A Proposal of Satellite-based FSO/QKD System for Multiple Wireless Users

Minh Q. VU[†], **Hoang D. LE**[†], ***Nonmembers***, ***and*** **Anh T. PHAM**[†a)], ***Member***

SUMMARY This paper proposes a satellite-based free-space optical (FSO) continuous-variable quantum key distribution (CV-QKD) system for multiple users. The proposed system imitates the entanglement-based scheme by using a dual-threshold direct-detection receiver. Therefore, it is simpler and possibly cheaper than the previously proposed discrete-variable (DV) and CV-QKD systems. In addition, for the first time, the scenario of multiple users is considered by using a large footprint of FSO signal. We model and theoretically analyze the performance of the proposed system in terms of the total final-key creation rates of all users, considering the channel loss, atmospheric turbulence-induced fading, and receiver noises. In our analysis, we assume the Gaussian beam model to evaluate the impact of geometric spreading on the signal received by multiple users and the possible attack from eavesdroppers. Based on the derived results, we can determine the sufficient number of users that the considered QKD system can support.

key words: *Free-space optics, quantum key distribution, satellite, multiple users, atmospheric turbulence, Gaussian beam*

1. Introduction

Quantum key distribution (QKD) is an emerging application of quantum mechanics that helps to distribute shared keys to remote users with information-theoretic security. Many QKD systems have been developed over the past few decades since its proposal in 1984 [1]. These systems are proposed for use in different transmission mediums, including optical fibers, terrestrial free-space optical (FSO) links, and satellite-based FSO links [2]. Recently, satellite-based QKD has attracted much attention from industry and academia as a feasible method to establish a global-scale quantum-key distribution network. Such a network is also expected to serve wireless, and mobile users, including intelligent, self-driving vehicles and unmanned aerial vehicles (UAV) [3].

Satellite-based QKD can be implemented based on either a prepare-and-measure or entanglement-based scheme. In the former, the satellite plays a role of a trusted relay node for legitimate users [2]. The disadvantages of this scheme come from the complexity and inefficiency as we need more than one phase to distribute secret keys. The latter method is more efficient when the satellite acts as a central source and sends two beams of entangled quantum states to legitimate users simultaneously [4]. In addition, based on how quantum states are represented, QKD systems can also be categorized into discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). Entangled photon pairs are sent from the satellite to legitimate users in entanglement-based DV-QKD. Then, independent measurements on received photons are performed using single-photon detectors. In entanglement-based CV-QKD, the satellite generates and sends a two-mode entangled state to Alice and Bob, and coherent detection receivers can be used. From a practical perspective, CV-QKD is more convenient to implement as it is compatible with standard optical communication technologies. Nevertheless, the requirement of a sophisticated phase-stabilized local light for coherent detection in CV-QKD results in a high cost [5].

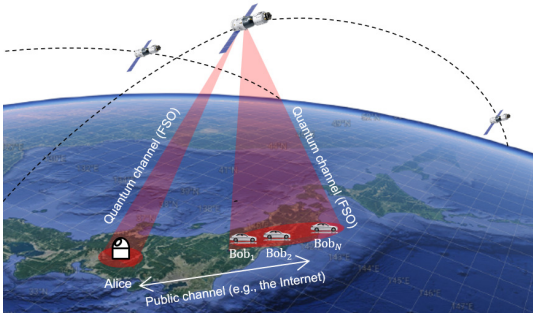

Fig. 1 Satellite-based QKD system for multiple users.

In order to simplify the system implementation further and reduce the cost, CV-QKD systems using a dual-threshold/direct detection (DT/DD) receiver have been proposed for the prepare-and-measure scheme in optical fiber [6] and optical wireless [7], respectively. As for the entanglement-based scheme, the satellite-based FSO CV-QKD system using the BBM92 protocol has also been recently proposed [8]. In that work and all previous ones, secret key distribution between only one pair of legitimate users (Alice and Bob) was considered. Practically, satellite-based QKD systems are, however, expected to support multiple users; therefore, in this paper, we propose an implementation to support multiple users in the satellite-based FSO CV-QKD system using non-coherent detection. We confirm the effectiveness of the proposed implementation by evaluating its total key rate.

2. Proposed Method, Model and Analysis

2.1 Proposed Method

Figure 1 shows the proposed CV-QKD system model with multiple users, in which a satellite (Charlie) distributes

[†]The author is with Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu, Japan.
a) E-mail: pham@u-aizu.ac.jp

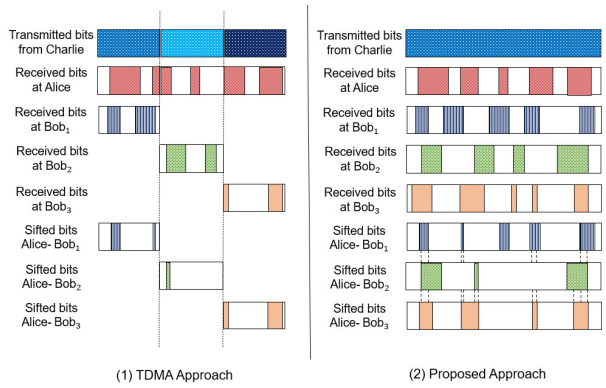

Fig. 2 TDMA vs. the proposed method for key distribution with $N = 3$.

secret keys to legitimate receivers, i.e., Alice and Bob$_i$, $i \in \{1, 2 \dots N\}$, via FSO channels using the BBM92 protocol. Alice plays the role of a server that performs post-processing procedures over the public channel with each user Bob$_i$ at Bob's side to create secret keys between Alice and each user Bob$_i$. For the sake of simplicity, the perfect pre-synchronization between Charlie, Alice, and Bob$_i$, which can be realized using GPS during the preparation stage, is assumed. The detail of the BBM92 protocol using DT/DD was given in [8]. To transmit the signal to multiple users at Bob's side, we consider two approaches that Charlie can use.

- Time Division Multiplexing Access (TDMA) Method: In this method, besides transmitting the signal to Alice, Charlie transmits the signal to each user Bob$_i$ within specified time slots. Alice and each user Bob$_i$ receive independent binary bit sequences from Charlie.
- Proposed Method: In our proposed system, Charlie sends all bit sequences to Alice and users Bob$_i$ at Bob's side. There are probabilities that users Bob$_j$, $j \neq i$, $j \in \{1, 2, \dots, N\}$ also have the received bit information of Bob$_i$. Alice and Bob$_i$ then could exclude the knowledge of their received bit information from other users Bob$_j$ to create their own secret keys.

Figure 2 illustrates the two methods for Charlie to transmit the signal to multiple users at Bob's side. The colored parts[†] of the received bits at Alice and Bob$_i$ denote the instants that Alice and Bob$_i$ decoded bits. Otherwise, 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.

2.2 Channel Model

The channel state $h_U, U \in \{A, B_i\}$ is formulated as $h_U = h_g^U h_l^U h_a^U$, where h_g^U is the geometric spreading loss, h_l^U is the atmospheric attenuation, and h_a^U is the atmospheric turbulence-induced fading. The details of each factor are given in [8].

[†]This figure is for illustrative purposes only. Practically, the Prob. of received/shift bit is much lower (about 10^{-3}) [8].

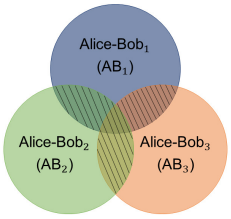

Fig. 3 Visualization for the relationship of sift probabilities between Alice and Bob$_i$, $i \in \{1, 2, 3\}$. The overlapping region is marked by diagonal stripes. This region shows the probabilities that Alice, Bob$_i$, and Bob$_j$, $j \neq i$, $j \in \{1, 2, 3\}$ can decode bits at the same time.

2.3 Performance Analysis

2.3.1 TDMA system

In the TDMA system, the sift probability is defined as the probability that both Alice and Bob$_i$ can decode the signal from Charlie. This probability for user Bob$_i$ is derived through the joint probabilities as

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

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" [8].

2.3.2 Proposed system

In the proposed system, Charlie sends all bit sequences to Alice and all users Bob$_i$ at Bob's side. In addition to the probability that both Alice and Bob$_i$ can decode bits using the DT threshold, there are probabilities that both Alice and Bob$_j$ can decode bits at the same time instants as both Alice and Bob$_i$. These probabilities are called *mutual sift probabilities*. The relationship of these probabilities can be visualized graphically using a Venn diagram for three users as in Fig. 3. Alice-Bob$_i$ (AB_i) is the sifting event that both Alice and user Bob$_i$ can decode bits using the DT threshold. The *overlapping region* of two sets AB_i and AB_j is the set of all decoded bits at the same time instants that belong to both AB_i and AB_j, and is denoted by $AB_i \cap AB_j$. Generally, the overlapping region of N sets AB_i is denoted as $\bigcap_{i=1}^{N} AB_i$. The probability of AB_i ($P(AB_i)$) actually is the sift probability between Alice and Bob$_i$, which is calculated as Eq. 1. To create independent secret keys with other users Bob$_j$, Alice and Bob$_i$ need to exclude the mutual sifting key information with other users (i.e., the overlapping region). Therefore, the sift probability between Alice and Bob$_i$ in the proposed system is determined as follows

$$P_{AB_i}^{\text{sift-excl}} = P(AB_i) - \varepsilon P(AB_i)_{\text{excl}}, \quad (2)$$

where $P(AB_i)_{\text{excl}}$ is the mutual sift probability with other

users Bob_j (i.e. the diagonal striped part in $P(AB_i)$), and ε is the exclusion ratio coefficient. $P(AB_i)_{\text{excl}}$ can be calculated as

$$P(AB_i)_{\text{excl}} = \sum_{j\neq i, 1\leq j\leq n} P(AB_i \cap AB_j) \quad (3)$$
$$+ \sum_{j_1\neq j_2\neq i, 1\leq j_1\leq j_2\leq n} P(AB_i \cap AB_{j_1} \cap AB_{j_2}) + \ldots + (-1)^{N+1} P(\bigcap_{i=1}^{N} AB_i),$$

where $P(AB_i \cap AB_j)$ is denoted for the mutual sift probability between two pairs. The first pair is Alice and Bob_i. The second pair is Alice and Bob_j. This mutual sift probability $P(AB_i \cap AB_j)$ is expressed as follows

$$\begin{aligned} P(AB_i \cap AB_j) = & P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(0,0,1) \quad (4) \\ & + P_{AB_iB_j}(0,1,0) + P_{AB_iB_j}(0,1,1) + P_{AB_iB_j}(1,0,0) \\ & + P_{AB_iB_j}(1,0,1) + P_{AB_iB_j}(1,1,0) + P_{AB_iB_j}(1,1,1), \end{aligned}$$

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

$$\begin{aligned} P_{AB_iB_j}(x,y,z) = & P_C(x) P_{A|C}(x|x) P_{B_i|C}(y|x) P_{B_j|C}(z|x) \\ & + P_C(y) P_{A|C}(x|y) P_{B_i|C}(y|y) P_{B_j|C}(z|y). \quad (5) \end{aligned}$$

We assume that the probabilities of transmitting bit "0" and bit "1" are equally likely to occur. Hence, $P_C(0) = P_C(1) = 1/2$. DT threshold is set so that the error conditional probabilities $P_{A|C}(y|x)$, $P_{B_i|C}(y|x)$, and $P_{B_j|C}(y|x)$, $x \neq y, x, y \in \{0,1\}$ is 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, Eq. (4) can be rewritten as

$$\begin{aligned} P(AB_i \cap AB_j) &\approx P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(1,1,1) \quad (6) \\ &= P_{A|C}(0|0) \left[P_{B_i|C}(0|0)\right]^2. \end{aligned}$$

From Eq. (6), we can simplify Eq. (3) as follows

$$P(AB_i)_{\text{excl}} \approx \sum_{k=0}^{N-2} (-1)^k C_{N-1}^{k+1} P_{A|C}(0|0) \left[P_{B_i|C}(0|0)\right]^{k+2}, \quad (7)$$

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.

By adjusting the permitted overlapped region ratio (r_o) in sift probabilities AB_i, the value of exclusion ratio coefficient ε can be derived as $\varepsilon = \frac{r_o P(AB_i) - P(AB_i)_{\text{excl}}}{r_o P(AB_i)_{\text{excl}} - P(AB_i)_{\text{excl}}}$.

2.3.3 Total final key-creation rate

We assume that there are two eavesdroppers (Eve_1 and Eve_2) who performs unauthorized receiver attacks near Alice's and Bob's sides, respectively. The distance from the beam footprint's center to eavesdroppers is approximately 25 meters. After sharing the sifted key between Alice and Bobs and performing error correction, Alice and Bobs estimate the information leaked to eavesdroppers and exclude it through privacy amplification to obtain the final key. 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, Bob and Eve_2, and Eve_1 and Eve_2, respectively. All of them can be determined by

$$I(Y;Z) = \sum_{y,z\in\{0,X,1\}} P_{YZ}(y,z) \log_2 \left[\frac{P_{YZ}(y,z)}{P_Y(y) P_Z(z)}\right], \quad (8)$$

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 approach, $P_{AB_i}(0,0)$ 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 approach, there is not any effect on $I(A;B_i)$.

The useful bit rate, namely *final key-creation rate*, after error correction and privacy amplification to exclude the amount of information leaked to Eve_1 and Eve_2 from that shared between Alice and user Bob_i at Bob's side, can be derived as

$$R_i^f = R_i^s \left[\alpha I(A;B_i) - \max(I(A;E_1), I(B_i;E_2), I(E_1;E_2))\right], \quad (9)$$

where R_i^s is the sifted-key rate, i.e., the length of the raw key that can be produced per unit time that contain the sifting factor. In case of the TDMA approach, $R_i^s = P_{AB_i}^{\text{sift}} \frac{R_b}{N}$. In case of the proposed approach, $R_i^s = P_{AB_i}^{\text{sift-excl}} R_b$. R_b is the system bit rate. α accounts for error correction efficiency in post-processing procedures. In this paper, we assume perfect error correction efficiency, i.e., $\alpha = 1$, as an upper bound evaluation of the system performance [6].

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

3. Results and discussions

This section investigates the performance of the proposed system with multiple users in terms of total final key-creation rates. We compare the proposed multiple access method with the TDMA one using the configuration data of the well-known Starlink satellite constellation. We assume that Alice is in Aizuwakamatsu (longitude: 139.9390°E, latitude: 37.5227°N; elevation: 209.093 m). Bobs are in Tokyo area (longitude: 139.7676°E, latitude: 35.6812°N; elevation: 5.4864 m). The elapsed time is set to 0 when Charlie starts seeing Alice and Bobs when the elevation angle is greater than the minimum acceptable elevation angle, which is 30°. We observe the system during the duration of the

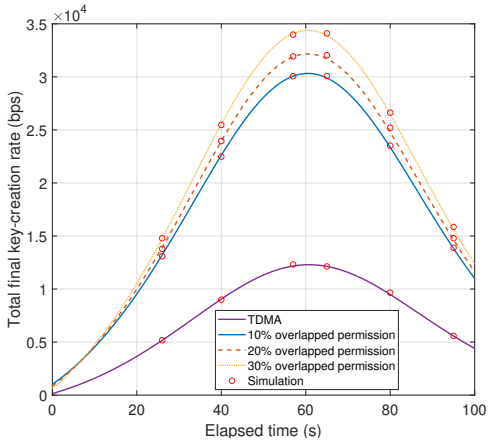

Fig. 4 Total final key-creation rate vs. the elapsed time with $N = 3$: Proposed system vs. TDMA

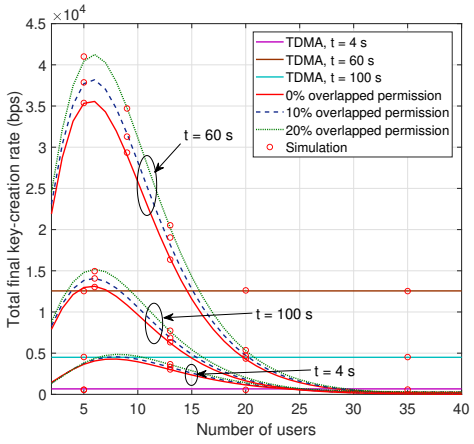

Fig. 5 Total final key-creation rate vs. the number of users (N): Proposed system vs. TDMA

satellite pass from Aizuwakamatsu to Tokyo. Simulated results were also given to confirm the accuracy of the theoretical analysis. Based on [8], we set three important parameters in satellite-based QKD systems using the BBM92 protocol: $\delta = 0.62$, $\varsigma_A = 3$, and $\varsigma_{B_i} = 0.9$. This guarantees that eavesdroppers' error probabilities are sufficiently high and that all users receive sufficient key information with an acceptable error rate.

Figure 4 shows the total final key-creation rates (R^f_{total}) versus the elapsed time of the considered satellite pass in the TDMA and proposed methods. The number of users is $N = 3$. It is observed that R^f_{total} in the TDMA system is lower nearly three times in comparison with the proposed one. The total final key-creation rates in the proposed system depend on the overlapped permission percentage in sift probabilities between Alice and Bob$_i$ (i.e., r_o%). If we allow a large percentage of overlapping region, we can increase R^f_{total}. For example, at $t = 60s$, $R^f_{\text{total}} = 34.372$ kbps if 30% overlapping region is permitted. R^f_{total} is decreased 30.322 kbps if only 10% overlapping region is permitted. However, the knowledge of key information among users is also increased if a large percentage of overlapping region is permitted. It can impair the security of the considered system.

Figure 5 illustrates the total final key-creation rates (R^f_{total}) versus the number of users N at three time instants $t = 4$s, 60s, and 100s. These time instants are the time at the beginning of the satellite pass, the time that the maximum sift probability can be achieved, and the time at the end of the satellite pass, respectively. In the TDMA system, R^f_{total} keeps constant values when the number of users increases. In the proposed system, similarly to the previous figure, it is observed that R^f_{total} also depends on the overlapped permission percentage in sift probabilities between Alice and Bob$_i$. In addition, it is possible to determine the optimum number of users that the considered system can support by observing the values of R^f_{total}. For example, at $t = 60$ s, R^f_{total} is maximum when the number of users is 6. If we continue to increase the number of users Bob$_i$, R^f_{total} is decreased. R^f_{total} can be even smaller than the value of R^f_{total} in TDMA system if the number of users are greater than 14. When the number of users increases to 30, R^f_{total} begins to asymptote to the value of 0.

4. Conclusion

This paper proposes satellite-based CV-QKD using DT/DD and the BBM92 protocol to distribute secret keys for multiple users. We analyzed the system performance regarding sift probability and total final-key creation rates for legitimate users. The numerical results are given under the effects of channel loss, atmospheric turbulence-induced fading, and receiver noises. Furthermore, the correctness of derived formulas was verified by Monte-Carlo simulations.

References

[1] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," *Archives of Computational Methods in Engineering,* vol. 28, pp. 3831–3868, Apr. 2021.

[2] Y. Cao *et al.,* "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 2, pp. 839–894, 2022.

[3] S. Khatri *et al.,* "Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet," *npj Quantum Inf,* vol. 7, no. 4, 2021.

[4] J. S. Sidhu *et al.,* "Advances in space quantum communications," *IET Quantum Communication,* vol. 2, no. 4, pp. 182–217, 2021.

[5] T. Hirano *et al.,* "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A,* vol. 68, Oct. 2003, Art. no. 042331.

[6] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise," *New Journal of Physics,* vol. 18, no. 1, Jan. 2016, Art. no. 013018.

[7] P.V. Trinh *et al.,* "Design and Security Analysis of Quantum Key Distribution Protocol over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver," *IEEE Access,* vol. 6, pp. 4159-4175, Jan. 2018.

[8] M.Q. Vu *et al.,* "Entanglement-based satellite fso/qkd system using dual-threshold/direct detection," *Proc. of the IEEE ICC 2022*, Seoul, South Korea, pp. 3245-3250.