable future space-based QKD mission," *EPJ Quantum Technol.*, vol. 3, 2016, Art. no. 16.

[19] D. Oi et al., "CubeSat quantum communications mission," *EPJ Quantum Technol.*, vol. 4, pp. 1–20, 2017.

[20] O. Lee and T. Vergoossen, "An updated analysis of satellite quantum-key distribution missions," 2019. [Online]. Available: https://arxiv.org/abs/1909.13061

[21] J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, pp. 1–5, Jun. 2020.
[22] S. Ecker, J. Pseiner, J. Piris, and M. Bohmann, "Advances in entanglement-based QKD for space applications," 2022. [Online]. Available: https://arxiv.org/abs/2210.02229
[23] H. Donovan, "Reduction of the minimum elevation angle for NASA satellite laser ranging tracking operations," MD, USA: Honeywell, 2001. [Online]. Available: https://cddis.nasa.gov/lw12/docs/Donovan_Reduction%20in%20the%20Minimum%20Elevation.pdf
[24] M. Q. Vu, H. D. Le, T. V. Pham, and A. T. Pham, "Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/direct detection," *IEEE Access*, vol. 10, pp. 113260–113274, 2022.
[25] X. Tang, R. Kumar, S. Ren, A. Wonfor, R. Penty, and I. White, "Performance of continuous variable quantum key distribution system at different detector bandwidth," *Opt. Commun.*, vol. 471, 2020, Art. no. 126034. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S003040182030451X
[26] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 881–919, Firstquarter 2019.
[27] T. Hirano et al., "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A*, vol. 68, Oct. 2003, Art. no. 042331.
[28] 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.
[29] 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.*, 2019, pp. 1–6.
[30] M. Q. Vu, T. V. Pham, N. T. Dang, and A. T. Pham, "Design and performance of relay-assisted satellite free-space optical quantum key distribution systems," *IEEE Access*, vol. 8, pp. 122498–122510, 2020.
[31] M. Q. Vu, H. D. Le, and A. T. Pham, "Entanglement-based satellite FSO/QKD system using dual-threshold/direct detection," in *Proc. IEEE Int. Conf. Commun.*, 2022, pp. 3245–3250.
[32] H. D. Le and A. T. Pham, "Level crossing rate and average fade duration of satellite-to-UAV FSO channels," *IEEE Photon. J.*, vol. 13, no. 1, Feb. 2021, Art. no. 7901514.
[33] H. D. Le et al., "Throughput analysis for TCP over the FSO-based satellite-assisted Internet of vehicles," *IEEE Trans. Veh. Tech.*, vol. 71, no. 2, pp. 1875–1890, Feb. 2022, doi: 10.1109/TVT.2021.3131746.
[34] Z. Y. WANG, J. L. Li, Q. Guo, and X. M. Gu, "Analysis on connectivity of inter-orbit-links in a MEO/LEO double-layer satellite network," *Chin. J. Aeronaut.*, vol. 19, no. 4, pp. 340–345, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1000936111603385
[35] 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.
[36] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. Bellingham, WA, USA: SPIE Press Book, 2005.
[37] E. B. Zantou, A. Kherras, and A. Addaim, "Orbit calculation and Doppler correction algorithm in a LEO satellite small ground terminal," in *Proc. 19th Annu. AIAA/USU Small Satell.*, Utah, 2005. [Online]. Available: https://digitalcommons.usu.edu/smallsat/2005/all2005/50/
[38] J. L. Green, B. W. Welch, and R. M. Manning, "Optical communication link atmospheric attenuation model," *Nat. Aeronaut. Space Admin.*, Feb. 2019. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190001012.pdf
[39] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communication: System and Channel Modeling With MATLAB*, 1st ed. Boca Raton, FL USA: CRC Press, 2013.
[40] H. Kaushal, V. K. Jain, and S. Kar, *Free Space Optical Communication*, 1st ed. Berlin, Germany: Springer, 2017.
[41] P. V. Trinh, 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.
[42] K. Bessho et al., "An introduction to himawari-8/9—Japan's new-generation geostationary meteorological satellites," *J. Meteorological Soc. Jpn.*, vol. 94, pp. 151–183, 2016.
[43] S. Cakaj, "The parameters comparison of the "Starlink" LEO satellites constellation for different orbital shells," *Front. Commun. Netw.*, vol. 2, 2021, Art. no. 643095. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frcmn.2021.643095
[44] CelesTrak, "Celestrak orbit visualization," 2021. [Online]. Available: https://celestrak.com/
[45] A. Carrasco-Casado and R. Mata-Calvo, *Space Optical Links for Communication Networks*. Berlin, Germany: Springer, 2020, doi: 10.1007/978-3-030-16250-4_34.
[46] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over FSO: Current development and future perspectives," in *Prog. IEEE Electromagn. Res. Symp. (PIERS-Toyama)*, 2018, pp. 1672–1679.
[47] A. Lyon, "Why are normal distributions normal?," *Brit. J. Philosophy Sci.*, vol. 65, no. 3, pp. 621–649, 2014. [Online]. Available: https://www.jstor.org/stable/26398398
[48] E. W. Weisstein, "Inclusion-exclusion principle. From MathWorld–A Wolfram Web Resource," Dec. 2022. [Online]. Available: https://mathworld.wolfram.com/Inclusion-ExclusionPrinciple.html