A DISSERTATION

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

IN COMPUTER SCIENCE AND ENGINEERING

Research on Satellite-Based Free-Space Optical Quantum Key Distribution Systems for Multiple Wireless Users

by

Vu Quang Minh

Email: d8222112@u-aizu.ac.jp

August 2023

Email: d8222112@u-aizu.ac.jp, August 2023

The dissertation titled

Research on Satellite-Based Free-Space Optical Quantum Key Distribution Systems for Multiple Wireless Users

by

Vu Quang Minh
Email: d8222112@u-aizu.ac.jp

is reviewed and approved by:

Chief referee	
Professor	Date
PHAM Tuan Anh Pham T. Anh	2023/08/10
Professor	Date
NAKAMURA Akihito A. Nak	Aug. 7, 2023
Senior Associate Professor	Date
LI Peng Peng Li	Aug. 8, 2023
Senior Associate Professor	Date
LU Guo-Wei	2023-7-25

THE UNIVERSITY OF AIZU

August 2023

Contents

List of Figures

List of Tables

List of Abbreviations

BPSK	Binary Phase-Shift Keying
CSI	Channel-State Information
CV	continuous-variable
CV-QKD	continuous-variable QKD
DD	direct detection
DT	dual-threshold
DV	discrete-variable
DV-QKD	discrete-variable QKD
EB	entanglement-based
ETSI	European Telecommunication Standards Institute
FSO	Free-Space Optics
GEO	geostationary orbit
IOS	International Organization for Standardization
ITU	International Telecommunication Union
LEO	Low-Earth orbit
M-C	Monte Carlo
NORAD	North American Aerospace Defense Command
OOK	On-Off Keying
PM	prepare-and-measure
QKD	Quantum Key Distribution
SIM	Subcarrier Intensity Modulation
SPDC	spontaneous parametric down-conversion

List of Symbols

A_c	The subcarrier signal
a_U	The aperture radius at user U
d_0^U	The detection threshold to detect bit "0"
d_1^U	The detection threshold to detect bit "1"
d_t^E	The optimal threshold of eavesdropper
δ	The intensity modulation depth
F_n	The amplifier noise figure
$g(t)$	The pulse shaping function
h_{e2e}^U	The channel state between Charlie and user U
h_{e2e}^U	The channel state between the satellite and the user U
h_g^U	The geometric spreading loss
h_l^U	The atmospheric attenuation
h_a^U	The atmospheric turbulence-induced fading
h_g^U	The fraction of power collected by each user's receiver
H_U	The altitude of user U
H_C	The altitude of satellite (Charlie)
i_r^U	The detected value of the received current signal at user U
k_B	The Boltzmann's constant
λ	The operating wavelength
L_{C-U}	The distance between Charlie to user U
$m(t)$	The subcarrier signal
Ω_r	The Sun's spectral irradiance from above Earth
P_{error}^E	The probability that Eve falsely detects Charlie's transmitted bits
$q(V)$	The atmospheric attenuation visibility coefficient
R_e	The responsivity of the photodetector
R_b	The system bit rate
R_L	The load resistance
$\boldsymbol{\rho}$	The radial vector from the beam footprint center
θ_C	The divergence angle of the transmitted beam
n_{e2e}^U	The receiver noise
σ_N^U	The standard deviation of the received noise at user U
T	The receiver temperature in Kelvin degree
U	User $U \in A, B$
V	The atmospheric visibility
ξ	The attenuation coefficient
ζ_U	The zenith angle between the transmitted beam to user U and the vertical direction

Acknowledgment

First and foremost, I would like to take this opportunity to express my deep gratitude to my supervisor, Prof. PHAM Tuan Anh, for his continuous support, guidance, and encouragement. I have had a great opportunity to work with him and have learned a lot from him throughout my five years in Master's and Doctoral programs at the University of Aizu. In addition, I would like to thank Dr. LE Doan Hoang for co-supervising me during my Doctoral program.

I would like to send my special appreciation and thanks to my Doctoral Dissertation Review Committee, Prof. NAKAMURA Akihito, Prof. LI Peng, and Prof. LU Guo-Wei, for taking the time out of their busy schedule to review my dissertation.

Thanks should also go to Prof. DANG The Ngoc and Prof. PHAM Thi Thuy Hien, professors at Posts and Telecommunications Institute of Technology-my undergraduate university. They always believe in me, give me helpful advice, and encourage me.

Thanks to my lab mates for their help and support over five years. I had many wonderful and memorable experiences with them in traveling, running, and skiing.

I gratefully acknowledge the financial support from the Japanese Government through Monbu Kagaku-sho (MEXT) scholarship during my graduate studies at the University of Aizu. My thanks also go to all staff at the University of Aizu, especially in Student Affairs Division, Administrative Liaison Office, and General Affairs and Budget Division. With their help, my paperwork as an international student became easier and more relaxed. I would like to thank the IEEE Communication Society, NEC C&C Foundation, and AIZU ZAIDAN for their travel grants to allow me to attend international conferences.

Last but not least, I am deeply indebted to my family. Whenever I have trouble, I always find them and receive their encouragement. They help me get out of the most challenging times. I cannot thank them enough.

Abstract

With the recent development of the Internet of Things (IoT), security has become crucial because much personal information is being stored and shared on a broad scale. One of the central issues in the network security provision is how legitimate parties can share secret keys in advance in a secure manner. Nowadays, public-key cryptography has been primarily used for the key distribution system (KDS). Nevertheless, as the security of public-key cryptography relies on mathematical complexities and assumptions about the computing power of a possible eavesdropper, it becomes vulnerable due to the discovery of new computational technologies, especially the recent advancement in quantum computing and artificial intelligence.

QKD, a technology that is based on the fundamental laws of quantum physics, has recently emerged as one of the solutions for secure key distribution. QKD allows legitimate parties to share secret keys frequently and efficiently so that unconditional security can be achieved, which may revolutionize the protection way of information exchange in the future. In practice, the achievable distance for QKD over optical fibers and terrestrial FSO has been limited to a few hundred kilometers, especially for mobile users. Considering the future scenario where QKD would be implemented globally for a wide range of applications, satellite-based FSO/QKD becomes a viable solution for global security service.

Satellite-based FSO/QKD systems can be classified into two different schemes: prepare-and-measure (PM) or the EB scheme to distribute secret keys between two ground stations (Alice and Bob). In the PM scheme, the satellite establishes two 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. On the other hand, in the EB scheme, the trusted requirement of the satellite 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. The EB scheme is more suitable for implementing a global-scale QKD network.

From this perspective, this dissertation presents a new design concept for satellite-based FSO/QKD using EB scheme to provide a less complex and low-cost implementation. Firstly, I design the proposed satellite-based FSO/QKD systems for Low-Earth orbit (LEO) satellites and investigate the feasibility of a case study for the Japan QKD network using the existing Starlink LEO satellite constellation. The LEO satellite can benefit from the low channel loss; nevertheless, its coverage is limited. A promising solution is combining geostationary orbit (GEO) and LEO satellites for the global-scale QKD network. Therefore, secondly, I present a novel satellite-based FSO/QKD that uses LEO and GEO satellites. The proposed systems can support multiple mobile users. Then, based on the design criteria for the proposed system, the feasibility of a case study for Japan QKD network using the existing GEO satellite and LEO satellite constellation to provide QKD service for legitimate users in Japan. Moreover, the secret key performance of the proposed system is also given based on the design criteria of transmitters and receivers. Monte Carlo (M-C) simulations are performed to verify analytical results.

Chapter 1

Introduction

1.1 Motivation of Study

QKD is a cryptographic method for establishing secret keys between two parties for encryption. Today's interest in QKD arises primarily from rapid progress in quantum computing. The conventional secret key distribution systems are based on public-key cryptography, where key security is protected by the computational complexity of solving mathematical problems. The development of quantum computing would thus make deployed key distribution systems obsolete, potentially leading to a fatal breakdown of the current communication infrastructure [1]. Unlike public-key cryptography, QKD offers information-theoretic security guaranteed by quantum mechanics, i.e., the secret key generated from a QKD protocol will remain secure even if an adversary has unlimited computing power. Thanks to QKD's characteristics, QKD has rapidly matured into a commercial technology since the first proposal emerged in 1984 by Bennett and Brassard [2]. Many commercial offerings are now available from worldwide vendors, such as Quintessence Labs, Qasky Quantum Science Technology, and ID Quantique [3]. The potential applications of QKD include securing critical infrastructures, financial institutions, and national defense.

While QKD has achieved remarkable progress in the optical fibers [4–8], and terrestrial FSO systems [9–16], satellite-based FSO/QKD systems, which is a possible solution to increase the range of QKD for a successful global-scale quantum network for both fixed and mobile users (e.g., autonomous vehicles, unmanned aerial vehicles), has attracted much recent research effort [17–25]. A milestone was reached in 2017 with the first complete satellite-to-ground QKD implementations realized with the Chinese satellite Micius- the world's first quantum communication satellite [1]. Later the same year, satellite-based FSO/QKD systems were also implemented by a payload on board the Tiangong-2 space laboratory [26]. After that, the Micius satellite was used to generate the cryptographic key for the stations in Vienna and Beijing in the first intercontinental quantum-secured communication, thus opening the era of satellite-based FSO/QKD [27].

LEO satellites have been mostly used to implement satellite-based FSO/QKD [1] due to their benefit from the low channel loss. Nonetheless, its coverage is limited [28]. The coverage can be extended by multiple LEOs organized into a constellation. However, the key relaying/routing in the network among LEO satellites would bring new security concerns. While a GEO satellite situated at 35,786 km in altitude can solve the coverage problem, the system suffers from a high path loss and limited key rates. Therefore, combining GEO and LEO satellites is an attractive research direction for implementing global-scale QKD networks.

Satellite-based FSO/QKD systems can be operated in two schemes: PM and EB schemes. In the PM scheme, quantum states are sent between a satellite and a ground station. The satellite, which acts as a single trusted node, establishes a secret key between the satellite itself and Alice (the first ground station) and, afterwards, a second key between itself and Bob (the second

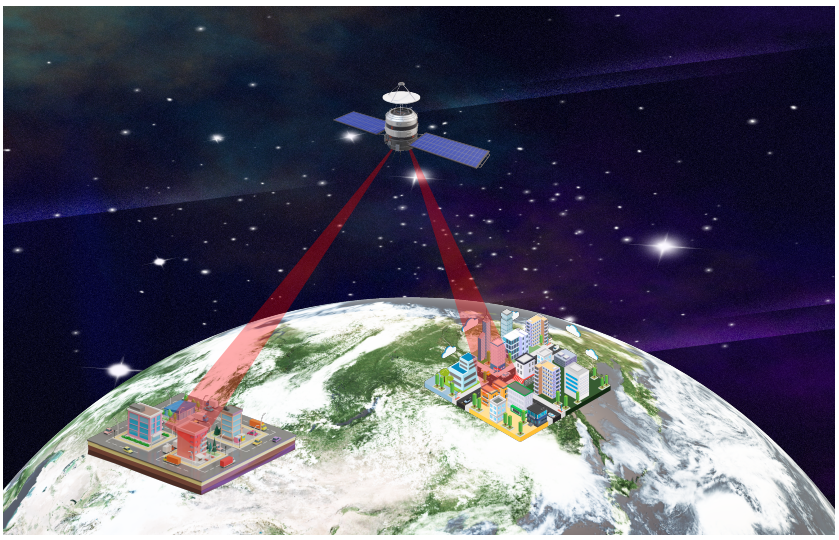


Figure 1.1: Satellite-based FSO/QKD could enable a global-scale QKD network.

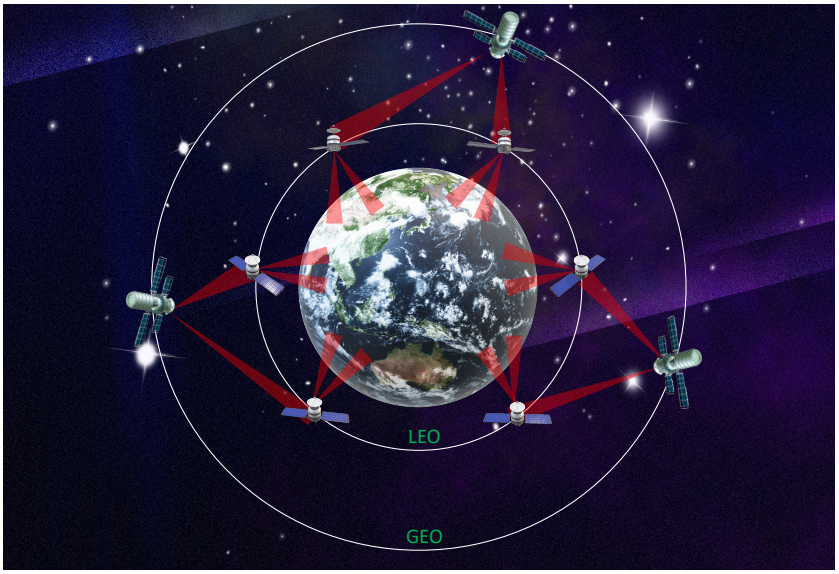


Figure 1.2: A global-scale QKD network using LEO satellite constellation and GEO satellites.

ground station). Then, the satellite combines these two secret keys with a mathematical operation and sends them to Alice and Bob [29]. The EB scheme differs from the PM scheme by relaxing the trusted requirement and processing payload from the satellite. In the EB scheme, Alice and Bob will simultaneously receive quantum states sent by satellite. Without the involvement of the satellite, Alice and Bob can then agree on the final secret keys [19]. This EB scheme is more suitable for implementing a global-scale QKD network.

In the EB scheme, depending on how quantum states are represented, there are two main approaches to implementing QKD systems: discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). Entangled photon pairs are sent from the satellite to Alice and Bob in entanglement-based DV-QKD. Alice and Bob then independently measure the received photons using single-photon detectors [27, 30]. The deployment of DV-QKD systems is, nevertheless, limited by the difficulty in generating entangled photon pairs and the expense of single-photon detectors [31]. In addition, DV-QKD is also incompatible with standard optical communication technology [32]. Compared to DV-QKD, CV-QKD is easier in terms of implementation as it is compatible with the standard optical communication technology [33]. In the EB CV-QKD, the

satellite generates a two-mode entangled state and sends it to Alice and Bob. These legitimate users then use coherent detectors, which operate faster and more efficiently than single-photon detectors [31, 34]. However, the weakness of CV-QKD is the requirement for a sophisticated phase-stabilized local light for coherent detection. It leads to a high cost for deploying CV-QKD systems [35].

In this dissertation, to provide a simplicity and cost-effective implementation for satellite-based FSO/QKD systems using the EB scheme, we consider non-coherent CV-QKD by employing dual-threshold (DT)/direct detection (DD) at receivers without the phase-stabilized local light or expensive single-photon detector. In addition, instead of only support for two legitimate users, we also focus on designing a system that can support multiple users. This implementation could join hands to enable the global coverage of QKD networks.

1.2 Contributions

The primary focus of this dissertation is the design, modeling, and performance analysis in terms of secret-key rates of the simplicity and cost-effectiveness implementation for satellite-based FSO/QKD systems. The major contributions of the dissertation are summarized as follows

1. *Firstly*, we propose a new design concept of satellite-based FSO/QKD systems by applying non-coherent detection for the EB scheme based on the BBM92 protocol [36]. This conventional protocol is the most popular EB DV-QKD protocol, also used in the Micius satellite to provide secret keys for ground stations [30]. Our proposed concept provides a less complex and low-cost implementation of the BBM92 protocol for EB satellite QKD systems by applying non-coherent CV-QKD. In the system model and analysis, the atmospheric channel between satellite and legitimate users is characterized by considering the geometric spreading loss, atmospheric attenuation, and atmospheric turbulence-induced fading.

2. *Secondly*, to solve the limited coverage problem of FSO/QKD systems using LEO satellites, we provide a novel FSO/QKD system that uses LEO and GEO satellites. We also focus on designing a system that can support multiple mobile users, which opens the potential to establish a global-scale QKD network.

3. *Finally*, based on the design criteria for the proposed satellite-based FSO/QKD systems, we investigate the feasibility of a case study for Japan's QKD network using the existing GEO satellite and LEO satellite constellation to provide QKD service for legitimate users in Japan. Moreover, the secret-key performance of the proposed systems is also given based on the design criteria of transmitters and receivers. M-C simulations are performed to verify analytical results.

1.3 Dissertation Organization

The remainder of the dissertation is organized as follows.

Chapter 2 provides the relevant background of the study. In particular, the motivation for QKD, QKD implementation, prominent QKD protocols, and satellite-based FSO/QKD are introduced. Recent developments of satellite-based FSO/QKD and opening issues are also presented.

Chapter 3, chapter 4, and chapter 5 focus on ***key contributions*** of this dissertation:

1. In chapter 3, a new implementation for satellite-based FSO/QKD systems using non-coherent CV-QKD protocol inspired by the BBM92 protocol for EB scheme is proposed.

This implementation is less complex and possibly cheaper than current DV-QKD and CV-QKD ones. The performance of the proposed system is modeled and analyzed in the context that a satellite distributes secret keys to two legitimate users. The content of this chapter was presented in part in

(a) Minh Q. Vu *et al.*, "Entanglement-based satellite FSO/QKD system using dual-threshold/direct detection," *ICC 2022 - IEEE International Conference on Communications,* Seoul, pp. 3245-3250, May 2022.

(b) Minh Q. Vu *et al.*, "Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/ direct detection," in *IEEE Access,* vol. 10, pp. 113260-113274, Oct. 2022.

2. Chapter 4 proposes designing a global-scale satellite-based FSO/QKD system using a GEO satellite as a secret key source and LEO satellites as trusted relay nodes to amplify and forward the signal from the source to multiple legitimate users on earth. The non-coherent CV-QKD protocol with DT/DD receivers inspired by the BBM92 protocol for EB scheme is employed. The content of this chapter was presented in part in

   (a) Minh Q. Vu *et al.*,"A Proposal of satellite-based FSO/QKD system for multiple wireless users," *IEICE International Conference on Emerging Technologies for Communications (ICETC),* Waseda, Japan, Nov. 2022.

   (b) Minh Q. Vu *et al.*,"Design of satellite-based FSO/QKD systems using GEO/LEOs for multiple wireless users," in *IEEE Photonics Journal,* vol. 15, no. 4, pp. 1-14, Aug. 2023, Art no. 7303314.

3. In the approach of the satellite-based FSO/QKD system in chapter 4, the eavesdropper may possess valuable information about the secret keys by analyzing received signals from satellites in the EB scheme. A feasible approach is using a network coding-aided hybrid EB/PM scheme, which can reduce the transmission phases (in the PM scheme) and prevent to leak the useful information about the secret keys to potential eavesdroppers (in the EB scheme). Chapter 5 presents this approach by implementing CV-QKD protocol with DT/DD receivers inspired by the BBM92 protocol for EB scheme to distribute shared secret keys to multiple users located in distant locations. The content of this chapter was presented in part in

   (a) Minh Q. Vu *et al.*,"Network coding aided hybrid EB/PM satellite-based FSO/QKD systems," *2023 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC),* Jeju, Jun. 2023.

   (b) Minh Q. Vu *et al.*,"Satellite-based quantum key distribution: hybrid EB/PM scheme-assisted multiple users," *Under Review.*

4. In all three chapters, the system performance is analyzed, 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 using the existing GEO and LEO satellite constellation. In addition, the secret-key rate performance of the proposed system is investigated, and M-C simulations are performed to verify analytical results.

Finally, chapter 6 concludes the dissertation with a summary and outlook on future research directions.

Chapter 2

Background of Study

2.1 Introduction of Quantum Key Distribution

2.1.1 Motivation of Quantum Key Distribution

Cryptography is the art of enabling confidentiality, integrity, and authentication to legitimate parties. Cryptography has been used for thousands of years to protect secret information against changing, stealing, and unauthorized access by adversaries. Nowadays, cryptography is of the utmost importance when our sensitive personal financial and health data and commercial and national secrets are frequently transmitted through the Internet with the rise of recent trends in the Internet of Things.

There are two kinds of cryptography: symmetric and asymmetric (public key). In symmetric cryptography, both the sender and receiver must use the same secret key for encryption and decryption. Generally, symmetric cryptography is widely used thanks to its simplicity and efficiency. The central question is how the sender (Alice) and the receiver (Bob) share a secret key in advance. It is called the key distribution problem, which is the major difficulty of symmetric cryptography. With the development of the Internet with its billions of users, distributing secret keys has become much more difficult and impractical.

Public-key cryptography, which uses two different keys for encryption and decryption, offers a solution to deal with this key distribution problem. Suppose Alice wishes to send Bob a secret key using public-key cryptography. Bob must generate two cryptographic keys, one a public key and the other a private one. Once Bob has generated his keys, he publishes the public key so that anybody can access the key and keeps the private key secretly. Alice then obtains Bob's public key and encrypts the secret key she wishes to send Bob, using Bob's public key to perform the encryption. Since the public key and the encoded message are the only information available to an eavesdropper, it will not be possible to recover the message.

On the other hand, Bob has additional information not available to an eavesdropper, the private key which helps Bob recover the secret key sent by Alice. The security of public key cryptography relies on unproven mathematical assumptions about the difficulty of solving factoring extremely large numbers. With current computing power, the adversaries can only extract the key in a feasible amount of time. However, with the discovery of new computational technologies, especially the recent advancement in quantum computing and Artificial Intelligence (AI), the security of public-key cryptography becomes susceptible. In particular, when an n-qubit quantum computer can be realized, it would bring as much as 2^n computational power potential compared to the binary-bit computers. A possible exponential increase in computational power, together with the huge potential of AI, would critically menace the integrity of public-key cryptography.

Quantum key distribution (QKD), a key agreement protocol based on the law of physics, is considered a promising method to distribute secret keys securely and overcome the possibility

of efficient quantum computers. The quantum no-cloning theorem implies that an unknown quantum state cannot be cloned reliably [37]. If Alice distributes a key via quantum signal, there is no way for the eavesdropper (Eve) to clone the quantum state reliably to make two copies of the same quantum state. If Eve tries to eavesdrop in QKD, she will unavoidably introduce disturbance to the quantum signals. Alice and Bob will then detect this disturbance. They can discard such a key and try the key distribution process again. An important advantage of QKD is that Eve has no classical transcript to keep once a QKD session is over since the communication is quantum. Therefore, Eve must break a QKD session in real time, or it will be secure forever. It is different from conventional key distribution schemes. QKD promises unconditional security [38–40], i.e., guaranteeing security without imposing any restriction on the power of eavesdroppers.

2.1.2 History of Quantum Key Distribution

Based on earlier ideas by Wiesner [41], the first complete QKD protocol using polarized photons was proposed by C. H. Bennett and G. Brassard in 1984. This protocol is called BB84, after the initials of the two inventors and the year [2]. In this protocol, the uncertainty principle of quantum mechanics plays an essential role. The key information is encoded into states of a single photon. Shortly afterward, there were two additional milestones in 1992. The first one is the invention of the BBM92 protocol using entangled photon pairs was proposed by Bennett, Brassard, and Mermin in 1992 [36]. The second one is the very first in-principle experimental demonstration [42]. Besides these protocols making use of polarized photons (i.e., discrete-variable QKD), a new family protocol in which the key information is encoded in the continuous quantum variables conveyed by the amplitude and phase of weakly modulated light pulses was proposed in the 2000s [43]- [46]. This family protocol is called continuous-variable QKD.

After these foundation works, the concept and feasibility of QKD attracted a great deal of interest from academia and industry. Improved from the first experimental demonstration, QKD had been implemented successfully in both wired, i.e., optical fiber [47]- [49], and wireless, i.e., free-space optical (FSO) communication links [9]- [13]. These implementations demonstrated that QKD could be sufficiently robust for real-world implementation. Recently, the distance of the QKD-based optical fiber system has been pushed to 500 km using ultra-low loss fiber [50, 51]. QKD-based FSO system also archives a recent landmark accomplishment of quantum satellite QKD experiment in 2017 over 1200 km by China [26] and 7600 km between China and Austria [27]. In Europe and many other countries, such as the U.S., Canada, Japan, and Singapore, there are ongoing satellite-based quantum communications efforts [52]- [55]. Commercial QKD systems are currently available on the market by several companies which pioneered this field, e.g., ID Quantique of Switzerland, BBN Technology of the U.S., MagiQ of the U.S., and Toshiba Corporation of Japan. Several institutes, such as European Telecommunication Standards Institute (ETSI), International Organization for Standardization (IOS), and International Telecommunication Union (ITU), have made significant attempts to address the standardization issues in QKD.

QKD has been used for many real-life applications. In 2007, QKD protected a Swiss election against hacking and accidental data corruption [56]. In 2010, a critical communications link was protected by QKD for the duration of the 2010 FIFA World Cup competition in Durban [57]. It was the first time using QKD at a world public event. In 2017, a QKD-protected video conference between China and Austria using the quantum satellite Micius as a trusted relay was held [27]. Shortly, QKD can be widely used to ensure long-term security for numerous users in the government, financial, and energy industries.

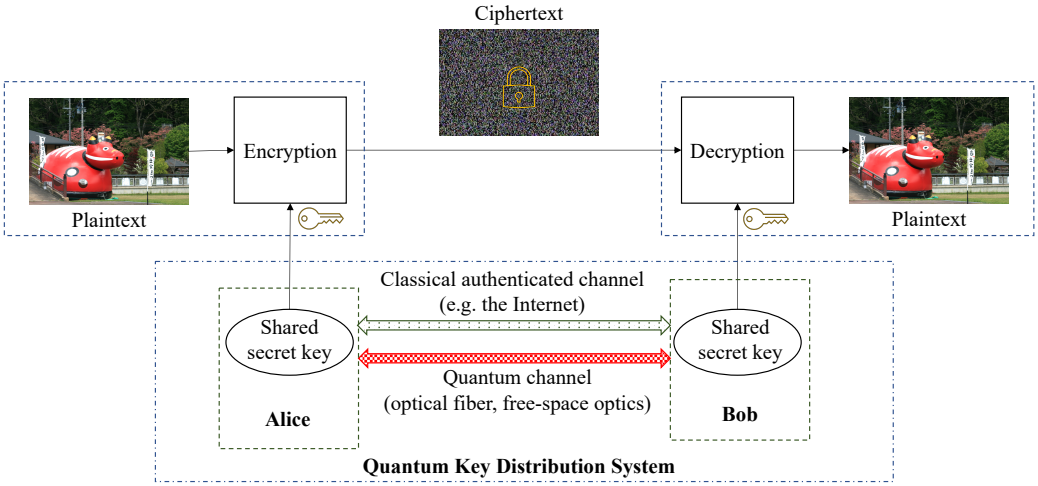


Figure 2.1: Generalization of the QKD system architecture.

2.1.3 Overview of Quantum Key Distribution Systems

QKD allows two legitimate parties (Alice and Bob) to share random and secret keys later used to encrypt and decrypt secret messages. The QKD system architecture generalization is shown in Fig. 2.1. Alice and Bob need to use two channels: the quantum channel and the classical channel. The quantum channel allows them to share the key information encoded by quantum signals. Otherwise, the classical channel is needed for the key sifting process and performing *information reconciliation* to correct erroneous bits in the shared key by error correction techniques and *privacy amplification* to produce a new shorter key based on hash functions in such a way that eavesdroppers have negligible information about the new key. Specifically, the general steps of a QKD protocol for distributing secret keys between two legitimate parties are summarized as follows

- Quantum state transmission and measurement: Alice and Bob use the quantum channel
  - *Step 1*: Alice encodes key information based on the uncertainty of quantum mechanics depending on a specific QKD protocol.
  - *Step 2*: Alice transmits encoded key bits to Bob over a quantum channel.
- Post-processing procedures: Alice and Bob use the classical channel
  - *Step 3*: The classical channel is authenticated. It means that Alice and Bob identify themselves. Bob discloses to Alice the time instants that he could detect the encoded key bits, forming their shared *raw keys*.
  - *Step 4*: Alice discloses to Bob her encoding schemes on the key bits he detected, forming their shared *sifted keys*.
  - *Step 5*: Alice and Bob public a random sample of their shared sifted keys and perform *information reconciliation*, which use error correction techniques to identify and remove erroneous bits.
  - *Step 6*: Alice and Bob perform *privacy information*, which uses hash functions to produce a new, shorter key so that Eve has only negligible information about their shared secret keys.

2.2 Quantum Key Distribution Implementation

2.2.1 Encoding-Decoding

Owing to how the key information is encoded in the properties of light and what corresponding detection techniques require, there exist two implementation methods of QKD protocols: discrete-variable (DV) and continuous-variable (CV).

2.2.1.1 Discrete-variable (DV)

DV-QKD is the earliest and simplest form of QKD. In DV-QKD, the key information is typically mapped to discrete features, such as the polarization of a single photon [2]. DV-QKD achieves unconditional security by employing the no-cloning theorem and theorem on the indistinguishability of arbitrary quantum states. The standard unit of DV-QKD is the quantum bit (often called a *qubit*). A classical bit is either 0 or 1. However, the situation is more complicated for a qubit. The qubit can be written as a linear combination (often called a linear superposition) of an orthonormal basis ($|b_0\rangle$, $|b_1\rangle$) as

$$|\psi\rangle = d_0|b_0\rangle + d_1|b_1\rangle, \tag{2.1}$$

where $|\psi\rangle$ is the standard quantum mechanical notation for a vector in a vector space. ψ is a label for the vector. The $|.\rangle$ notation indicates that the object is a vector. It is important to notice that to get information out of a qubit, we have to measure it. After we measure this qubit, its state will jump to either $|b_0\rangle$ or $|b_1\rangle$. Measurement of the qubit perturbs its coherent superposition. The probability of its state being $|b_0\rangle$ is $|d_0|^2$; the probability of $|b_1\rangle$ is $|d_1|^2$. Naturally, $|d_0|^2 + |d_1|^2 = 1$, since the probabilities must sum to one. Now, for example, we connect the classical bits 0 and 1 to the basis vectors. We associate the $|b_0\rangle$ vector with the state $|0\rangle$ and the $|b_1\rangle$ vector with the state $|1\rangle$. Two states $|0\rangle$ and $|1\rangle$ can correspond to the states 0 and 1 for a classical bit. When we measure the qubit, we obtain 0 with probability d_0^2 and 1 with probability d_1^2.

Let's consider an example of two legitimate parties exchanging a secret message using the discrete variable. The sender (Alice) wants to send a secret message to the receiver (Bob). Alice measures qubits using her orthonormal basis ($|a_0\rangle, |a_1\rangle$). Bob measures the qubits that Alice sends to him using his orthonormal basis ($|b_0\rangle, |b_1\rangle$). If Alice wants to send 0, she sends a qubit in state $|a_0\rangle$. After Bob receives this qubit, he measures it with respect to his ordered basis. To calculate what happens, $|a_0\rangle$ is written as a linear combination of Bob's basis vectors as

$$|a_0\rangle = d_0|b_0\rangle + d_1|b_1\rangle. \tag{2.2}$$

When Bob measures the qubit, its state jumps to state $|b_0\rangle$ with probability $|d_0|^2$, and he writes down 0, or its state jumps to state $|b_1\rangle$ with probability $|d_1|^2$, and he writes down 1. Bob would receive 0 with certainty whenever Alice sent 0 and 1 with certainty whenever Alice sent 1 only if Alice and Bob chose to use the same basis.

DV-QKD requires perfect single-photon sources which emit only one photon at a time. Because these sources are notably hard to build, they have been replaced by weak coherent-state sources, which can be realized easily by attenuating laser lights. The arriving photon pulses are processed at the receiver side by beam splitters or interferometers. After optical processing, the photons are detected by single-photon detectors. A single-photon detector is an optically-sensitive device that probabilistically transforms a single-photon into a macroscopically detectable signal. The main quantities characterizing single-photon detectors are the quantum efficiency which represents the probability of a detector clicking when a photon hits the detector, and the dark-count rate characterizing the noise of the detector. Dark counts occur when a detector sends an impulse even if no photon has entered it. The most commonly used single-photon

detectors in DV-QKD systems are avalanche photodiodes (APDs). Particularly, for wavelengths from approximately 400-1000 nm, Si APD can be used. For wavelengths from about 950 nm to 1650 nm, InGaAs/InP APD are most often applied [58].

2.2.1.2 Continuos-variable (CV)

As an alternative to DV-QKD, which is ideally based on a single-photon detection, CV-QKD encodes the key information onto the quadrature variables of a light field [59]. CV-QKD uses coherent detection techniques, such as homodyne or heterodyne detection, in which the received signal field is coupled to a local oscillator (LO) to determine the light's quadratures. CV-QKD's advantages over DV-QKD include a cost-effective detection technique instead of a dedicated single-photon-counting technique, its compatibility with off-the-self optical hardware [60], and high detection efficiency without the requirement of cooling as DV-QKD systems [61]. Depending on the modulation method of quantum states, CV-QKD has two main modulation approaches, including *Gaussian-modulation* approach and *discrete-modulation* approach.

The first *Gaussian-modulation* approach was based on squeezed states of light, which are modulated with a Gaussian distribution in the position p or the momentum q quadrature by Alice (in other words, the state of light is squeezed in either quadrature p or q). Bob randomly chooses either p or q of the modulated state to measure using the homodyne detector. A proposed QKD protocol based on this approach was given in [45]. Another CV-QKD protocol based on the Gaussian modulation of squeezed states of light was also proposed in [62]. The need for a source of squeezed light is the main drawback of this approach. Therefore, a second Gaussian QKD approach was discovered in which Alice generates coherent states of light, which are modulated with a Gaussian distribution in the quadrature p and q. At the same time, Bob still performs homodyne detection to measure randomly either p or q of the coherent state of light [46]. A first experiment was conducted with bulk optical elements on an optics table [63]. In this approach, Alice simply forgets the quadrature that Bob does not measure. Discarding half of her data may look like a loss of efficiency since some information is transmitted and then lost. A third approach was proposed, in which Alice still transmits coherent states of light, but Bob performs heterodyne detection instead of homodyne detection [64].

Using heterodyne detection, Bob simultaneously measures both p and q quadratures. Because Bob acquires a pair of quadrature p and q, this seems to imply that the rate is doubled at first sight. Since the measurement of heterodyne detection affects one additional unit of vacuum noise on the measured quadrature, the two quadratures measured by Bob are noisier than the single quadrature in the homodyne detection. Nevertheless, an improvement in key rate may be offered when the two quadratures are measured simultaneously. Moreover, an advantage of this heterodyne detection is that there is no need to choose a random quadrature to measure at Bob's side. The experiment of this approach was realized in [65]. A fourth Gaussian-modulation approach was introduced in [66]. Alice sends squeezed states again in this approach, as in the first approach, but Bob performs heterodyne measurements, as in the third approach. The fourth approach is associated with the highest rate and range. However, it requires a source of squeezed light.

Besides *Gaussian-modulation* approach, there exists a different kind of approach using *discrete-modulation*. *Discrete-modulation* approach is the first proposal of QKD using continuous-variable [43]. Alice first prepares a discrete number N of random coherent states in this approach. Then Bob uses either homodyne (or heterodyne) detection to measure the quadrature p or the quadrature q (or both p and q). This approach is more practical because a real Gaussian modulation can never be perfectly implemented, and this approach can simplify the crucial step of error correction. There are security proofs for this approach where N = 2, 3, 4 given in [67–69], respectively.

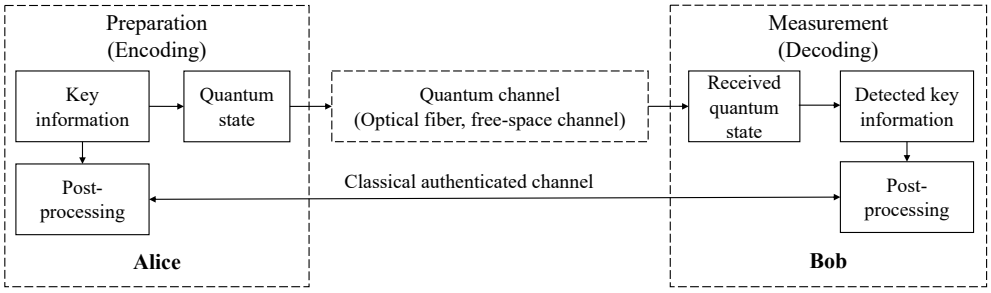


Figure 2.2: Schematic diagram of PM scheme.

2.2.2 Operating scheme

There are two types of operating schemes, namely PM and EB schemes [33]. A PM scheme is based on individual qubits (in case of DV-QKD) or CV quantum states (in case of CV-QKD), while an EB scheme is based on entangled qubits (in case of DV-QKD) and a two-mode entangled state (in case of CV-QKD). Both schemes can securely share secret keys between two legitimate parties. In the following, each scheme is briefly described.

2.2.2.1 Prepare-and-measure scheme

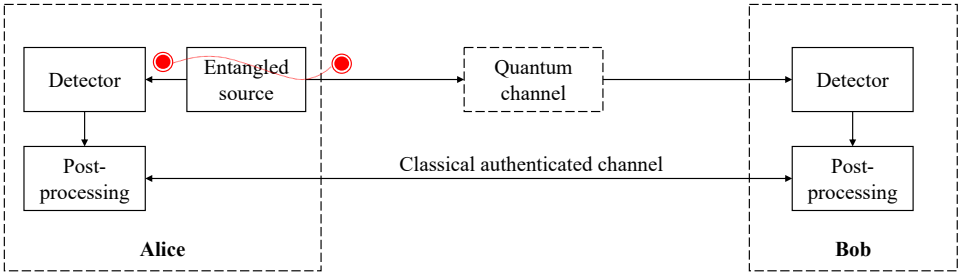
Alice prepares quantum states in a PM scheme and encodes the key information onto the quantum states. These quantum states are then sent to Bob over a quantum channel (optical fiber, free-space link). After receiving these quantum states, Bob measures them using single-photon detectors (in the case of DV-QKD) or homodyne (heterodyne) detectors (in the case of CV-QKD). A schematic diagram of the PM scheme is illustrated in Fig. 2.2. An example of QKD protocol that is based on DV-QKD and uses PM scheme is BB84 [2], while Gaussian-modulated coherent state (GMCS) protocol [46, 63] is a CV-QKD protocol using PM scheme.

2.2.2.2 Entanglement-based scheme

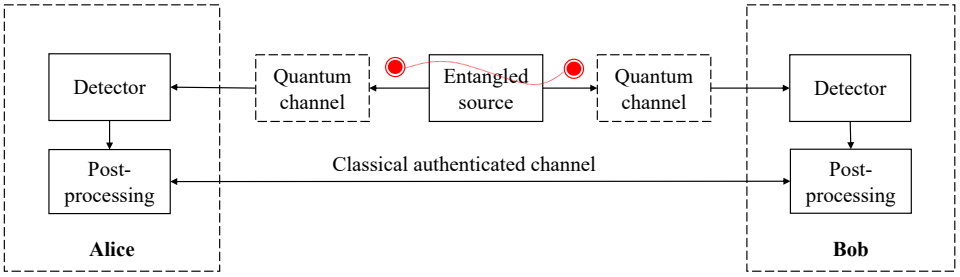
EB scheme focuses on quantum states in which two objects are linked together, forming a combined quantum state. The concept of entanglement means that the measurement of an object thereby affects the other. In EB scheme, there are two ways to implement which are illustrated in Fig.2.3. In the first way, Alice equips an entangled source that could prepare entangled pairs of quantum states and then send half of each to Bob. Alternatively, a third party equips an entangled source and sends halves to Alice and Bob. This scheme reflects real-life situations more accurately since, due to distance limitations, a practical implementation could involve a central source, such as a satellite, sending signals to multiple receivers. In DV-QKD, a spontaneous parametric down-conversion (SPDC) source is normally adopted for the EB scheme [70]. In the PDC process, a high-frequency photon is converted to a pair of the low-frequency photon. On the other hand, in Gaussian CV-QKD, two-mode squeezed vacuum states are generated and then sent each mode of a state to Alice, and Bob [71,72]. Alice and Bob then perform measurements on their states to create correlated data. If the same measurement is performed on both states at Alice and Bob, the result on the first state at Alice implies the result on the second state at Bob. An example of the protocol that uses this scheme is BBM92 [36].

2.2.3 Communication Channel

IIn a real-world implementation, the quantum channel with mature optical communication technology has been built for QKD systems. There are two widely adopted channels for QKD:



a) Entangled source is equipped by Alice



b) Entangled source is equipped by a third party

Figure 2.3: Two ways to implement the EB scheme.

optical fiber and free-space optics (FSO) [73].

2.2.3.1 Optical Fiber

Optical fiber is the most common channel used in QKD [4]- [8]. In optical fiber, the photon transfer is rarely disturbed by external conditions, e.g., background light, weather conditions, or other environmental obstructions. Nevertheless, fiber suffers from optical attenuation, which depends exponentially on the channel distance L as $10^{-\alpha L/10}$. The attenuation coefficient α, whose value is strongly dependent on the wavelength, is minimal in the two "optical transmission windows" around 1330 nm ($\alpha \simeq 0.34$ dB/km) and 1550 nm ($\alpha \simeq 0.2$ dB/km). In addition, fiber also suffers from problems such as chromatic dispersion, polarization mode dispersion, birefringence, and so forth [74]. Therefore, the attainable distance of fiber-based QKD is limited to a few hundred kilometers [51], [75]- [80].

2.2.3.2 Free-space Optics

FSO features some advantages compared to optical fiber. FSO has the immediate advantage of lower losses [81]- [83]. FSO also offers a high data rate, cost-effectiveness, license-free operation, and convenient flexibility in infrastructure deployment and redeployment. FSO/QKD have gained much interest in terrestrial applications with fixed ground stations [84]- [87], and satellite-based FSO/QKD [88]- [91]. Nevertheless, there are also some drawbacks concerning free space. 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. As fiber-based QKD systems, relaying is also an appealing solution to extend the operation range of FSO/QKD systems. In [92], 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 atmospheric distortion. To provide secret keys for a location, [93, 94] proposed to use a high-altitude platform (HAP) as relay

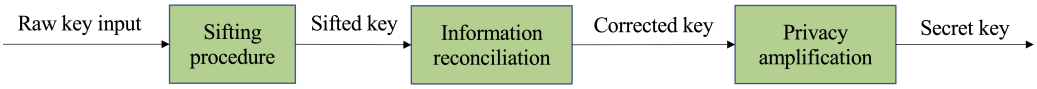


Figure 2.4: Postprocessing procedures.

stations between satellites and mobile stations in vehicular networks, while [88] considered several scenarios involving space transmission among distant ground stations and satellites, where satellites are relaying nodes.

2.2.4 Post-processing procedures

Alice and Bob use the classical authenticated channel to perform post-processing procedures listed in Fig. 2.4. Bob discloses to Alice the time instants that he could detect the encoded key bits, forming their shared raw keys. Then, Alice discloses to Bob her encoding schemes on the key bits he detected, forming their shared sifted keys.

The sifted keys may contain errors due to imperfections in the system. Alice and Bob perform an information reconciliation procedure (i.e., error correction) on the sifted keys. The simplest error correction technique is one including XOR operations. Alice randomly chooses pairs of bits and announces their XOR value. Depending on whether Bob XOR value is the same for the corresponding bits, he can either accept or reject this XOR value in his reply. If Bob accepts this XOR value, Alice and Bob keep the first bit of the pair and discard the second. Otherwise, they discard both bits. After this procedure, Alice and Bob both have identical keys.

Since the information reconciliation procedure was performed using a classical public channel, some information about the key can be leaked to Eve. The privacy amplification procedure ensures that Eve cannot figure out any information about the final secret key from the data she can receive during the information reconciliation procedure. In the privacy amplification procedure, by using the simplest approach, Alice randomly chooses pairs of bits and computes their XOR value. At this time, Alice only announces which bits she chooses. Bob then finds the corresponding bits in his key. Alice and Bob then replace these bits with their XOR value. Thus, the final key is much shorter. If Eve wants to know a value in the final key, she needs to know what the values of Alice's and Bob's bits were before the XOR operation was applied to them. After the information reconciliation and privacy amplification procedures are applied to the sifted keys, Alice and Bob use the resulting final secret keys to encrypt/decrypt secret messages.

2.3 Prominent QKD Protocols

Owing to how the key information is encoded (discrete-variable (DV) or continuous-variable (CV)) and how quantum states are sent and measured (PM scheme or EB scheme), there exist many QKD protocols which helps Alice and Bob distribute secret keys securely. In this dissertation, we will introduce several well-known QKD protocols which are based on PM scheme, such as BB84 (DV-QKD) and GMCS (CV-QKD) or based on EB scheme, such as BBM92 (DV-QKD) and entanglement-based Gaussian CV-QKD protocol (CV-QKD).

2.3.1 BB84 Protocol

BB84 protocol is the best-known QKD protocol which derived its name from its inventors, Charles Bennett, and Gilles Brassard, and the year that it was invented, 1984 [2]. In BB84 protocol, a sequence of single photons which carries qubit states is sent by Alice to Bob through

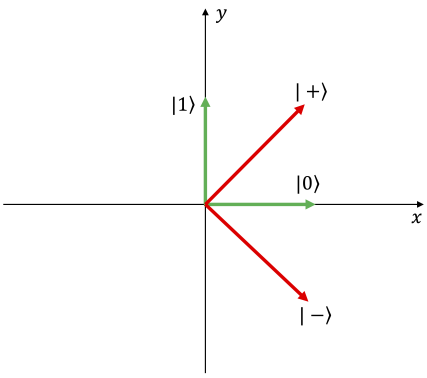


Figure 2.5: The four states being employed in BB84 protocol.

Alice's random bit	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**
Alice's random choosing basis	×	+	×	+	+	×	+	+	×
Photon states Alice sends	↘	↑	↗	↑	→	↘	↑	→	↗
Bob's random measuring basis	+	+	×	×	+	+	+	×	×
Photon states Bob measures	↑	↑	↗	↘	→	↑	↑	↗	↗
Compatibility	☒	☑	☑	☒	☑	☒	☑	☒	☑
Sifted key		**1**	**0**		**0**		**1**		**0**

Figure 2.6: Example of BB84 protocol.

a quantum channel (optical fiber or free-space optics). Recall that a qubit is presented as a vector in a bi-dimensional Hilbert space, which is deduced by the following basis vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.3}$$

The states in Eq. (2.3) ($|0\rangle$ and $|1\rangle$) are referred to as the computational basis (or rectilinear basis). This basis is one of two bases which is used in BB84 protocol. The other is the diagonal basis which is constituted by two states

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{2.4}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{2.5}$$

Four states of the rectilinear and diagonal bases are illustrated in Fig. 2.5. Specifically, the operation steps of this protocol proceeded as follows

1. Alice generates a string of random bits much longer than the desired length of the key.

2. Alice randomly chooses between rectilinear ($\oplus$) or diagonal ($\otimes$) bases to encode every bit she wants to send on a single photon as quantum bits. If $\oplus$ was chosen, bit "0" and bit "1" was mapped onto the state $|0\rangle$ and the state $|1\rangle$, respectively. If $\otimes$ was chosen, bit "0" and bit "1" was mapped onto the state $|+\rangle$ and the state $|-\rangle$, respectively. The encoded quantum bits are then transmitted over the quantum channel to Bob's receiver.

3. At the receiver, Bob detects encoded photons, or qubits, by single-photon detectors. Bob

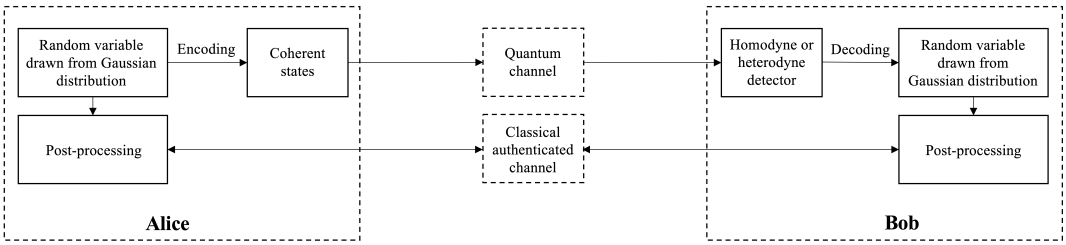


Figure 2.7: Schematic diagram of GMCS protocol.

randomly chooses either the rectilinear ($\oplus$) or the diagonal ($\otimes$) basis for measuring the received qubits. If Alice's encoding and Bob's decoding bases are the same, the corresponding bit value is detected correctly with a high probability. By contrast, if the two bases are different, the received photon is measured by one of two polarization states of the used basis at Bob's receiver. For example, let's consider the first bit of the example in Fig. 2.6 having the value "1", which is encoded in the rectilinear basis ($\oplus$), but measured in the diagonal basis ($\otimes$). A bit value "1" in the diagonal basis is expressed as a function of the diagonal basis as

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{2.6}$$

As a consequence, when $|-\rangle$ is measured in the rectilinear basis, it is equally likely to collapse either to the state $|0\rangle$ (bit "0") or the state $|1\rangle$ (bit "1").

4. After detection, Alice and Bob publicly announces their basis choices through an authenticated classical channel. Alice and Bob discard the states that have been encoded and detected in different bases. They keep only those states on the same basis to form the sifted key.

5. Alice and Bob can choose a random sample of the sifted key bits and compare them to compute the quantum bit error rate (QBER). If the computed QBER is too high, they abort. By contrast, they proceed with classical post-processing, such as error correction and privacy amplification, to produce the final secret key.

2.3.2 Gaussian-modulated Coherent State (GMCS) protocol

This protocol, which is based on CV-QKD and PM scheme, was proposed by Grosshans *et al.* in 2003 [63]. A schematic diagram and an example of this protocol using homodyne detection are illustrated in Fig. 2.7 and Fig. 2.8, respectively. This protocol is the simplest and most widely developed CV-QKD protocol due to its simplicity in preparing, modulation and detecting coherent states. The operational steps of this protocol are described as follows

1. Alice generates random real numbers a_q obey a zero-centred Gaussian distribution $\mathcal{N}(0, V_m)$, where V_m is the modulated variance.

2. Alice also generates another set of random real numbers a_p which also obey the Gaussian distribution $\mathcal{N}(0, V_m)$.

3. Next, Alice prepares coherent states modulated by the amounts of a_q and a_p generated previously in step 1 and step 2 so that a resulting coherent state has a value of (a_q,a_p). For instance, $a_q = 0.86$ and $a_p = -2.74$ are chosen for the first element of the key in steps 1 and 2, respectively. Hence, a coherent state (0.86, -2.74) is prepared by Alice. The prepared coherent states are transmitted over the quantum channel to Bob.

Alice										
1	Raw Gaussian key (a_p)	0.86	3.86	0.71	-0.2	-1.14	5.47	-0.01	-2.09	0.44	4.03
2	Raw Gaussian key (a_q)	-2.74	-1.23	2.51	-1.2	-3.66	1.31	3.9	-1.64	-0.26	-2.66
3	Coherent state preparation	(0.86, -2.74)	(3.86, -1.23)	(0.71, 2.51)	(-0.2, -1.2)	(-1.14, -3.66)	(5.47, 1.31)	(-0.01, 3.9)	(-2.09, -1.64)	(0.44, -0.26)	(4.03, -2.66)
Bob										
4	Detection quadrature	p	p	q	p	q	q	p	q	q	p
5	Detected Gaussian key	0.86	3.86	2.51	-0.2	-3.66	1.31	-0.01	-1.64	-0.26	4.03
Post-processing										
6	Sifted Gaussian key	0.86	3.86	2.51	-0.2	-3.66	1.31	-0.01	-1.64	-0.26	4.03

Figure 2.8: Example of GMCS protocol.

4. If Bob uses homodyne detection, he generates a random variable u for each incoming state and chooses either q or p quadrature for detection depending on the value of u. After detection, Bob obtains a real variable b_q or b_p depending on the chosen quadratures. As seen in the example, p quadrature is chosen for detecting the first element of the key. Thus, Bob obtains a value of -2.74 when he measures the first received coherent state. If Bob uses heterodyne detection at the receiver, he measures the q and p quadrature components and obtains (b_q, b_p).

5. After all the received coherent states have been measured by Bob, the post-processing procedure proceeded with the sifting process. If homodyne detection is used, Bob reveals the value of u, i.e., whether he measured the q or p quadrature, and Alice retains a_q or a_p depending on the value of u. Otherwise, if heterodyne detection is used, the sifting process is unnecessary since both of the real random variables generated by Alice are used to generate the key [64]. Thus, the secret-key rates are higher than using homodyne detection.

   In the example, the sifted Gaussian key is the same for Alice and Bob. Nevertheless, if Eve or noise can present, Bob's key will be a noisy version of Alice's key. Thus, Alice and Bob obtain correlated Gaussian keys.

6. Next, Alice, and Bob perform parameter estimation in which they reveal a randomly chosen subset of their correlated Gaussian keys. It allows them to estimate the parameters of the channel and limit the maximum amount of information Eve can deduce from their values.

7. Alice and Bob perform the information reconciliation procedure. This procedure involves quantizing Alice's and Bob's correlated Gaussian keys into binary keys and performing error correction.

8. Alice and Bob perform privacy amplification to a new, shorter binary key so that Eve has only negligible information about their secret keys.

2.3.3 BBM92 Protocol

In the BBM92 protocol, instead of Alice sending particles to Bob, there is a central source creating pairs of entangled particles, each described by a *Bell state*. The entangled particles are then separated and sent to Alice and Bob, each getting one-half of each pair.

To understand this protocol, we need to acquaint ourselves with the concept of multiple qubits. Suppose we have two qubits. If these were two classical bits, there would be four possible states: 00, 01, 10, and 11. Correspondingly, a two-qubit system has four basis states

designated $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. The state vector describing the two qubits is expressed as follows

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{2.7}$$

Similar to the case for a single qubit, the measurement results in x (= 00, 01, 10, or 11) occurs with probability $|\alpha_x|^2$. Since the probabilities must sum to one, the condition of the probabilities is therefore expressed by $\sum_{x\in\{0,1\}^2}|\alpha_x|^2$, where the notation '$\{0,1\}^2$' means 'the set of strings of length two with each letter being either zero or one.' A two-qubit state ($|\Psi\rangle_{AB}$) shared between two parties Alice (A) and Bob (B), is defined to be *entangled* if the state cannot be written as a *tensor product* of the states of the individual parties ($|\Psi\rangle_A$ and $|\Psi\rangle_B$) such that

$$|\Psi\rangle_{AB} \neq |\Psi\rangle_A|\Psi\rangle_B, \tag{2.8}$$

where $|\Psi\rangle_A|\Psi\rangle_B$ is denoted for the *tensor product*, which is a way of putting vector spaces together to form larger vector spaces. An important entangled state is the *Bell state* or *Einstein, Podolsky, and Rosen (EPR) pair* is presented as

$$\begin{aligned} |\Phi^+\rangle &= \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \\ &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \end{aligned} \tag{2.9}$$

where $|00\rangle_{AB} = |0\rangle_A|0\rangle_B$ and $|11\rangle_{AB} = |1\rangle_A|1\rangle_B$ are two-qubit states shared between two parties Alice and Bob. $|0\rangle_A$ and $|1\rangle_A$ are states of qubit of Alice, and $|0\rangle_B$ and $|1\rangle_B$ are states of qubit of Bob. The Bell state has the remarkable property that upon measuring the first qubit, one obtains two possible results: 0 with probability $1/2$, leaving the post-measurement state $|\Phi^+\rangle' = |00\rangle$, and 1 with probability $1/2$, leaving the post-measurement state $|\Phi^+\rangle' = |11\rangle$. Consequently, a measurement of the second qubit always gives the same results as the first qubit. The measurement outcomes are correlated. It turns out that other types of measurement can be performed on the Bell state by first applying some operations to the first or second qubit and that interesting correlations still exist between the result of a measurement on the first and second qubit. In other words, if the two-qubit state is entangled, the measurement of one will affect the other. Similarly, there are three other two-qubit states called the *Bell state* as follows

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.10}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.11}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.12}$$

The BBM92 protocol using entangled qubit pairs in DV-QKD systems was proposed by Bennett, Brassard, and Mermin in 1992 [36]. The original protocol with four steps can be described as follows:

1. Charlie generates entangled photon pairs and transmits to Alice and Bob separately via FSO channels, in which each pair has the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

2. Alice and Bob randomly select polarization bases, i.e., either rectilinear basis ($\oplus$) or diagonal one ($\otimes$), to measure received entangled photons. Two bases $\oplus$ and $\otimes$ constitute four polarization states $(0^\circ, 90^\circ)$ and $(-45^\circ, 45^\circ)$, respectively.

3. Through a classical public channel, Alice broadcasts the basis choice she used for each received photon. Then, Bob reveals which detected photons he used on the same basis as

Table 2.1: An Example of BBM92 Protocol Operation.

Charlie		**Alice**				**Bob**				Sifted key
Time	Entangled photon pairs state	Time	Basis	Measured state	Bit	Time	Basis	Measured state	Bit (inverted)	
t_0	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	t_0	$\oplus$	$0°$	0	t_0	$\oplus$	$90°$	0	0
t_1	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	t_1	$\oplus$	$0°$	–	t_1	$\otimes$	$45°$	–	*discarded*
t_2	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	t_2	$\otimes$	$45°$	1	t_2	$\otimes$	$-45°$	1	1
t_3	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	t_3	$\otimes$	$-45°$	–	t_3	$\oplus$	$90°$	–	*discarded*

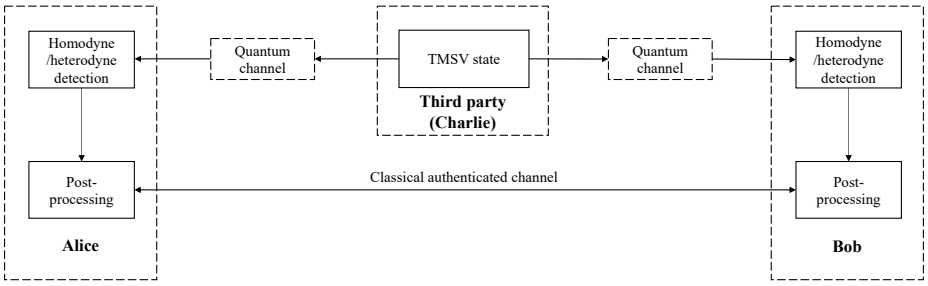


Figure 2.9: Schematic diagram of entanglement-based Gaussian CV-QKD protocol.

Alice. They both discard photon measurements with different bases. This step is known as the *sifting process*.

Alice and Bob convert the remaining results by assigning them for bit "0" and bit "1" to form the *sifted key* as follows:

$$\left.\begin{array}{ll}\text{The polarization state} & 0^\circ \\ \text{The polarization state} & -45^\circ\end{array}\right\} \rightarrow \text{Bit "0"} \tag{2.13}$$

$$\left.\begin{array}{ll}\text{The polarization state} & 90^\circ \\ \text{The polarization state} & 45^\circ\end{array}\right\} \rightarrow \text{Bit "1"} \tag{2.14}$$

As the photon pairs are (anti-correlated) entangled, Bob needs to invert his detected bits so that he and Alice can get an identical bit string. An example of the derived sifted key in the BBM92 protocol is in Table 2.1.

4. Alice and Bob perform post-processing procedures including *information reconciliation* and *privacy amplification* over the public channel to correct transmission errors and produce the *final secret key*.

2.3.4 Entanglement-based Gaussian CV-QKD protocol

Entanglement-based Gaussian CV-QKD protocol has been widely considered in [95]- [98] and implemented experimentally in [99]. The operational steps of this protocol are described as follows

1. A Gaussian two-mode entangled state (two-mode squeezed vacuum state (TMSV)) is generated. Alice could prepare this state, keep one mode, and then send the other mode through the quantum channel to Bob. Alternatively, a trusted third party could prepare this state and send each mode to Alice and Bob through the quantum channel. Figure 2.9 illustrates the second way of sending the TMSV state to Alice and Bob using a trusted third party.

2. Alice and Bob then proceed by measuring their modes using homodyne or heterodyne detectors. As the result of their measurement, Alice and Bob end up with two sets of Gaussian-distributed random variables, which are correlated to each other.

3. Following the generation of the correlated data, Alice and Bob perform a post-processing procedure over a classical authenticated channel to generate secret keys for the encryption and decryption of secret messages.

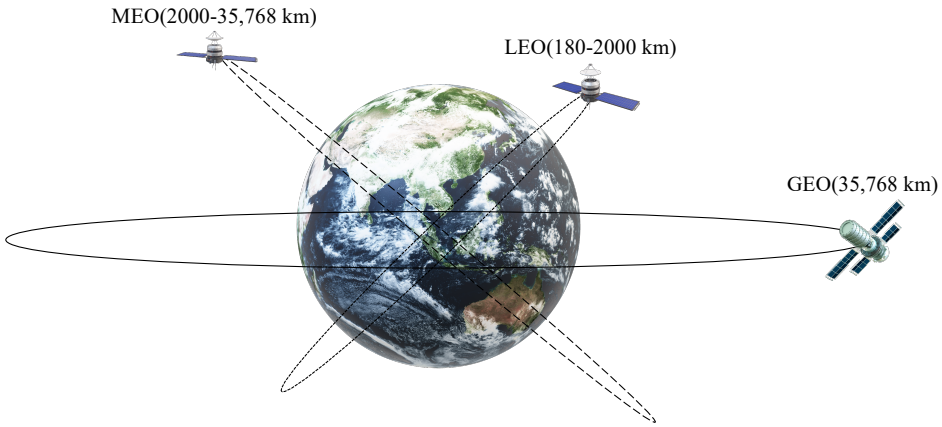


Figure 2.10: Three main classes of satellite orbits.

2.4 Satellite-based Free-Space Optical Quantum Key Distribution

The QKD systems can be implemented over optical fiber, terrestrial free-space optics (FSO), or satellite-based FSO links [31]. Fiber-based QKD has been well studied and scaled up to network-level implementations, as in Tokyo, DARPA, and SECOQC QKD networks [100]. The QKD deployment over terrestrial FSO links has also been considered for point-to-point connections. However, the range of terrestrial FSO/QKD links is limited to several kilometers, especially for mobile users [15, 87, 101]. Considering the future scenario where QKD would be implemented globally for a wide range of applications, including mobile users like autonomous vehicles and unmanned aerial vehicles (UAVs), satellite-based QKD technology becomes a viable solution for global security service. The feasibility of satellite-based QKD has been investigated over the past decade [25, 55, 102, 103], and a significant milestone was reached in 2017 when a satellite-to-ground QKD implementation was realized with the world's first quantum LEO satellite Micius [1]. Since then, the era of satellite-based QKD has been opened with a series of experiments and implementations [26, 27, 87].

2.4.1 Orbit Altitude of Satellites

There are three main classes of satellite orbits as shown in 2.10

- Geostationary orbit (GEO): This orbit has an altitude of 35,786 km. Satellites in this orbit constantly stay above one particular place over the Earth. They offer substantial advantages, such as broad coverage, continuous link to ground stations, 24/7 operation, and no expensive equipment for tracking required. This orbit's disadvantages are the large link losses and high latency due to the long-distance propagation.

- Medium-Earth orbit (MEO): This orbit comprises a wide range of orbits between 2000 km and 35,768 km. It offers a greater width of satellite view than the low-Earth orbit and a greater proximity to the Earth's surface than the geostationary Earth orbit. The MEO is very commonly used by navigation satellites.

- Low-Earth orbit (LEO): This orbit is situated between 160 and 2000 km in altitude. A satellite in LEO benefits from proximity to the surface which significantly reduces losses due to beam diffraction. Compared to satellites in GEO and MEO, the LEO satellite is less expensive to launch into orbit, has lower latency, and has less power consumption. On the other hand, there are shortcomings in the high speed of the LEO satellite relative to the Earth, which compromises pointing accuracy during signal transmission and the limited time period during which QKD can be performed.

Thanks to the advantages of LEO, for past and current satellite-based FSO/QKD, the LEO satellite is the most common option [1]. In the future, to provide a global-scale QKD network, future studies and projects might seek altitudes in the MEO, or GEO range [104].

2.4.2 Operating Wavelength

The wavelength of QKD signal from the satellite is an important parameter, as it directly influences many aspects such as atmospheric and optical fiber transmissions, diffraction, and detection efficiency. Two wavelengths are considered: 810 nm and 1550 nm. The former, 810 nm, is typically used in SPDC sources, whereas 1550 nm is the standard telecom wavelength. The advantage of using 810 nm wavelength is that it has less diffraction and is compatible with efficient single-photon detectors. The advantage of using 1550 nm wavelength is that it has lower atmospheric attenuation, good behavior of the photodetectors' responsivity, and compatibility with standard telecom fibers. From the eye-safety point of view, 1550 nm wavelength is preferred because the eye fluids absorb this wavelength before being focused on the retina.

2.4.3 Operating Scheme of Satellite-based FSO/QKD

In the scenario of distributing secret keys for two distant ground stations (Alice and Bob), two operation schemes of QKD can be used to implement satellite-based FSO/QKD, including the prepare-and-measure scheme and entanglement-based scheme.

2.4.3.1 Satellite-based FSO/QKD using prepare-and-measure scheme

A satellite carries out QKD operation with Alice and Bob to establish independent secret keys with each of them by using the prepare-and-measure scheme. The details of this scheme are mentioned in section 2.2.2.1. The satellite holds all keys, while the stations only have access to their keys. To share a common secret key to Alice and Bob, the satellite combines their respective keys K_A and K_B and broadcasts their bit-wise parity $K_C = K_A \oplus K_B$. Using this announcement, the stations can retrieve each other keys by performing a mathematical operation with their key as $K_A \oplus (K_A \oplus K_B) = K_B$ and $K_B \oplus (K_A \oplus K_B) = K_A$. Because the original keys are independent secret strings, their bit-wise parity is a uniformly random string. Therefore, the parity announcement does not reveal any useful information to potential eavesdroppers. However, since the satellite holds all keys, access to the data obtained by the satellite would give the eavesdropper complete knowledge of the key. Thus, the satellite must be trusted in this setting. Moreover, the disadvantages of the scheme include complexity and inefficiency as we need more than one phase to distribute a key from Alice to Bob ultimately. All steps in satellite-based FSO/QKD using the prepare-and-measure scheme are illustrated in Fig.2.11.

2.4.3.2 Satellite-based FSO/QKD using entanglement-based scheme

An untrusted node is preferred to avoid the potential key leakage in the satellite since the eavesdropper gets no information even if she takes full control of the satellite. In this scheme, the satellite acts as the central source and sends two beams of entangled quantum states to Alice and Bob simultaneously [87] as shown in Fig.2.12. They then make independent measurements of the received quantum state and decide on the final secret key without the involvement of the satellite. Therefore, the trust requirement of the satellite can be relaxed. This scheme is more suitable for implementing a global-scale QKD network.

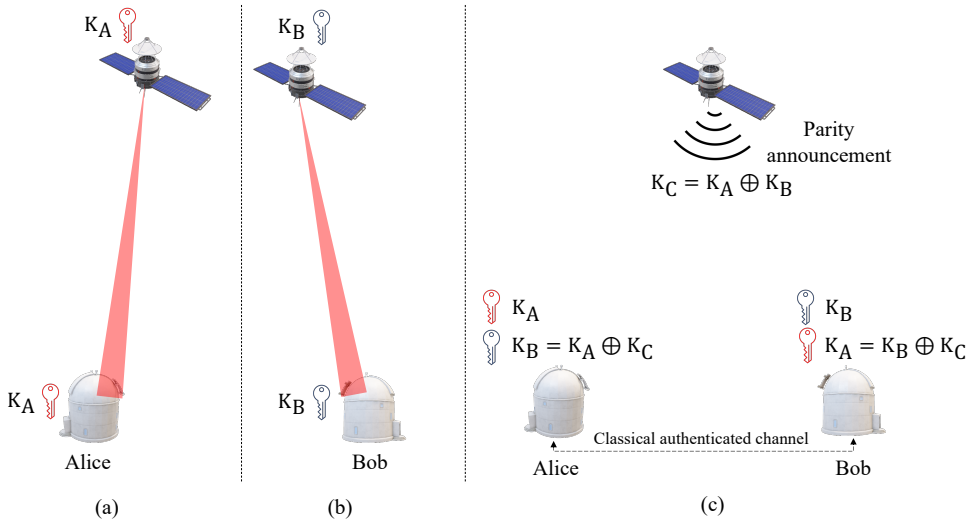


Figure 2.11: Illustration of satellite-based FSO/QKD using prepare-and-measure scheme: (a) the satellite established a shared secret key K_A with Alice, (b) the satellite established a shared secret key K_B with Bob, (c) the satellite make a parity announcement of two keys, so that both Alice and Bob can derive each other's key and then use it to encrypt private communication between them.

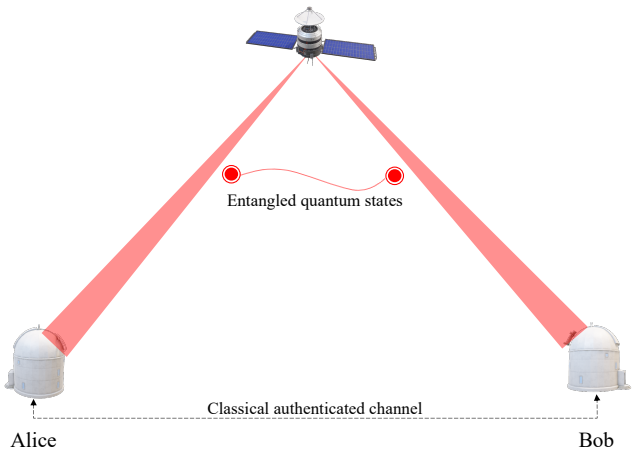


Figure 2.12: Illustration of satellite-based FSO/QKD using entanglement-based scheme.

Table 2.2: Recent achievement milestones for satellite FSO-based QKD experiments

Year	Authors	Encoding & Decoding	Scheme	Distance	Secret-key rate (SKR)	Notes
2015	R. Vallone *et al.* [103]	DV-QKD	Prepare-and-measure	1000-1500 km	N/A	LEO satellite
2017	S. K. Liao *et al.* [17]	DV-QKD	Prepare-and-measure	1200 km	1 kbps	LEO satellite (Micius)
2017	J. Yin *et al.* [19]	DV-QKD	Entangled-based	500-1000 km	3.5 bps	LEO satellite (Micius)
2017	S. K. Liao *et al.* [26]	DV-QKD	Prepare-and-measure	388-719 km	91 bps	LEO satellite (Tiangong-2 space lab)
2017	K. Gunthner *et al.* [107]	CV-QKD	Prepare-and-measure	38600 km	N/A	Homodyne detector, GEO satellite (Alphasat)
2017	H. Takenaka *et al.* [55]	DV-QKD	Prepare-and-measure	650-1000 km	N/A	LEO microsatellite (SOCRATES)
2018	S. K. Liao *et al.* [27]	DV-QKD	Prepare-and-mearsure	600-1000 km	3 kbps - 9kbps	Decoy state, LEO satellite (Micius)
2020	J. Yin *et al.* [30]	DV-QKD	Entangled-based	750 km	0.12 bps	LEO satellite (Micius)

2.4.4 Recent Developments of Satellite-based FSO/QKD and Opening Issues

The biggest milestone in satellite-based QKD was the successful launch of the first quantum satellite Micius in August 2016 [1]. Micius was also used for demonstrating an intercontinental quantum network, distributing the keys for a text and video exchange between the ground stations of Xinglong, Nanshan (China), and Graz (Austria) [27]. In 2017, an experimental demonstration of space-to-ground QKD from Tiangong-2 space lab to Nanshan ground station was reported in [26]. In this experiment, the communication distance is between 388 km and 719 km, and the final key rate is about 91 bps. In the same year, NICT also developed the SOTA lasercom terminal for testing the optical downlinks and quantum communication with a low-cost platform (the microsatellite SOCRATES) at an altitude of 650 km [55]. Nanosatellites, CubeSats in particular, are low-cost alternative ways for traditional, large platforms. Many recent studies propose to use nanosatellites for QKD implementation [21]- [24]. They have opened a new page in developing small, low-cost satellites, making it possible for many research institutes and companies to use QKD technology. Most quantum satellite experiments focused on DV-QKD technologies [19, 26]. Recently, CV-QKD technologies have begun to apply for satellite FSO-based QKD in both prepare-and-measure [25] and entangled-based scheme [71, 97]. The feasibilities of satellite quantum communication at the MEO and the GEO have been demonstrated in [105–107]. The summary achievements of satellite-based FSO/QKD experiments are given in Table 2.2.

Even though DV-QKD and CV-QKD have been focused and recently implemented in satellite-based FSO/QKD, both of them are expensive due to the requirement of bulky single-photon

Table 2.3: Comparison between different QKD technologies [32]

Characteristics	DV-QKD [2]	CV-QKD [59]	Non-coherent CV-QKD [32]
Source	Weak laser pulse (single-photon)	Laser	Laser
Modulation	Polarization	Amplitude & Phase	Intensity
Detection	Single-photon detection	Coherent detection	Direct detection
System Complexity	Very high	High	Low
Implementation Cost	Very high	High	Low
Compatibility with Standard Technologies	No	Yes	Yes
Key Rate	Low	High	High

detectors in DV-QKD and homodyne/heterodyne detectors which need sophisticated phase-stabilized local light for coherent detection in CV-QKD [35]. Considering the future scenario where QKD would be implemented globally for a wide range of applications, including mobile users like autonomous vehicles and UAVs, simple setup and low cost are necessary features. To achieve these features, non-coherent CV-QKD by employing DT/DD at receivers is a suitable solution [32] thanks to its advantage as shown in Table 2.3. This implementation has been firstly proposed for fiber QKD systems [108] and then for terrestrial FSO/QKD systems [32], and satellite FSO/QKD [94] only in *prepare-and-measure scheme*.

Specifically, in the QKD implementation of [108], the transmitter sends two slightly intensity-modulated pulses employing On-Off Keying (OOK). The receiver detects the transmitted signal directly by a PIN detector with dual thresholds. By adjusting two thresholds at high and low levels of two intensity-modulated signals with small amplitude differences, the sifting process of two non-orthogonal photon bases in the conventional BB84 QKD protocol is mimicked. Because of quantum noise, the received signal exceeds thresholds randomly and is uncorrelated for receivers and Eve. If thresholds are not exceeded, two intensity-modulated pulses are indistinguishable. Thus, if Eve guesses the states randomly, she will inevitably introduce errors.

Channel-State Information (CSI) is required at the receiver to optimize the setting of DT. In the case of optical fiber, CSI estimation can be easily attained because of the non-fading channel characteristics. On the other hand, CSI estimation for DT setting over fading channels in case of OOK signaling is more complex due to the asymmetry of binary signals (e.g., noise variances are different in bit "0" and "1"). Thus, non-coherent CV-QKD by employing DT/DD at receivers in [32], and [94] is slightly different from the first implementation in [108] by using Subcarrier Intensity Modulation (SIM)/Binary Phase-Shift Keying (BPSK) signaling and DT/DD over FSO channel. The CSI estimation over the atmospheric turbulence-induced fading channels will be relaxed by using FSO/BPSK signaling whose signals of bit "0" and "1" are symmetric over the "zero" level.

As mentioned above, *entanglement-based scheme* is more suitable for implementing a global-scale QKD network. Non-coherent CV-QKD with a simple setup and cost-efficient implementation would be implemented globally for a wide range of applications. Therefore, it is necessary to design non-coherent CV-QKD for satellite-based FSO/QKD in *entanglement-based scheme*.

Moreover, since the coverage and flyover time of one LEO satellite is limited, establishing the constellation of LEO satellites is a possible solution. Nevertheless, the key relaying/routing in the network among LEO satellites would bring new security concerns while QKD is performed for two distant ground stations. In contrast, GEO satellites can access ground stations continuously and have a broad coverage. However, their signal can suffer from high channel

loss and limited key generation rate. According to [109], the future quantum constellation will be comprised of high and low orbits satellites. Combining both GEO and LEO satellites to build QKD networks is a research direction worth exploring.

Satellite-based FSO/QKD systems are recently designed to distribute secret keys to two legitimate users (Alice and Bob) [87, 118]. With the rapid development of next-generation networks, the number of mobile users, such as mobile devices and autonomous vehicles, in the coverage region of the satellite will overgrow. It is necessary to find a way for satellite-based FSO/QKD systems to distribute secret keys to multiple users simultaneously instead of repeating QKD operations for each pair of two legitimate users.

Chapter 3

Design of Practical Satellite-Based FSO/QKD Systems

This chapter[1] proposes a new implementation of non-coherent CV-QKD protocol for satellite FSO/ QKD systems using the dual-threshold/direct detection (DT/DD) receivers inspired by the BBM92 protocol[2] for EB scheme. The proposed system is less complex and, therefore, possibly cheaper than current discrete-variable (DV) and CV-QKD ones using coherent detection receivers. We model and analyze the performance of the proposed system in the context that a satellite distributes secret keys to two legitimate users. The analytical results are derived by considering channel loss, atmospheric turbulence-induced fading, and receiver noises. The Gaussian beam model is considered to evaluate the impact of geometric spread on the signal received by legitimate users and the possibility of being eavesdropped. Based on the design criteria for the system and analytical results, we investigate the feasibility of a case study for the Japan QKD network using the existing low-Earth orbit (LEO) satellite constellation.

3.1 Proposed Implementation of Non-coherent CV-QKD Protocol using DT/DD inspired by BBM92

This section describes our newly proposed non-coherent CV-QKD systems using DT/DD receivers. We also describe how our system, while it is physically distinct, can be considered as an implementation inspired by the BBM92 protocol. Figure 3.1 shows the considered scenario in which a satellite (Charlie) distributes secret keys to two legitimate users (Alice and Bob) via FSO channels. For the sake of convenience, Alice, Bob, and Charlie are denoted by "A", "B", and "C" in notation, respectively. In the figure, H_U and H_C are used to denote the altitude of user $U \in \{A, B\}$, and Charlie, respectively. The zenith angle, which is the angle between the transmitted beam to user U and the vertical direction, is denoted as ζ_U. In addition, the elevation angle, which is the angle between the transmitted beam to user U and the horizontal direction, is determined by $(\pi/2 - \zeta_U)$.

In practical scenarios, to prevent the transmitted signal from being blocked by high-rise buildings and minimize the effect of atmospheric attenuation and turbulence, the minimum acceptable elevation angle for satellite tracking is set to 30°. In other words, a satellite is not

[1] The content of this chapter was presented in part in

1. Minh Q. Vu *et al.*, "Entanglement-based satellite FSO/QKD system using dual-threshold/direct detection," *ICC 2022 - IEEE International Conference on Communications,* Seoul, pp. 3245-3250, May 2022,.
2. Minh Q. Vu *et al.*, "Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/ direct detection," *in IEEE Access,* vol. 10, pp. 113260-113274, Oct. 2022.

[2] The BBM92 protocol is introduced in Sec. 2.3.3

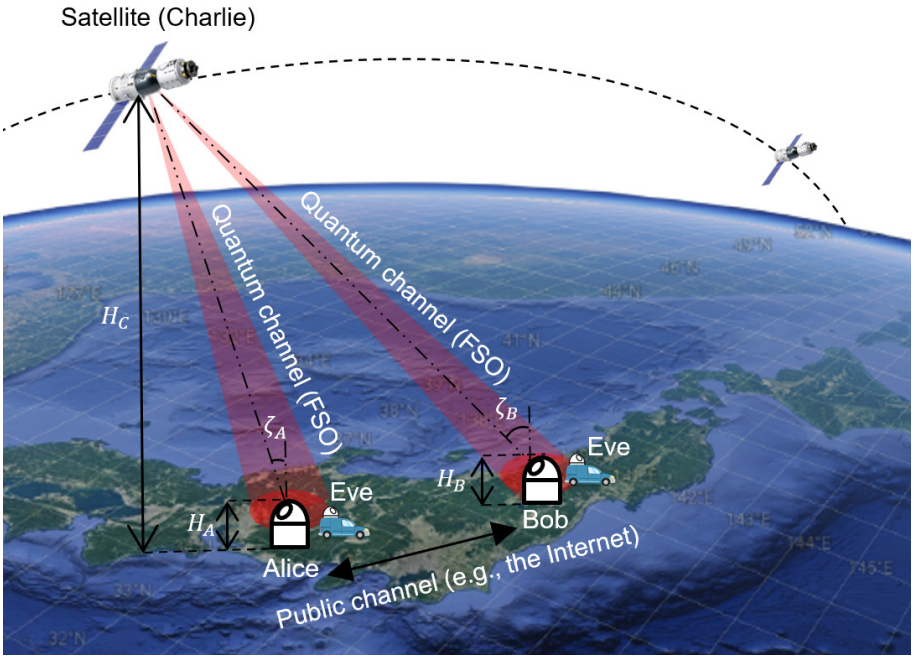


Figure 3.1: The considered scenario of satellite QKD system. (Map data: Google Earth)

tracked when it is below 30° of the horizon.

Eavesdroppers (Eves) try to perform an unauthorized receiver attack (URA), the most popular attacking strategy for practical FSO systems. In this attack, Eves tries to tap the transmitted signal from Charlie by locating their receivers within the beam footprint near legitimate users at a distance d_E m. Following are the operational steps of our proposed implementation of the BBM92 protocol for CV-QKD systems using DT/DD, which are also summarized in the flowchart illustrated in Fig. 3.2.

Step 1: Charlie generates subcarrier intensity modulation/binary phase-shift keying (SIM/BPSK) modulated signals with a small modulation depth ($0 < \delta < 1$), representing binary random bits "0" or "1", and transmits simultaneously to both Alice and Bob over FSO channels.

Step 2: Both Alice and Bob individually detect the received signals using their own DT/DD receiver following the detection rule as

$$\text{Decision} = \begin{cases} 0 \text{ if } \left(i_d^U \leq d_0^U\right), \\ 1 \text{ if } \left(i_d^U \geq d_1^U\right), \\ \text{X otherwise}, \end{cases} \tag{3.1}$$

where i_r^U is the detected value of the received current signal at user U. 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. It is important to note that these levels are chosen independently. Furthermore, "X" represents the case when either Alice or Bob does not detect a data bit based on the detection rule. This illustrates the case of different basis selections between Alice and Bob, as in the BBM92 protocol.

Step 3: Using a public channel, Bob notifies Alice of the time instants that he detected bits from received signals. They also discard values at the time that no bit is detected. After that, Alice and Bob can share an identical bit string, i.e., *sifted key*. An example of the proposed protocol is shown in Table 3.1.

Step 4: Finally, as in the original BBM92 protocol, further information reconciliation and privacy amplification are carried out over public channels to obtain the *final secret key*.

The security of the original BBM92 protocol relies on two factors. First, it is Charlie's generation of entangled photon pairs randomly using one of two non-orthogonal bases. This

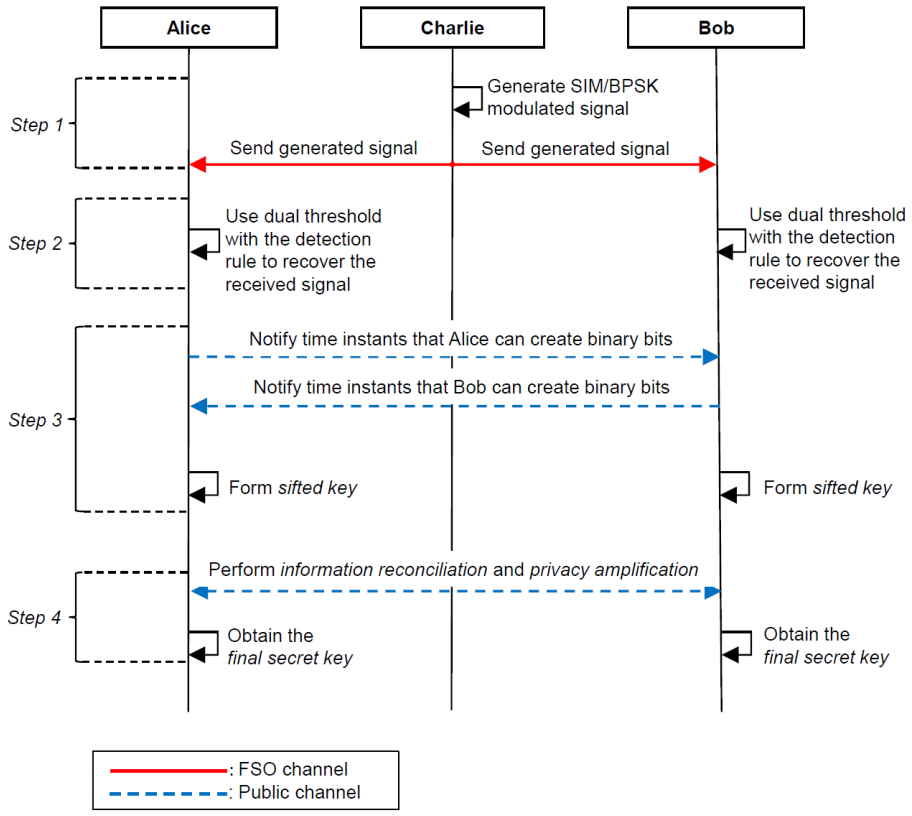


Figure 3.2: The flowchart of the proposed implementation inspired by the BBM92 protocol for EB scheme.

guarantees that an Eve cannot simultaneously maintain perfect correlations while detecting information about the measurement result. In other words, Eve will suffer a high ratio of incorrect detection. Secondly, Alice and Bob decode the received data by measuring their respective photons randomly in two non-orthogonal bases. This guarantees that only a fraction of information can be detected in a random fashion.

Similarly, the security of our proposed system is also from two factors: (1) the modulation depth δ of the SIM/BPSK signals is small enough, and (2) Bob and Alice should independently choose dual-threshold levels at which only a tiny fraction of transmitted bits can be detected [32, 94]. The first condition guarantees a very high bit error rate, so Eve will likely get a significant fraction of transmitted bits incorrectly. As Eve cannot obtain the knowledge of Alice's and Bob's dual-threshold values, her best choice is to use the optimal threshold $d_t^E = 0$ to get as much key information as possible. Ideally, when Eve uses the optimal threshold to detect bits from Charlie, Eve's error probability (P_{error}^E), which is the probability that Eve falsely detects Charlie's transmitted bits, is approximately 0.5. However, it was shown that $P_{\text{error}}^E \approx 10\%$ is good enough provided that Alice and Bob also can receive a small fraction of transmitted bits due to the DT detection [94]. The second condition guarantees this requirement when a large portion of data is randomly discarded. In fact, we aim to design the system so that the rate of signal detection (sift probability) is very low (around 10^{-3}), which is much smaller than that of the original BBM92[3].

Table 3.1: An Example of the Proposed Implementation Inspired by the BBM92 Protocol for EB Scheme

Satellite (Charlie)			**Alice**			**Bob**			Sifted key
Time	Bit	Signal	Time	Threshold	Bit	Time	Threshold	Bit	
t_0	0	i_0	t_0	d_0^A	0	t_0	d_0^B	X	*discarded*
t_2	1	i_1	t_2	d_1^A	X	t_2	d_1^B	X	*discarded*
t_3	0	i_0	t_3	d_0^A	0	t_3	d_0^B	0	0
t_4	1	i_1	t_4	d_1^A	1	t_4	d_1^B	1	1
t_5	0	i_0	t_5	d_0^A	X	t_5	d_0^B	0	*discarded*

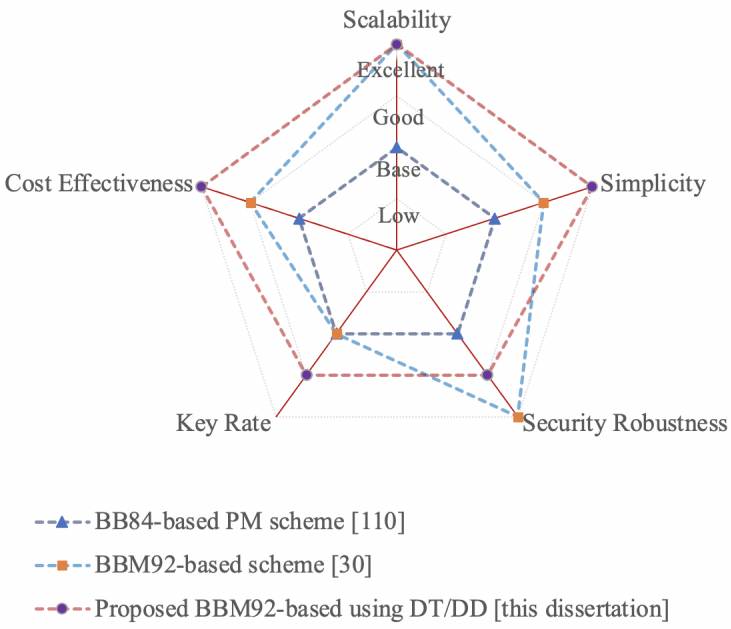


Figure 3.3: A comparison of QKD implementation schemes in satellite FSO/QKD systems.

3.1.1 Key Features of the Proposed Scheme

We consider a scenario in which two distant legitimate users (Alice and Bob) exchange secret keys using the FSO-based satellite systems. While there are many different implementations of QKD, we illustrate key features of our proposed scheme by comparing it with two original QKD systems based on the BB84 [110] and BBM92 protocol [30]. For the sake of convenience, we denote scheme 1, scheme 2, and scheme 3 for the BB84-based PM, the conventional BBM92-based EB systems, and our proposed non-coherent CV-QKD protocol using DT/DD inspired by the BBM92 protocol, respectively. Different performance metrics, including simplicity, cost-effectiveness, security robustness, flexibility, and scalability, are evaluated and discussed. In the discussion, the first-ever QKD protocol of BB84 is regarded as having the base performance.

- **Scalability:** It is the ability to support network expansion and upgrading when the number of users increases. In the BBM92-based schemes, end users do not need the capability to transmit signals to a satellite; new users can be added as long as they are in the satellite coverage area. This feature also makes it easy to expand the network by adding new satellites without requiring re-configuring users. Expansion of the BB84-based networks is more complicated as the uplink connection from users (Alice, Bob) to the satellite is needed. Therefore, both schemes 2 and 3 offer a much better level of scalability in comparison with the base scheme.

- **Simplicity:** As for scheme 1, the satellite acts as a trusted relay node for legitimate users, where the secret key is distributed from Alice to Bob via the satellite. In this implementation, we need two phases to complete the key distribution, i.e., from Alice to the satellite and then from the satellite to Bob. *Regarding scheme 2*, the satellite acts as the source, which simultaneously sends two beams of entangled quantum states to Alice and Bob. These legitimate users then make independent measurements of received quantum states and decide the final secret key without the involvement of the satellite. Therefore, it is simpler than the first scheme as it needs only one phase for the key distribution. Our proposed implementation (i.e., scheme 3), which is also based on the BBM92, is even more straightforward as CV source and DT/DD receiver are employed.

- **Security Robustness:** As the satellite relays the key in the base scheme (scheme 1), it needs to be secured. This negatively affects the security robustness of scheme 1. The BBM92-based schemes (schemes 2 and 3) can remedy this issue by having the satellite to act as a random sequence distributor. Alice and Bob then settle the secret key without the involvement of the satellite. In addition, compared to scheme 3, scheme 2 achieves a higher level of security robustness as it inherits all the quantum features in the distribution of the secret key to legitimate parties. In the proposed scheme (scheme 3), the weakness in terms of the security robustness is the requirement of the channel state information (CSI) from the legitimate receivers for the proper selection of dual-threshold values.

- **Key Rate:** The inherent issue with the DV-QKD, i.e., schemes 1 and 2, is the low key rate due to the limited capability of single-photon detectors. The key rate is dependent on the transmission distance. However, it is typically in the range of kb/s up to Mb/s over 100 km. The proposed scheme 3 employs the CV-QKD, which potentially offers a higher key rate as it is actually implemented using conventional optical systems [32]. Even when only a tiny fraction of transmitted bits can be detected (typically, it is about 0.1%), we can still achieve Mb/s key rates over optical systems offering Gb/s connections.

[3] As the proposed system can be implemented on modern FSO links with the bit rate of Gb/s, a high key rate (100 kb/s or higher) can still be achieved with such a low sift probability.

- **Cost-Effectiveness:** Cost is an essential performance metric to popularize QKD systems. Both schemes 1 and 2 use the DV-QKD, which requires bulky and expensive devices. Scheme 3 uses the CV-QKQ, by which the satellite can use an off-the-shelf laser source to generate the signal. Legitimate users employ a simple direct detection to detect the received signals [31]. Therefore, compared to schemes 1 and 2, the QKD function in scheme 3 achieves the lowest implementation cost. Compared to the base scheme (scheme 1), the BBM92-based system is potentially cheaper as it requires only one transmitter (on the satellite), while the BB84 needs two (at Alice and on the satellite).

3.2 System Models

Figure 3.4 depicts the block diagram of the proposed system, including three main parts: a satellite (Charlie) and two legitimate users (Alice and Bob). For the sake of simplicity, a perfect pre-synchronization between Alice, Bob, and Charlie, which can be realized using the global positioning system (GPS) during the preparation stage, is assumed.

At the satellite, a sequence of binary data (the raw key), denoted as $d(t)$, is first modulated onto a radio frequency (RF) subcarrier signal using BPSK modulation scheme. The subcarrier signal, denoted as $m(t)$, is then used to modulate the intensity of a continuous-wave laser beam to form the subcarrier intensity modulated (SIM) signal as

$$P_s(t) = \frac{P}{2}\left[1 + \delta m\left(t\right)\right], \tag{3.2}$$

where P is the peak laser power, and δ is the intensity modulation depth ($0 < \delta < 1$). The subcarrier signal $m(t)$ is given by $m(t) = A_c g(t)\cos(2\pi f_c t + d\pi)$, where A_c is the subcarrier amplitude, $g(t)$ is the pulse shaping function, f_c is the subcarrier frequency, and $d \in \{0, 1\}$ corresponding to binary data bit "0" and bit "1". To simplify the analysis, we normalize the power of $m(t)$ to unity.

The received optical signal is first passed through an optical band-pass filter (OBPF) and converted into an electrical signal by a PIN photodetector at each user. The electrical signal at the output of the photodetector is determined as

$$i_r^U\left(t\right) = \frac{1}{2}R_e P h_{\text{e2e}}^U\left(t\right)\left[1 + \delta m\left(t\right)\right] + n_{\text{e2e}}^U\left(t\right), \tag{3.3}$$

where $i_r^U(t)$ is the electrical signal at the output of user U's photodetector, R_e is the responsivity of the photodetector, $h_{\text{e2e}}^U(t)$ are the channel state between Charlie and user U, and $n_{\text{e2e}}^U(t)$ is the receiver noise. After the DC term is filtered out by OBPF, the electrical signal is passed through the BPSK demodulator to get the demodulated electrical signal $r_d^U(t)$ which is calculated as

$$r_d^U(t) = i_r^U(t)\cos(2\pi f_c t) = \begin{cases} i_0^U = -\frac{1}{4}R_e P h_{\text{e2e}}^U\left(t\right) + n_{\text{e2e}}^U\left(t\right) \\ i_1^U = \frac{1}{4}R_e P h_{\text{e2e}}^U\left(t\right) + n_{\text{e2e}}^U\left(t\right) \end{cases}, \tag{3.4}$$

where i_0^U and i_1^U are the received current signals for bit "0" and bit "1", respectively. It is assumed that the dark current is insignificant. Hence, the received noise, including shot noise, background noise, and thermal noise, can be modeled as zero-mean additive white Gaussian noise (AWGN) with variance

$$(\sigma_N^U)^2 = (\sigma_{sh}^U)^2 + (\sigma_b^U)^2 + (\sigma_{th}^U)^2, \tag{3.5}$$

where σ_N^U is the standard deviation of the received noise at user U. $(\sigma_s^U)^2$, $(\sigma_b^U)^2$, $(\sigma_{th}^U)^2$ are the variances of the shot noise, background noise, and thermal noise at user U, respectively. These

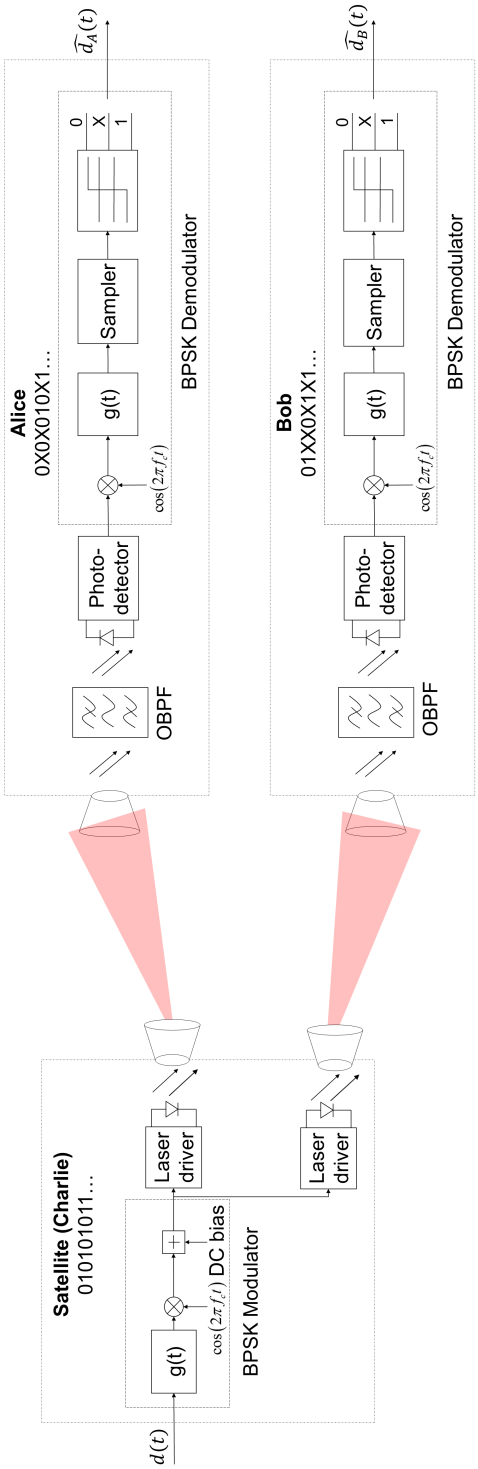


Figure 3.4: The block diagram of the proposed satellite QKD system using SIM/BPSK and DT/DD receivers.

variances are calculated as

$$(\sigma_{sh}^{U})^2 = 2qR_e \left(\frac{1}{4} P \delta h_{\text{e2e}}^{U}\right) \Delta_f, \tag{3.6}$$

$$(\sigma_{b}^{U})^2 = 2qR_e P_b \Delta_f, \tag{3.7}$$

$$(\sigma_{th}^{U})^2 = \frac{4k_B T}{F_n} \Delta_f, \tag{3.8}$$

where q is the electron charge, $P_b = \Omega_r \pi a_U^2 \Delta\lambda$ is the background noise power collected at user U's receivers, Ω_r is the Sun's spectral irradiance from above Earth, a_U is the aperture radius at user U, $\Delta\lambda = \frac{B_0 \lambda^2}{c}$, B_0 is the optical bandwidth, λ is the operating wavelength, c is the speed of light in vacuum, k_B is the Boltzmann's constant, F_n is the amplifier noise figure, $\Delta f = \frac{R_b}{2}$ is the efficient bandwidth with the system bit rate R_b, T is the receiver temperature in Kelvin degree, and R_L is the load resistance.

3.3 Channel Models

The channel state h_{e2e}^{U} between the satellite and the user U can be described as $h_{\text{e2e}}^{U} = h_g^U h_l^U h_a^U$, where h_g^U is the geometric spreading loss, h_l^U is the atmospheric attenuation, and h_a^U is atmospheric turbulence-induced fading. Here, we assume that a fine tracking system [111] with perfect alignment is deployed. Besides, as reported in [112], the maximum frequency shift between an LEO satellite and a fixed ground station is in the order of several GHz. These values are, nonetheless, within the capability of the current receiver design for optical satellite communications, which can deal with the frequency shift up to ± 14 GHz [113]. Therefore, we ignore the Doppler effect in the performance analysis.

3.3.1 Geometric Spreading Loss

Considering Gaussian beams provided by Charlie, the normalized spatial distribution of the transmitted intensity L_{C-U}, which are distances between Charlie to user U, is given as [114]

$$I_{beam}\left(\boldsymbol{\rho}; L_{C-U}\right) = \frac{2}{\pi \omega_{L_{C-U}}^2} \exp\left(-\frac{2\|\boldsymbol{\rho}\|^2}{\omega_{L_{C-U}}^2}\right), \tag{3.9}$$

where $\boldsymbol{\rho}$ is the radial vector from the beam footprint center, $\|.\|$ is the Euclidean norm, $L_{C-U} = (H_C - H_U)/\cos(\zeta_U)$ with H_C and H_U being altitudes of Charlie and user U, respectively, and ζ_U being zenith angles between Charlie and user U. $\omega_{L_{C-U}}$ is the beam radius at distance L_{C-U} and can be computed as $\omega_{L_{C-U}} = \omega_{0,C}\left[1 + \left(\frac{L_{C-U}\lambda}{\pi \omega_{0,C}^2}\right)^2\right]^{1/2}$, where $\omega_{0,C} = \lambda/2\theta_C$ is the beam waist at the transmitter of Charlie, λ is the operation wavelength, and θ_C is the divergence angle of the transmitted beam. The geometric spreading loss with respect to the position vector from the center of the beam footprint $\boldsymbol{r}$ is then given by [115]

$$h_g^U\left(\boldsymbol{r}; L_{C-U}\right) = \int_{A_r^U} I_{beam}\left(\boldsymbol{\rho} - \boldsymbol{r}; L_{C-U}\right) d\boldsymbol{\rho}, \tag{3.10}$$

where $h_g^U(.)$ denotes the fraction of power collected by each user's receiver, whose area is A_r^U. The approximated result of this integration is derived as [115]

$$h_g^U(\boldsymbol{r}; L_{C-U}) \approx A_0^U \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega_{L_{C-U},eq}^2}\right), \tag{3.11}$$

where $\|\boldsymbol{r}\|$ is the radial distance from the center of beam footprint, $A_0^U = [\text{erf}(\nu_U)]$ is the fraction of the collected power at $\boldsymbol{r} = 0$ with $\nu_U = \frac{\sqrt{\pi}a_U}{\sqrt{2}\omega_{L_{C-U}}}$, where a_U is user's receiver radius, and $\omega_{L_{C-U},eq}^2 = \left(\omega_{L_{C-U}}^2 \frac{\sqrt{\pi}\text{erf}(\nu_h)}{2\nu_h \exp(-\nu_h^2)}\right)^{1/2}$ is the equivalent beam radius at distance L_{C-U}.

When each user is placed at the center of Charlie's beam footprint, the fraction of collected power is given as $h_g^U(0; L_{C-U}) \approx A_0^U$.

3.3.2 Atmospheric Attenuation

The atmospheric attenuation is described by the exponential Beer-Lambert's law as

$$h_l^U = \exp(-\xi L_{h-U}), \tag{3.12}$$

where ξ is the attenuation coefficient found in [117]. ξ is determined by

$$\xi(\lambda) = \frac{3.912}{V}\left(\frac{\lambda}{550}\right)^{-q(V)}, V = [\text{km}], \lambda = [\text{nm}] \tag{3.13}$$

where V is the atmospheric visibility. Values of V depend on the weather conditions (e.g., fog, rain, drizzle, clear). Based on the value of V with respect to the considered weather condition, the value of the atmospheric attenuation visibility coefficient $q(V)$ is modeled as

$$q(V) = \begin{cases} 1.6, & V > 50 \text{ km}, \\ 1.3, & 6 \text{ km} < V < 50\text{km}, \\ 0.585V^{1/3}, & V < 6\text{km}. \end{cases} \tag{3.14}$$

As reported in [118], the atmospheric attenuation mainly occurs below the altitude of $H_h = 20$ km, resulting in the propagation distance of each user, i.e., L_{h-U}, is determined as $L_{h-U} = (H_h - H_U)/\cos(\zeta_U)$.

3.3.3 Atmospheric Turbulence-induced Fading

Atmospheric turbulence is a random phenomenon caused by the variation of temperature and pressure of atmosphere along the propagation link. It results in the received optical signal fluctuations at receivers. The strength of turbulence is determined by the Rytov variance, denoted as σ_R^2. The values of σ_R^2 in weak, moderate, and strong turbulence conditions correspond to $\sigma_R^2 < 1$, $\sigma_R^2 \approx 1$, and $\sigma_R^2 > 1$ [119]. For LEO satellite-to-ground links, the turbulence strength is usually weak ($\sigma_R^2 < 1$) with the zenith angles being equal to or less than $60°$[4] [112]. Therefore, to model the signal fluctuation due to atmospheric turbulence-induced fading, we use the log-normal distribution that suits for weak-and moderate-turbulence regimes. The distribution of h_a^U is written as follows [120]

$$f_{h_a^U}(h_a^U) = \frac{1}{\sqrt{8\pi}h_a^U\sigma_X^U}\exp\left(-\frac{\left[\ln(h_a^U) - 2\mu_X^U\right]^2}{8(\sigma_X^U)^2}\right), \tag{3.15}$$

[4]The zenith angles between the satellite and users are always equal to or less than $60°$ as the minimum acceptable elevation angle for satellite tracking is set to $30°$ mentioned in Sec. 3.2.

where μ_X^U and $(\sigma_X^U)^2$ are respectively the mean and variance of log-amplitude fluctuation. The fading coefficient is normalized so that its average value $\mathbb{E}[h_a^U] = 1$ to ensure that the fading does not attenuate or amplify the average power; hence, $\mu_X^U = -(\sigma_X^U)^2$. The variance $(\sigma_X^U)^2$ is given as [120]

$$(\sigma_X^U)^2 = \frac{1}{4}\sigma_R^2 \approx 0.56k^{7/6}\sec^{11/6}(\zeta_U)\int_{H_U}^{H_G} C_n^2(h)(h-H_U)^{5/6}\mathrm{d}h, \tag{3.16}$$

where $k = 2\pi/\lambda$ is the wave number, $\sec(x) = 1/\cos(x)$ is the secant function, and ζ_U is the zenith angle between the satellite and user U. $C_n^2(\mathrm{m}^{-2/3})$ is the refractive index structure parameter modeled by Hufnagel-Valley (H-V) model [120] as follows

$$\begin{aligned} C_n^2(h) = 0.00594\left(\frac{w}{27}\right)^2(10^{-5}h)^{10}\exp\left(-\frac{h}{1000}\right)\exp\left(-\frac{h}{1500}\right) \\ +2.7\times 10^{-16}\exp\left(-\frac{h}{1500}\right)+C_n^2(0)\exp\left(-\frac{h}{100}\right), \end{aligned} \tag{3.17}$$

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.

3.4 Performance Analysis

3.4.1 Sift Probability

3.4.1.1 Sift probability between the satellite and the legitimate user

Sift probability (P_{sift}) between Charlie and the legitimate user U is the probability that the user is able to decode bits using the DT detection. This probability is derived as

$$P_{\text{sift}} = P_{C,U}(0,0)+P_{C,U}(0,1)+P_{C,U}(1,0)+P_{C,U}(1,1), \tag{3.18}$$

where $P_{C,U}(x,y)$ ($x,y \in \{0,1\}$) is the probability that bit "x" sent by Charlie coincides with the decoded bit "y" of user U. $P_{C,U}(x,y)$ is determined by

$$P_{C,U}(x,y) = P_C(x)P_{U|C}(y|x), \tag{3.19}$$

where $P_C(x)$ is the probability that Charlie sends bit "x". We assume that bits "0" and "1" are equally likely to be transmitted from Charlie; hence, $P_C(x) = \frac{1}{2}$. $P_{U|C}(y|x)$ is the conditional probabilities that user U detects bit "y" when Charlie transmits bit "x" and defined as

$$P_{U|C}(0|x) = \int_0^\infty Q\left(\frac{i_x^U - d_0^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{3.20}$$

$$P_{U|C}(1|x) = \int_0^\infty Q\left(\frac{d_1^U - i_x^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{3.21}$$

where $i_0^U = -i_1^U = -\frac{1}{4}R_e P\delta h_{\text{e2e}}^U$ are the received current signals for bit "0" and bit "1", respectively, and $Q(.)$ is the Q-function. The dual threshold (i.e., d_0^U and d_1^U) are determined by

$$d_0^U = \mathbb{E}[i_0^U] - \varsigma_U\sigma_N^U, \tag{3.22}$$

$$d_1^U = \mathbb{E}[i_1^U] + \varsigma_U\sigma_N^U, \tag{3.23}$$

where ς_U is the DT scale coefficient of user U and $\mathbb{E}[.]$ is the expectation operator. Thus, $\mathbb{E}[i_0^U] = -\frac{1}{4}R_e P\delta h_g^U h_l^U$ and $\mathbb{E}[i_1^U] = \frac{1}{4}R_e P\delta h_g^U h_l^U$ as $\mathbb{E}[h_{\text{e2e}}^U] = \mathbb{E}[h_g^U h_l^U h_a^U] = h_g^U h_l^U$ with $\mathbb{E}[h_a^U] = 1$ as the mean irradiance is normalized to unity. Approximate expressions for (4.13) and (4.14) can be derived by using the Gauss-Hermite quadrature. Particularly, by making a change of variable $y = \frac{\ln\left(h_a^U\right)+(\sigma_X^U)^2}{\sqrt{8\pi}h_a^U\sigma_X^U}$, (4.13) and (4.14) are written in the form $\int_{-\infty}^{\infty} g(y)\text{exp}(-y^2)\text{d}y$, where $g(y)$ is a function of the variable y [32]. Then, using the Gauss-Hermite quadrature, this integral is approximated as [121]

$$\int_{-\infty}^{\infty} g(y)\text{exp}(-y^2)\text{d}y \approx \sum_{i=1}^{n}\omega_i g(x_i), \tag{3.24}$$

where n is the order of approximation, while ω_i and x_i are weight factors and zeros of the Hermite polynomial, respectively. It is worth noting that the Gauss-Hermite used for (4.13) and (4.14) quickly converges to the exact-form expressions for a finite value of n, i.e., n = 20 terms.

3.4.1.2 Sift probability between two legitimate users

Sift probability (P_{sift}) between two legitimate users is the probability that both Alice and Bob are able to decode bits using the DT detection. This probability is derived through the joint probabilities as

$$P_{\text{sift}}=P_{A,B}(0,0)+P_{A,B}(0,1)+P_{A,B}(1,0)+P_{A,B}(1,1), \tag{3.25}$$

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

$$P_{A,B}(x,y) = P_C(x)P_{A|C}(x|x)P_{B|C}(y|x) + P_C(y)P_{A|C}(x|y)P_{B|C}(y|y). \tag{3.26}$$

3.4.2 Quantum Bit Error Rate

Similar to the quantum bit error rate (QBER) defined in the conventional QKD protocol, we also use the QBER to reflect the bit error rate in the sifted key. The QBER of the proposed system is given as [32]

$$\text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}}, \tag{3.27}$$

3.4.2.1 QBER between the satellite and the legitimate user

$$P_{\text{error}} = P_{C,U}(0,1) + P_{C,U}(1,0), \tag{3.28}$$

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

3.4.2.2 QBER between two legitimate users

$$P_{\text{error}} = P_{A,B}(0,1) + P_{A,B}(1,0), \tag{3.29}$$

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

An approximate expression for QBER can be achieved by plugging the conditional probabilities' approximations in (A.1) into (4.12), (4.17), (4.25), (4.26), and (4.27).

3.4.3 Eve's error probability

As mentioned in Sec. 3.1, we consider that Eve uses the optimal threshold ($d_t^E = 0$) to detect the received data from the satellite. Eve's error probability (P_{error}^E) is the probability that Eve falsely detects Charlie's transmitted bits. Eve's error probability is calculated as

$$P_{\text{error}}^E = P_{C,E}(0,1) + P_{C,E}(1,0), \tag{3.30}$$

where $P_{C,E}(0,1)$ and $P_{C,E}(1,0)$ are, respectively, the joint probabilities that Eve falsely detects Charlie's transmitted bits, which are expressed as

$$P_{C,E}(0,1) = P_C(0)P_{E|C}(1|0), \tag{3.31}$$

$$P_{C,E}(1,0) = P_C(1)P_{E|C}(0|1), \tag{3.32}$$

where $P_C(x)$ is the probability that Charlie sends bit "x". Additionally, $P_{E|C}(y|x)$ is the conditional probabilities that Eve detects bit "y" given that Charlie transmitted bit "x" and is given as

$$P_{E|C}(1|0) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_t^E - i_0^E}{\sigma_N^E}\right) f_{h_a^E}(h_a^E)\mathrm{d}h_a^E, \tag{3.33}$$

$$P_{E|C}(0|1) = \frac{1}{2}\int_0^\infty Q\left(\frac{i_1^E - d_t^E}{\sigma_N^E}\right) f_{h_a^E}(h_a^E)\mathrm{d}h_a^E, \tag{3.34}$$

where $i_0^E = -i_1^E = -\frac{1}{4}R_e P\delta h_g^E h_l^E h_a^E$ denote the received current signals at Eve. Here, h_g^E, h_l^E, and h_a^E are, respectively, the geometric spreading loss, the atmospheric attenuation-induced fading, and the atmospheric turbulence over Charlie-to-Eve channels, which can be determined in Sec. 3.3. It is noted that the fading channels of legitimate users and Eve are not correlated, contrary to the work in [122]. The reason is that the distance between Eve and legitimate users is in the order of tens of meters. These values are, nonetheless, much greater than the receiver's aperture separation in the case of correlated channels (i.e., in the order of centimeters or shorter) [123]. Besides, using (A.1), approximate expressions for (3.33) and (3.34) can be obtained.

3.4.4 Normalized secret key rate

We assume that an eavesdropper performs URA near each user, as illustrated in Fig. 3.1. Eve_1 (denoted by E_1) is the eavesdropper near Alice. Eve_2 (denoted by E_2) is the eavesdropper near Bob. The normalized secret key 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 Bob can be derived as [108]

$$S = \mu I(A;B) - \max\left[I(A;E_1), I(B;E_2), I(E_1;E_2)\right], \tag{3.35}$$

where $I(A;B)$, $I(A;E_1)$, $I(B;E_2)$, and $I(E_1;E_2)$ are the mutual information between Alice and Bob, Alice and Eve_1, Bob and Eve_2, and Eve_1 and Eve_2, respectively. μ is the error correction efficiency. For the sake of simplicity, we also assume 100% error correction efficiency (i.e., μ = 1) to evaluate the upper bound of the performance of the system performance [108].

We evaluate the above-described mutual information utilizing the following formula [124]

$$I(Y;Z) = \sum_{y,z\in\{0,X,1\}} P_{Y,Z}(y,z)\log_2\left[\frac{P_{Y,Z}(y,z)}{P_Y(y)P_Z(z)}\right], \tag{3.36}$$

In the above expression, $I(Y;Z)$ is the mutual information between Y and Z, $P_Y(y)$ and $P_Z(z)$ are the probabilities that Y and Z detect y and z, respectively. $P_{Y,Z}(y,z)$ is the joint probability that Y's bit y coincides with Z's bit z. We evaluate the joint probability between Alice and Bob, Alice and Eve_1, Bob and Eve_2, and Eve_1 and Eve_2 by using (4.13), (4.14), (4.18), and then evaluate the mutual information by substituting them into (3.36).

Table 3.2: System Parameters

Name	Symbol	Value
LEO Satellite (Charlie)		
Wavelength	λ	1550 nm
Bit rate	R_{b}	1 Gbps
Altitude	H_{C}	550 km
Divergence angle	θ_C	50 μrad
Transmitted power	P	30 dBm
FSO Channel		
Sun's spectral irradiance from above the Earth	Ω_{v}	0.2 $\text{kW}/\text{m}^2\cdot\mu\text{m}$
Wind speed	w	21 m/s
The refractive index structure parameter at the ground level	$C_n^2(0)$	$10^{-15}\text{m}^{-2/3}$
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

3.5 Practical QKD System Design based on Starlink Satellite Constellation

This section investigates the feasibility of our proposed satellite-based QKD system based on the well-known Starlink satellite constellation. In this constellation, nearly 1440 satellites orbiting at 550 km in planes inclined 53 degrees are implemented to provide 24/7 global coverage [125], [126]. For a concrete scenario, we assume that Alice (a fixed user in Aizuwakamatsu City, Fukushima Prefecture, Japan) wants to communicate with Bob securely. LEO satellites in the Starlink constellation play a role as Charlie in the proposed QKD system. These satellites are supposed to equip with optical transmitters for FSO downlink transmission, as depicted in Fig. 3.4. Proper parameter settings for system design are provided, including transmitter's as well as receiver's parameters and operational regions of Bob. Based on these parameter settings, the secret key rate of our proposed QKD system is analyzed.

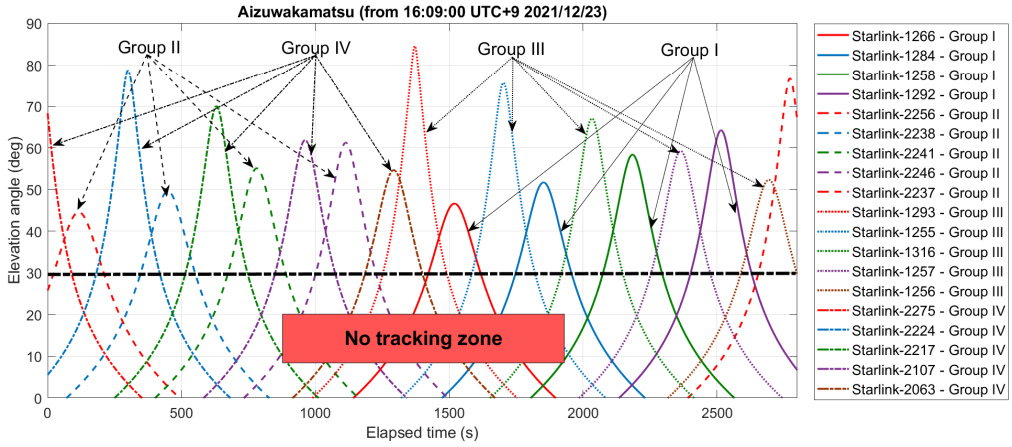


Figure 3.5: Elevation angle of Starlink satellites versus elapsed time from 16:09:00 UTC+9 2021/12/23 over Aizuwakamatsu City, Fukushima Prefecture, Japan. (Calculated from the collected data in [127])

3.5.1 Review of Starlink Satellite Constellation over Japan

Over Japan, there are seven orbital planes of Starlink satellite constellation from northwest to southeast, as shown in Fig. 3.6. Each plane consists of a group of satellites that go across Japan alternatively. Each group is numbered in order for the right to the left respectively, with the orbital planes in Fig. 3.6. With these seven orbital planes of Starlink satellite constellation, there is always a satellite that can be seen by a user locating in Japan with the minimum acceptable elevation angle for tracking is 30°. This argument is proved by Fig. 3.5, which shows the elevation angles versus time of LEO satellites in orbital planes over Japan from 16:09:00 UTC+9 Dec. 23, 2021, with users located in Aizuwakamatsu City (longitude: 139.93899°E, latitude: 37.52266°N; elevation: 209.093 m). In this figure, it is observed that the user can always alternatively see satellites in two groups of two orbital planes, and these two groups are substituted cyclically due to the rotation of the Earth. For example, from 16:09:00 UTC+9 Dec.23, 2021, the user alternatively saw satellites of groups 2 and 4. Then, the user continued to see satellites of groups 1 and 3 following the same template. This process is repeated with other groups of satellites in the above orbital planes in the following time.

As mentioned above, we focus on designing the proposed QKD systems based on the existing LEO satellite constellation over Japan. We aim to find the operational range for Bob so that Alice and Bob can exchange secret keys. Without loss of generality, we consider the second cycle of satellites that Alice can observe from 16:09:00 UTC+9 Dec.23, 2021. After designing the proposed QKD systems with satellites in the second cycle, the same setting can be applied to satellites in the following cycles. As depicted in Fig. 3.5, there are 9 satellites in the second cycle, including Starlink-1293, Starlink-1266, Starlink-1255, Starlink-1284, Starlink-1316, Starlink-1258, Starlink-1257, Starlink-1292, and Starlink-1256. These satellites belong to group I and group III of satellites across Japan. For the sake of simplicity, we consider Starlink-1266 and Starlink-1293 as representers for group I and group III, respectively, and set elapsed time return to 0 at the beginning of the second cycle (i.e., the time that Starlink-1293 started communicating with Alice).

3.5.2 Transmitter Design

In the transmitter design, Eve's basic strategy of unauthorized receiver attack (URA) is considered as we focus on our goal of the proposal's feasibility and the preliminary study on the

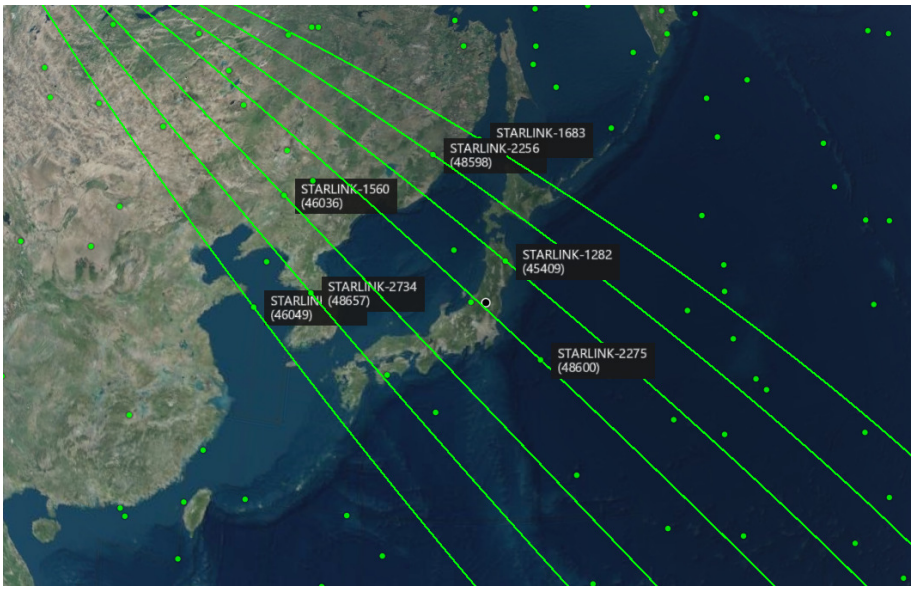


Figure 3.6: Starlink satellites' orbits over Japan [127].

system design. More sophisticated strategies, such as collective attacks, are reserved for future study. In the URA, eavesdroppers (Eve) tries to tap the transmitted signal from the transmitter (i.e., Charlie) by locating their receivers within the beam footprint near legitimate users at a distance d_E m. To prevent URA from happening, we need to select a small modulation depth δ at Charlie so that Eve suffers from a high error rate when she tries to detect the received signal by the optimal threshold $d_t^E = 0$ as mentioned in Sec. 3.1. To carry out this purpose, we investigate in Fig. 3.7, which shows the impact of different values of d_E on P_{error}^E over a range of intensity modulation depth values. In this figure, we consider a minimal propagation distance from Charlie to the legitimate user (i.e., the zenith angle between Charlie and the user is 90 degrees) as a worst-case scenario, where Eve can eavesdrop on the maximum possible information. Other system parameters are provided in Table 3.2. Using Fig. 3.7, we can select a suitable value of intensity modulation depth δ to guarantee that P_{error}^E is sufficiently high. For example, to make sure that $P_{\text{error}}^E > 0.1$, even the distance between Eve and the legitimate user is only 10 meters, the intensity modulation depth should be chosen as $\delta \leq 0.6$. It is noted that higher values of δ lead to higher values of e, while the bit error rate at Alice and Bob is increased with a small value of δ. As a result, we use $\delta = 0.6$ for the transmitter design. From this figure, the analytical results closely follow the simulated ones, which confirms the correctness of the model and analysis.

3.5.3 Receivers' Design

3.5.3.1 Alice design

We assume that Charlie starts the communication with Alice first when the elevation angle between Alice and Charlie is greater than 30°. As shown in Figs. 3.8, 3.9, we can control the sift probability and QBER between Alice and Charlie by adjusting the dual threshold at Alice d_0^A and d_1^A through ς_A, respecting the criteria for receiver design at Alice. In particular, our main target is to control: (1) $P_{\text{sift}} \geq 10^{-3}$ *to guarantee that Alice receives sufficient key information, i.e., to achieve a sifted-key rate at Mbps with the typical transmission rates at Gbps of FSO communications*; (2) QBER $\leq 10^{-3}$ *so that the error is small enough that it can be efficiently corrected at such Mbps of sifted-key rates by error-correcting code*. By using Figs. 3.8(a), 3.9(a), 3.8(b), and 3.9(b), we can define the range of ς_A values to satisfy the requirement for P_{sift} and QBER in case Charlie is Starlink-1293 or Charlie is Starlink-1266, respectively. The

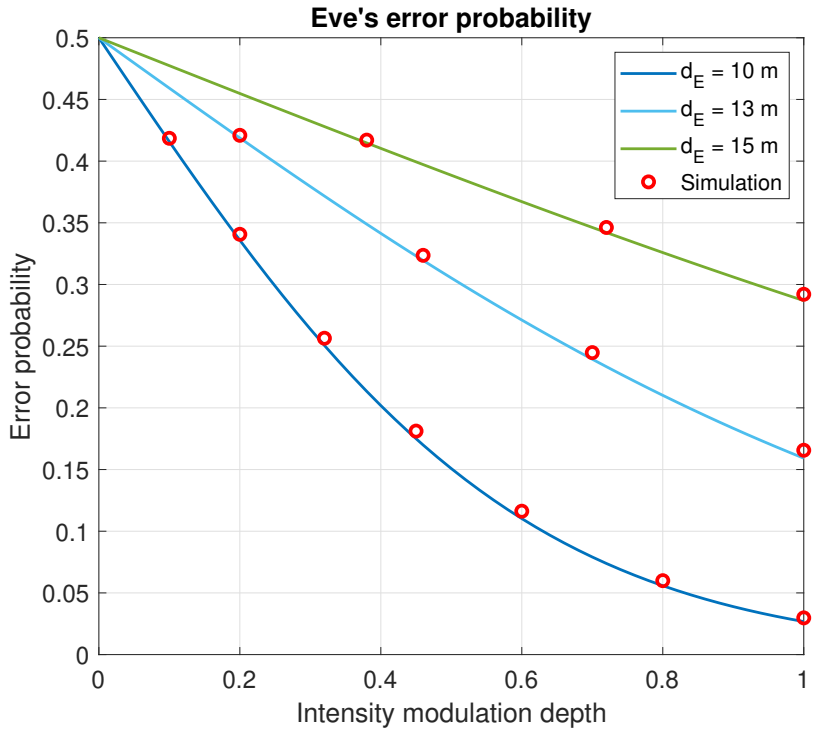
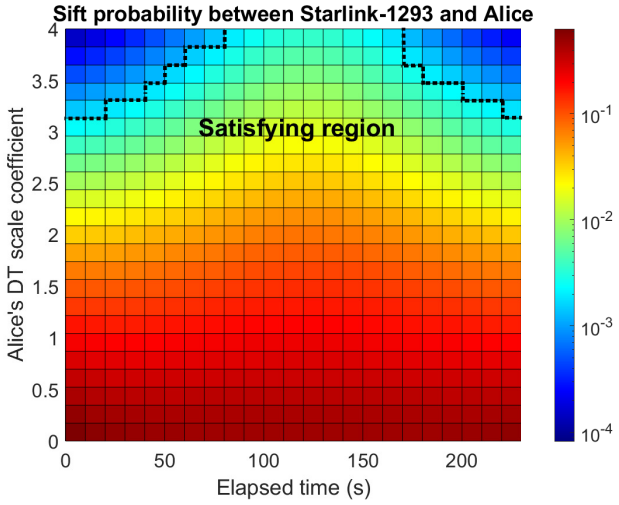


Figure 3.7: Eve's error probability versus intensity modulation depth of the satellite's transmitter.

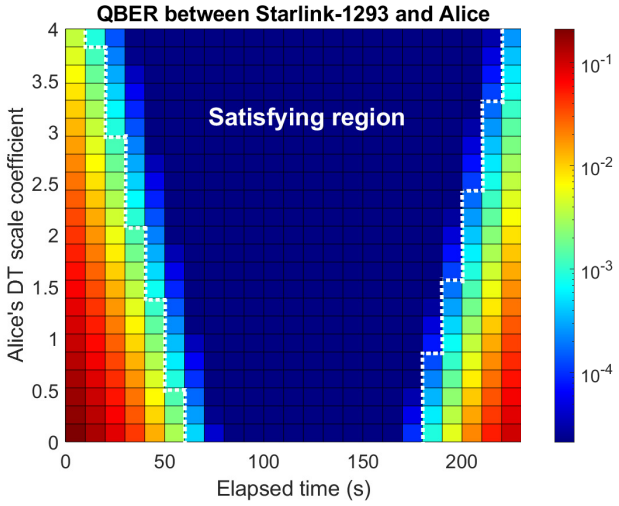
satisfying range of ς_A forms satisfying regions in Figs. 3.8(a), (b) and 3.9(a), (b). Then, by combining these satisfying regions, we can get the operational region of ς_A for Alice to work with Charlie, as shown in Fig. 3.8(c) and Fig. 3.9(c). In the operational region of ς_A, it is recommended that $2.434 < \varsigma_A < 3.304$ if Charlie is Starlink-1293 and $2.737 < \varsigma_A < 3.368$ if Charlie is Starlink-1266. When these settings for ς_A are applied, the communication time can be maximized up to 3 minutes and 2 minutes in the case of Starlink-1293 and Starlink-1266, respectively. Alice can work smoothly when Charlie changes from Starlink-1293 to Starlink-1266 in the cycle if we combine two recommended ranges of ς_A. Thus, the operational range of ς_A at Alice is $2.737 < \varsigma_A < 3.304$.

3.5.3.2 Bob design

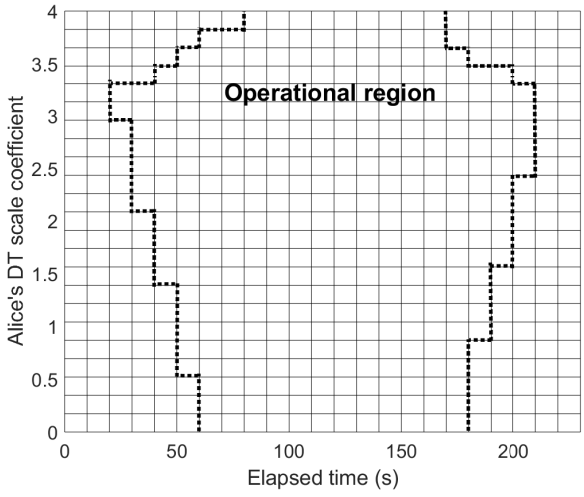
We consider that Bob can be a mobile station (e.g., self-driving cars). The operational area of Bob is determined by each satellite. It is noted that the QKD system, including two legitimate users (Alice and Bob) and the satellite (Charlie), works when both Alice and Bob can see Charlie (i.e., the elevation angle between Alice and Charlie and between Bob and Charlie is greater than 30°). Fig. 3.10(a) and 3.12(a) show the operational area of Bob at the time instant that the elevation angle between each satellite and Alice is maximum. In addition, Figs. 3.10(b) and 3.12(b) show the communication time duration of each location in the operational area of Bob in the case of Starlink-1293 and in the case of Starlink-1266, respectively. The communication time duration is the total time that both Alice and Bob can see Charlie. We assume that the communication time duration among Alice, Bob, and Charlie need to be greater than 180 seconds to implement quantum transmission of the secret key and post-processing procedure. Firstly, when Charlie is Starlink-1293, the greater-180-second communication time duration is bounded by the coverage region, which has an elevation angle greater than 54° as shown in Figs. 3.10(a) and (b) with the pinned location (longitude: 136.781°E, latitude: 39.6871°) on the



(a) $P_{\text{sift}} \geq 10^{-3}$

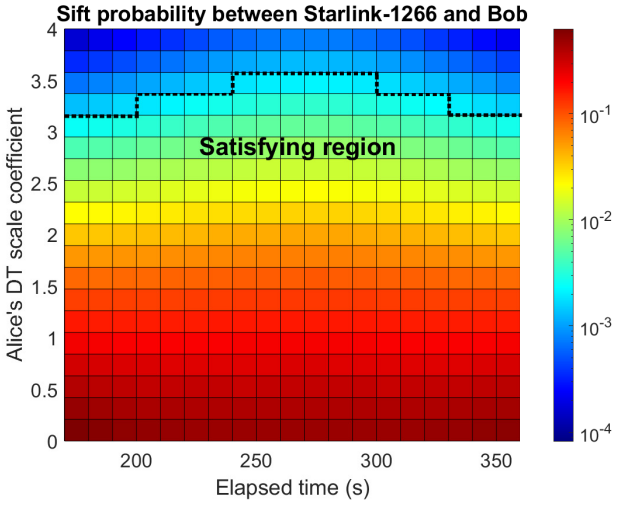


(b) QBER$\leq 10^{-3}$

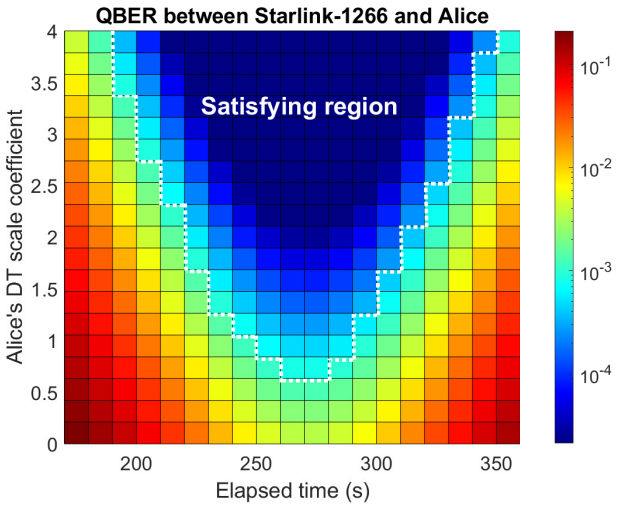


(c) $P_{\text{sift}} \geq 10^{-3}$,QBER$\leq 10^{-3}$

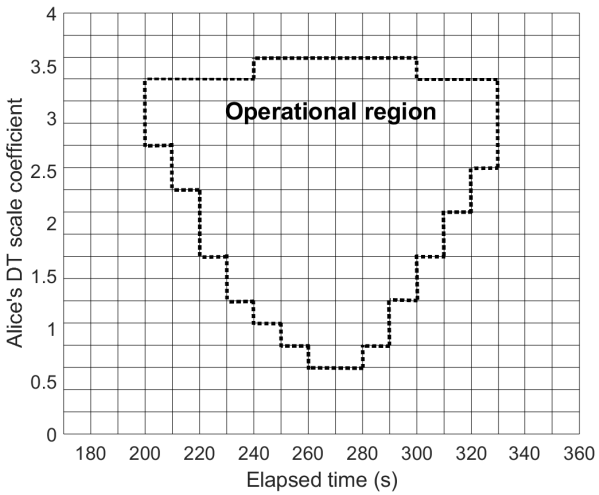
Figure 3.8: P_{sift} and QBER between Starlink-1293 and Alice versus Alice's DT scale coefficient and the elapsed time in seconds.



(a) $P_{\text{sift}} \geq 10^{-3}$

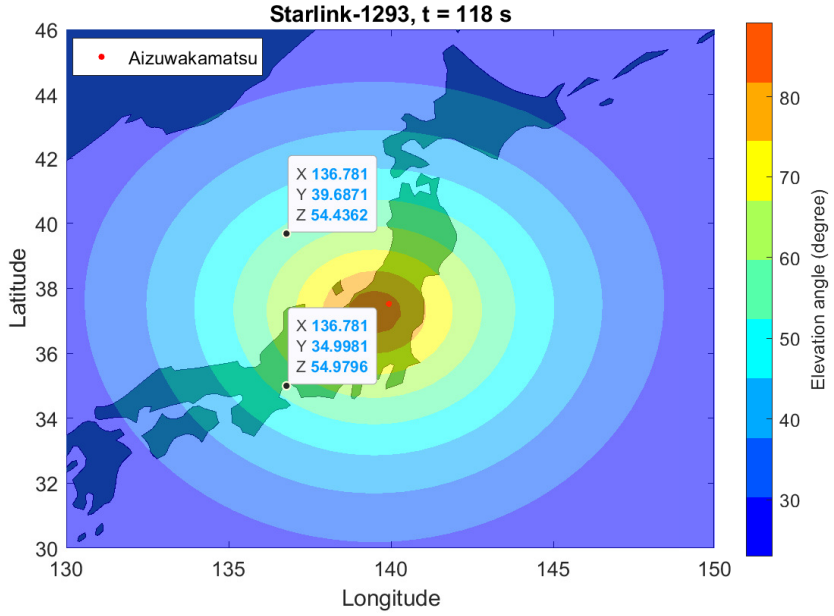


(b) QBER$\leq 10^{-3}$

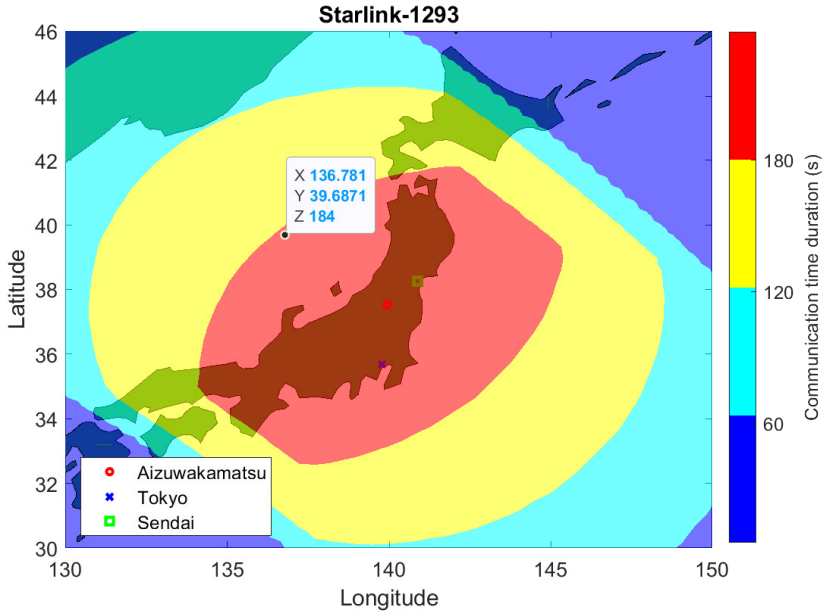


(c) $P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$

Figure 3.9: P_{sift} and QBER between Starlink-1266 and Alice versus Alice's DT scale coefficient and the elapsed time in seconds.

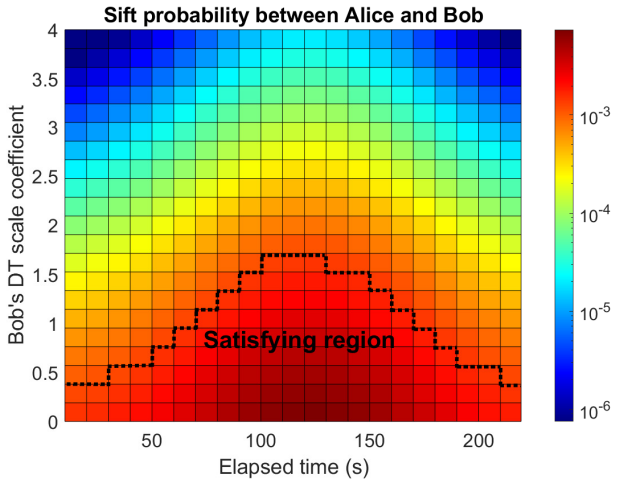


(a) The coverage area of Starlink-1293

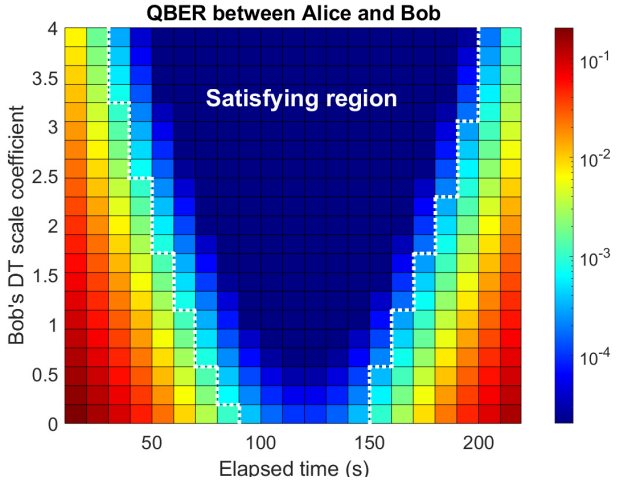


(b) The communication time duration

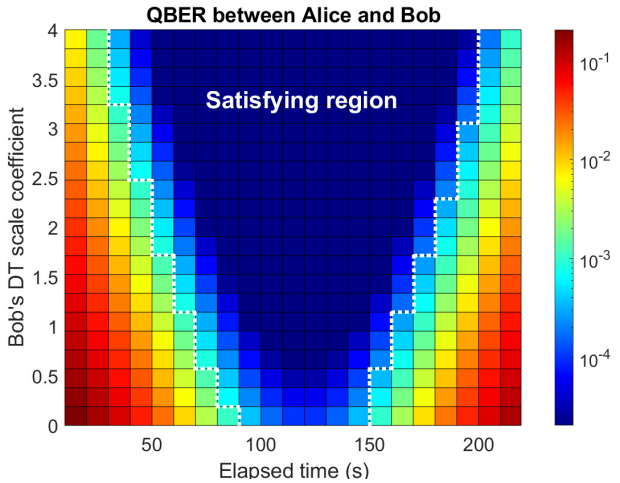
Figure 3.10: The coverage area of Starlink-1293 at time instant that the elevation angle between the satellite and Alice is maximum and the distribution of communication time duration between Bob and Alice (Alice is located in Aizuwakamatsu City).



(a) $P_{\text{sift}} \geq 10^{-3}$



(b) QBER$\leq 10^{-3}$



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

Figure 3.11: P_{sift} and QBER between Alice and Bob versus Bob's DT scale coefficient and the elapsed time in seconds when Charlie is Starlink-1293.

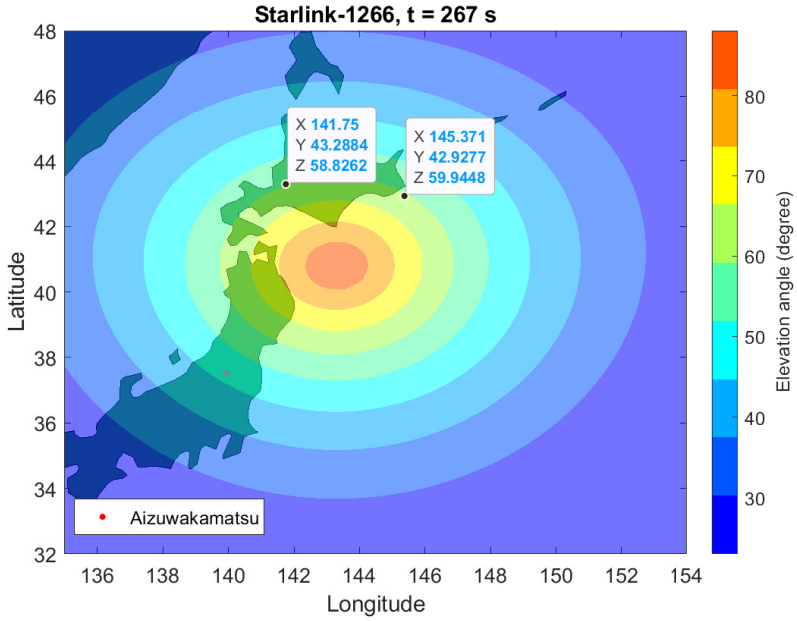
boundary. We consider the other pinned location (longitude: 136.781°E, latitude: 34.9981°) in Fig. 3.10(a), whose elevation angle is also greater than 54° and distance to Alice is farthest, as the boundary for the coverage area of Bob. We then determine the efficient values of Bob's DT scale coefficient (ς_B) so that the proposed QKD system can work properly based on the above design criteria for Alice. To guarantee the requirements of the sift probability and QBER between Alice and Bob, i.e., $P_{\text{sift}} \geq 10^{-3}$ and QBER $\leq 10^{-3}$, we can find the satisfying regions of ς_B as Figs. 3.11(a), (b) when $\varsigma_A = 3$. Then, by combining these satisfying regions, we can get the operational region of ς_B for Bob so that the proposed QKD system can operate, as shown in Fig. 3.11 (c). It is suggested that $0.571 < \varsigma_B < 1.143$ for the longest communication time. The same setting for Bob at the boundary can be used with other locations in Bob's coverage area. Similarly, when Charlie is Starlink-1266, the greater-180-second communication time duration is bounded by the coverage region, which has the elevation angle greater than 58.826° as shown in Figs. 3.12(a) and (b) with the pinned location (longitude: 141.75°E, latitude: 43.2884°) on the boundary. We consider the other pinned location (longitude: 145.371°E, latitude: 42.9277°) in Fig. 3.12(a), whose elevation angle is also greater than 58.826°, and the distance to Alice is farthest as the boundary for the coverage area of Bob. We then determine the efficient values of ς_B so that the proposed QKD system can work properly based on the above design criteria for ς_A. To guarantee the requirements of the sift probability and QBER between Alice and Bob, i.e., $P_{\text{sift}} \geq 10^{-3}$ and QBER $\leq 10^{-3}$, we can find the satisfying regions of ς_B as Figs. 3.13(a), (b) when $\varsigma_A = 3$. Combining these satisfying regions allows us to get the operational region of ς_B for Bob so that the proposed QKD system works properly, as shown in Fig. 3.11(c). It is suggested that $0 < \varsigma_B < 0.632$ for the longest communication time.

3.5.4 Secret Key Rate Performance

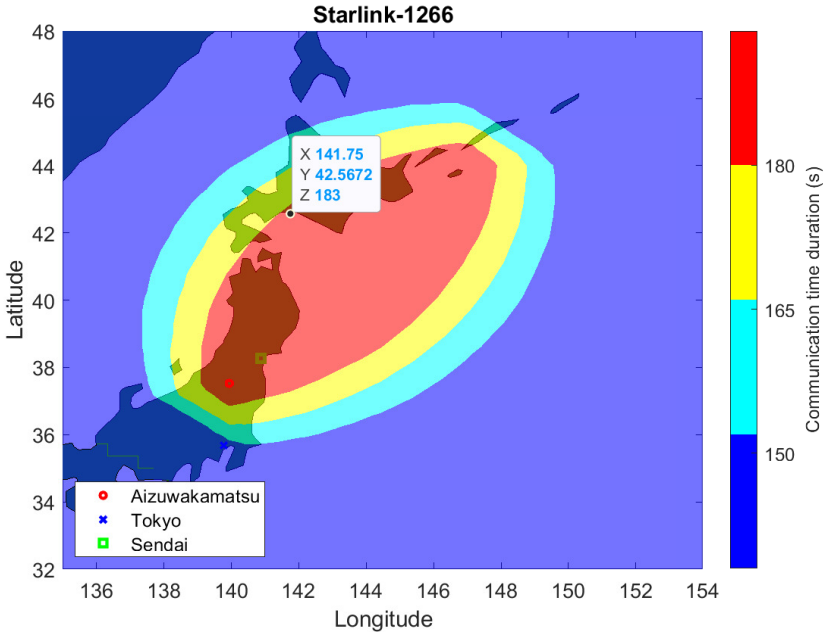
First, we consider the case that Charlie is Starlink-1293 during its operational time duration. Figure 3.14 depicts the spatial distribution of normalized secret key rate (SKR) of the proposed system (the calculation of SKR can be found in 3.4.4) when Alice is located in Aizuwakamatsu City. There is an eavesdropper who performs unauthorized receiver attacks near each user, as illustrated in Fig. 3.1. The distance from the user to the eavesdropper is assumed to be 25 meters. The value of Alice's and Bob's DT scale coefficient is set to 3 and 0.7, respectively. The spatial distribution is shown in three instants: (a) the time that Alice and Bob start receiving secret keys via the quantum channel, (b) the time that the elevation angle between Alice and the satellite is maximum (i.e., the shortest slant path between Alice and the satellite), and (c) the time that the key transmission over the quantum channel from the satellite terminates.

Using these three figures, we can obtain the location of Bob that can keep the high normalized SKR. Specifically, at the beginning of the transmission, the normalized SKR can be up to 0.0014 bit/s/Hz if Bob is in the northwestern region. The normalized SKR gradually decreases from Japan's northwestern region to the southeastern region of the figure. Suppose Bob is in the pale green tier or farther tiers of Japan's southeastern region. In that case, the QKD system can not work effectively due to the negative values of the normalized SKR (i.e., the mutual information between Eve and a legitimate user is greater than the mutual information between Alice and Bob). After that, the light red region, which has a higher normalized SKR than other regions, is moved with the satellite's movement from northwest to southeast. At the time instant when the elevation angle between Alice and the satellite is maximum, the normalized SKR can be up to 0.0043 bit/s/Hz if Bob is in the highest normalized SKR region, covering Kanto and part of the Tohoku and Chubu regions in Japan. These three regions continue to have higher normalized SKRs than other regions until the key transmission terminates.

To investigate the variation of the normalized SKR of the proposed QKD system versus time, the temporal distributions of the normalized SKR if Alice is located in Aizuwakamatsu City and Bob is in four major cities in Japan are shown in Fig. 3.15(a), (b), (c), and (d). It is observed that the normalized SKR of the proposed system always gets the maximum normalized SKR

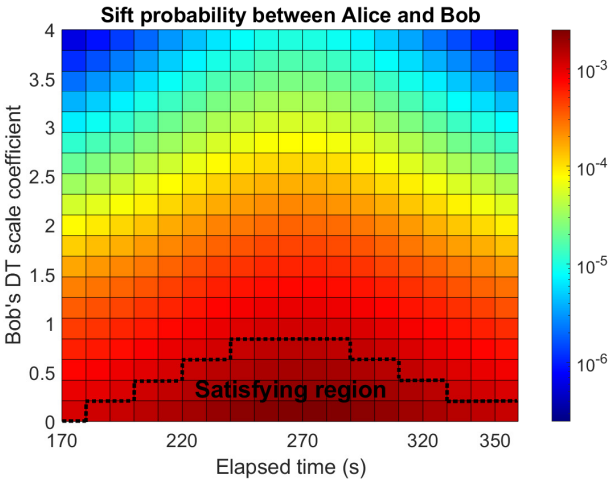


(a) The coverage area of Starlink-1266

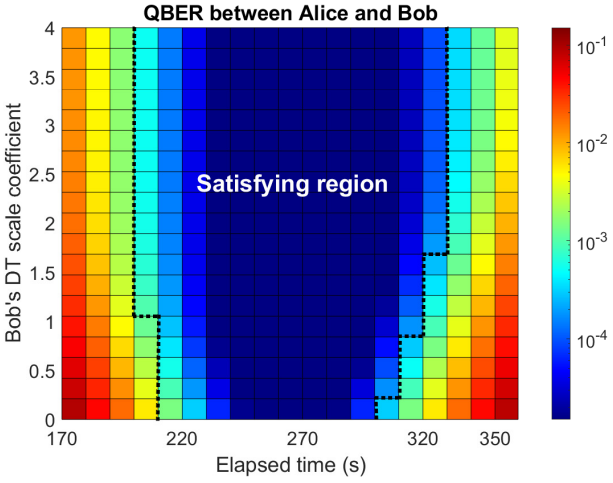


(b) The communication time duration

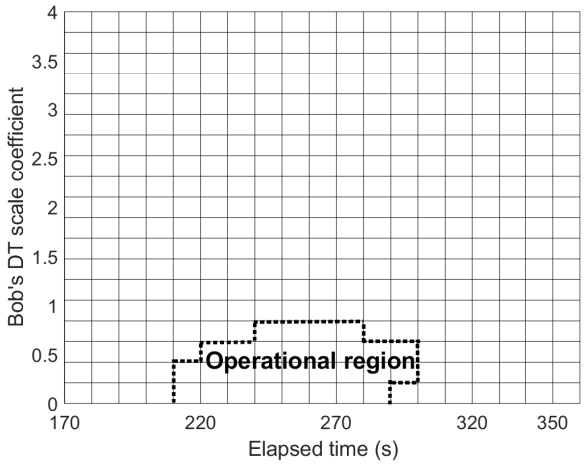
Figure 3.12: The coverage area of Starlink-1266 at time instant that the elevation angle between the satellite and Alice is maximum and the distribution of communication time duration between Bob and Alice (Alice is located in Aizuwakamatsu City).



(a) $P_{\text{sift}} \geq 10^{-3}$

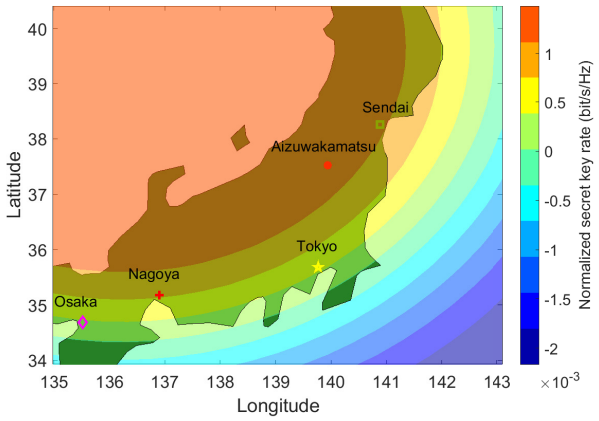


(b) QBER$\leq 10^{-3}$

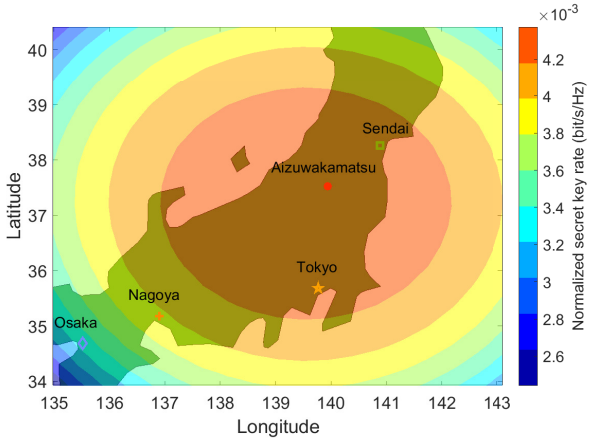


(c) $P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$

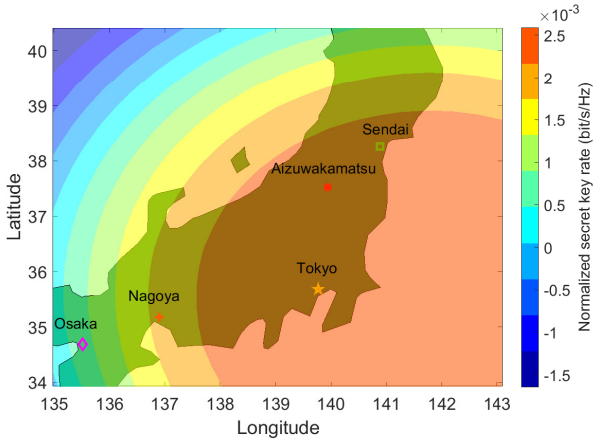
Figure 3.13: P_{sift} and QBER between Alice and Bob versus Bob's DT scale coefficient and the elapsed time in seconds when Charlie is Starlink-1266.



(a) t = 60 s

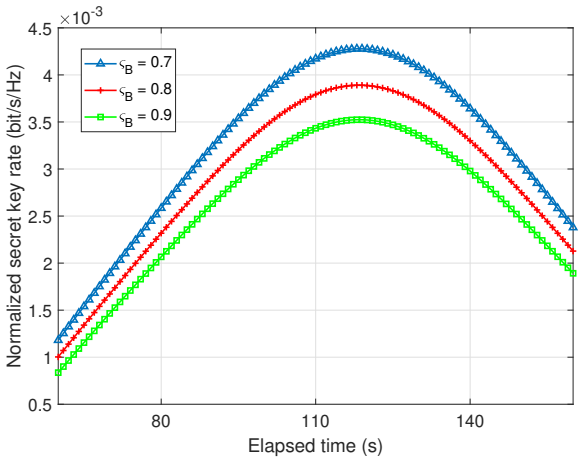


(b) t = 116 s

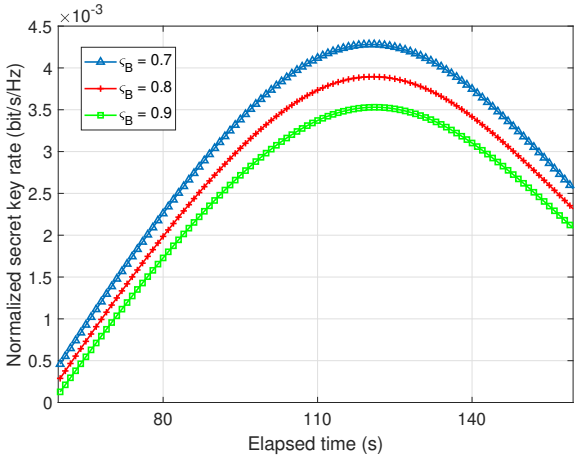


(c) t = 160 s

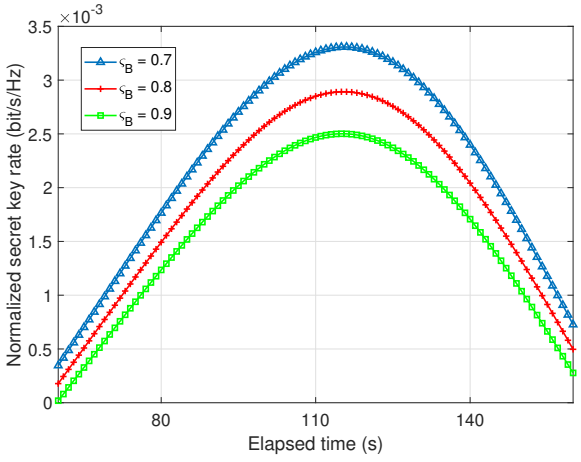
Figure 3.14: The spatial distribution of normalized secret key rate of the proposed QKD system when Charlie is Starlink-1293 during its operational time duration (Alice is located in Aizuwakamatsu City).



(a) Bob is in Sendai



(b) Bob is in Tokyo



(c) Bob is in Osaka

Figure 3.15: The temporal distribution of normalized secret key rate of the proposed QKD system when Charlie is Starlink-1293 during its operational time duration (Alice is located in Aizuwakamatsu City).

in the middle of operational time duration. For example, if Bob is in Sendai, the maximum of the normalized SKR is 0.004277 bit/s/Hz when the elapsed time is 118 seconds. The maximum normalized SKR of the proposed QKD system also depends on the distance between Alice and Bob. Moreover, if the value of ς_B increases, the normalized SKR is decreased. Specifically, the maximum normalized SKR is decreased to 0.00389 bit/s/Hz when ς_B increases from 0.7 to 0.8, as shown in Fig. 3.15(a).

3.6 Conclusions

We presented a design framework for the design criteria of the satellite-based QKD system implementing the non-coherent CV-QKD protocol using DT/DD receivers inspired by the BBM92 protocol for EB scheme to distribute secret keys to legitimate users. The proposed QKD system was realized by the existing LEO satellite constellation over Japan. Our proposed protocol was designed to achieve QKD function with a simplified and low-cost implementation, which helps to enable the worldwide mass deployment of QKD. Based on numerical results, the operational regions for the satellite and legitimate users' parameters are derived. The normalized secret key rates of the proposed system over the atmospheric channel are also given to show the feasibility of the system design.

Chapter 4

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

This chapter[1] proposes a design of a global-scale satellite-based FSO/QKD systems using a GEO satellite as a secret key source and LEO satellites as trusted relay nodes to amplify and forward the signal from the source to multiple legitimate users on Earth. The non-coherent CV-QKD protocol with DT/DD receivers inspired by the BBM92 protocol for EB scheme is employed. The system performance is analyzed, 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 using the existing GEO and LEO satellite constellation. In addition, we investigate the secret-key rate performance of the proposed system and perform M-C simulations to verify analytical results.

4.1 System Descriptions

4.1.1 System Model

Figure 4.1 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$_i$, $i \in \{1, 2 \dots N\}$, 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°.

We consider the scenario in which Eavesdroppers (Eves) can compromise the system by attempting URA or BSA, as shown in Fig. 4.1. 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

[1]The content of this chapter was presented in part in

1. Minh Q. Vu *et al.*,"A Proposal of satellite-based FSO/QKD system for multiple wireless users," *IEICE International Conference on Emerging Technologies for Communications (ICETC),* Waseda, Japan, Nov. 2022.
2. Minh Q. Vu *et al.*,"Design of satellite-based FSO/QKD systems using GEO/LEOs for multiple wireless users," in *IEEE Photonics Journal,* vol. 15, no. 4, pp. 1-14, Aug. 2023, Art no. 7303314.

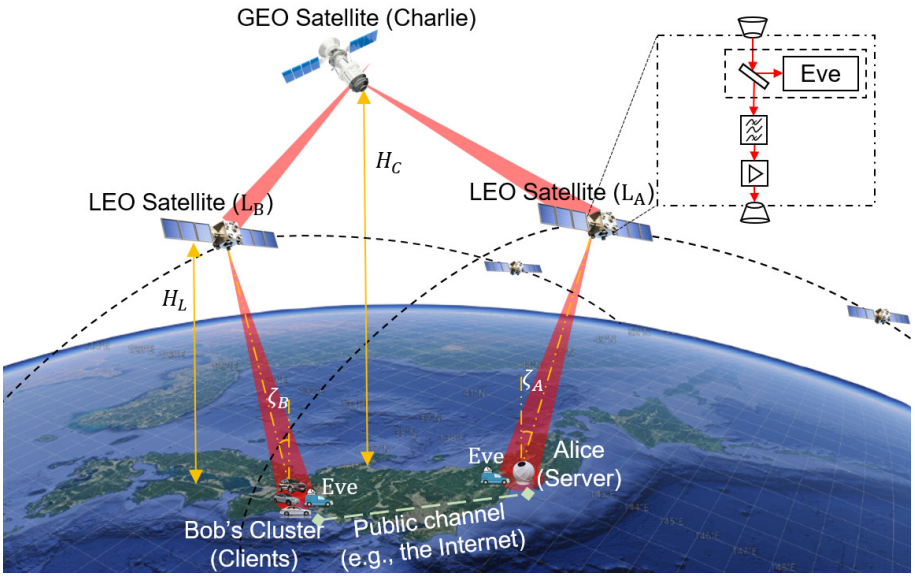


Figure 4.1: The proposal of satellite-based FSO/QKD system using GEO and LEO satellites. (Map data: Google Earth)

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.

4.1.2 Non-Coherent CV-QKD Scheme Inspired by BBM92

In this section, the implementation of non-coherent CVQKD inspired by the BBM92 protocol is reviewed and applied it to the new scenario of this chapter 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.
- **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)

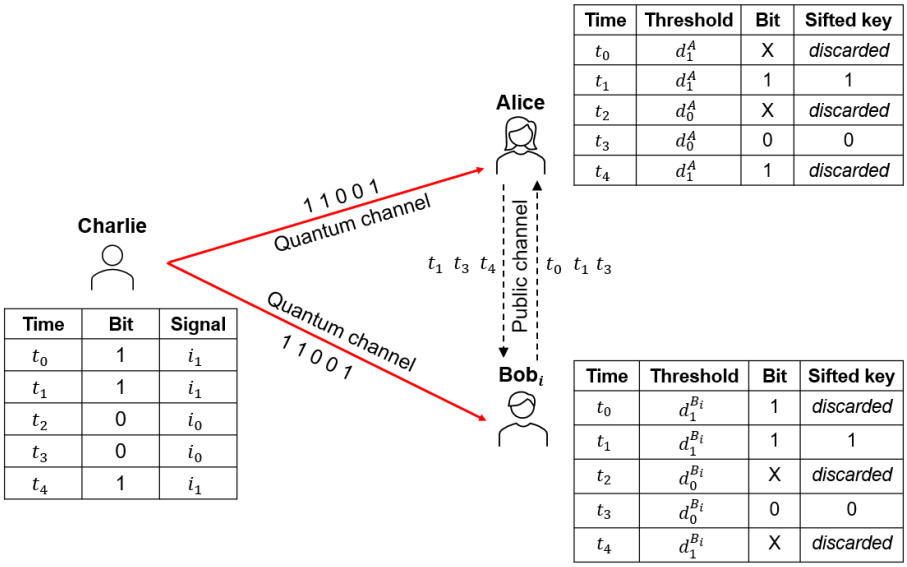


Figure 4.2: An example of non-coherent CV-QKD inspired by the BBM92 protocol for EB scheme.

- **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. 4.2.
- **Post-processing:** Alice and Bob$_i$ perform error correction and privacy amplification to turn the sifted key into a *final shared secret key*.

4.1.3 Signal Model

The block diagram of the proposed system is illustrated in Fig. 4.3. 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

$$P_s(t) = \frac{P}{2}\left[1 + \delta m\left(t\right)\right], \tag{4.1}$$

where P is the peak laser power, δ is the intensity modulation depth, and $m(t)$ is the subcarrier signal [128].

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

$$i_p^U(t) = \frac{1}{2} R_e P G_a h_{\text{e2e}}^U\left(t\right)\left[1 + \delta m\left(t\right)\right] + n_{\text{e2e}}^U\left(t\right), \tag{4.2}$$

where R_e is the responsivity of the photodetector, G_a is the EDFA gain at the LEO satellite,

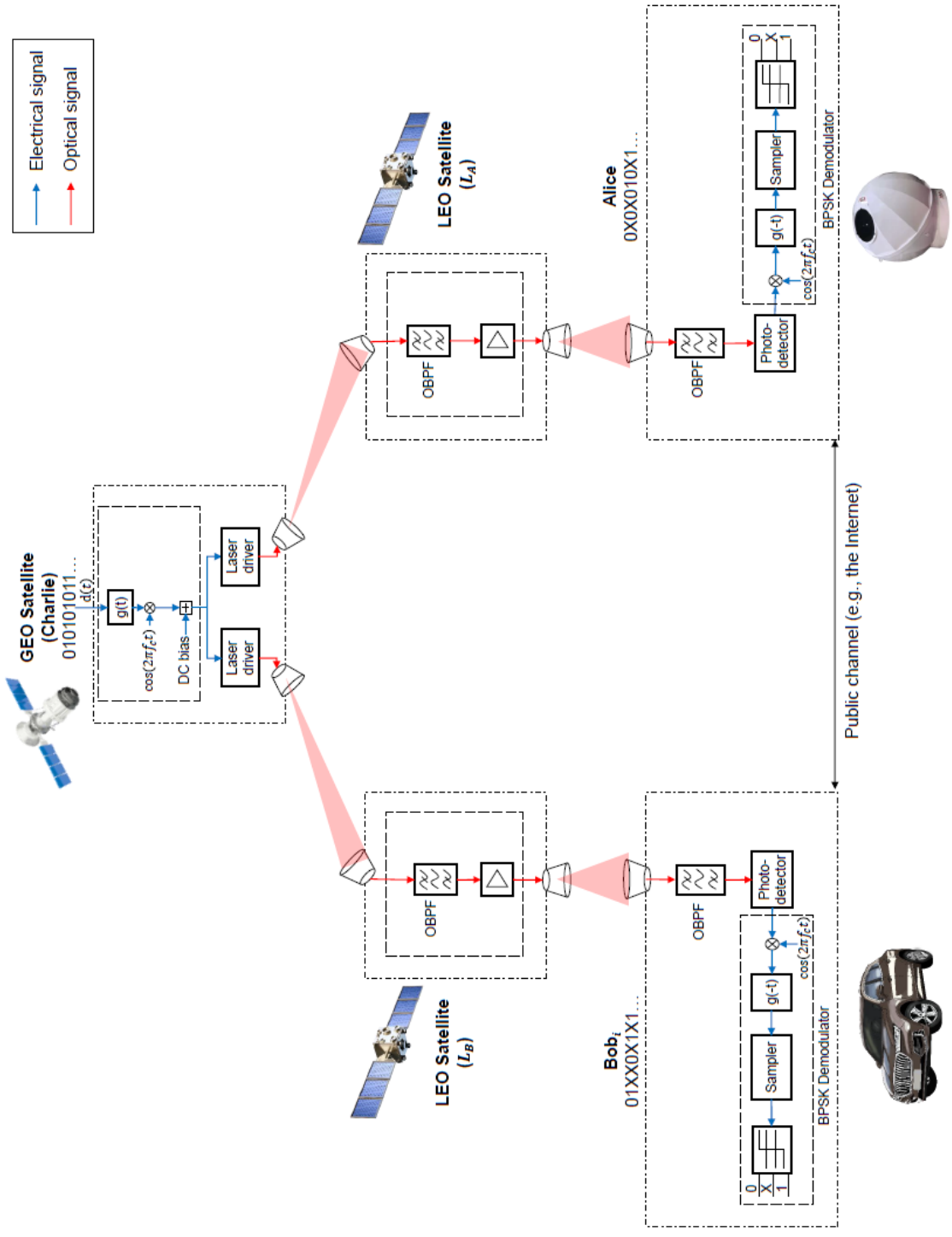


Figure 4.3: The block diagram of the proposed satellite-based GEO/LEO satellite FSO/QKD system.

$h^U_{\text{e2e}}(t)$ are the channel state between Charlie and user U, and $n^U_{\text{e2e}}(t)$ is the receiver noise.

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

$$r^U_d(t) = \begin{cases} i^U_0 = -\frac{1}{4} R_e P \delta G_a h^U_{\text{e2e}}(t) + n^U_{\text{e2e}}(t) \\ i^U_1 = \frac{1}{4} R_e P \delta G_a h^U_{\text{e2e}}(t) + n^U_{\text{e2e}}(t) \end{cases}, \tag{4.3}$$

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

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

$$(\sigma^U_N)^2 = (\sigma^U_{\text{sh}})^2 + (\sigma^L_b)^2 + (\sigma^U_b)^2 + (\sigma^L_a)^2 + (\sigma^U_{\text{th}})^2, \tag{4.4}$$

where $(\sigma^L_b)^2 = 2qR_e P^L_b h_U \Delta_f$ and $(\sigma^L_a)^2 = 2q\Re P^L_a h^U_L \Delta_f$ are variances of the amplified background noise from the LEO satellite and the ASE noise, respectively. $(\sigma^U_{\text{sh}})^2 = 2qR_e \left(\frac{1}{4} P \delta G_a h^U_{\text{e2e}}\right) \Delta_f$, $(\sigma^U_b)^2 = 2qR_e P^U_b \Delta_f$, $(\sigma^U_{\text{th}})^2 = \frac{4k_B T}{F_n} \Delta_f$ 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^U_L is the channel state between the LEO satellite and user U. $P^L_b = \Omega_l \pi a^2_L \Delta\lambda$ is the background noise power collected at the LEO satellite, $P^U_b = \Omega_r \pi a^2_U \Delta\lambda$ 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. $P^L_a = \frac{hc}{\lambda}(n_{\text{sp}} - 1) G_a B_0$ 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. 5.1.

4.1.4 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 the same bit sequence to Alice and all users Bob$_i$. As mentioned in Sec. 3.1, 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.

Figure 4.4 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.

4.2 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.

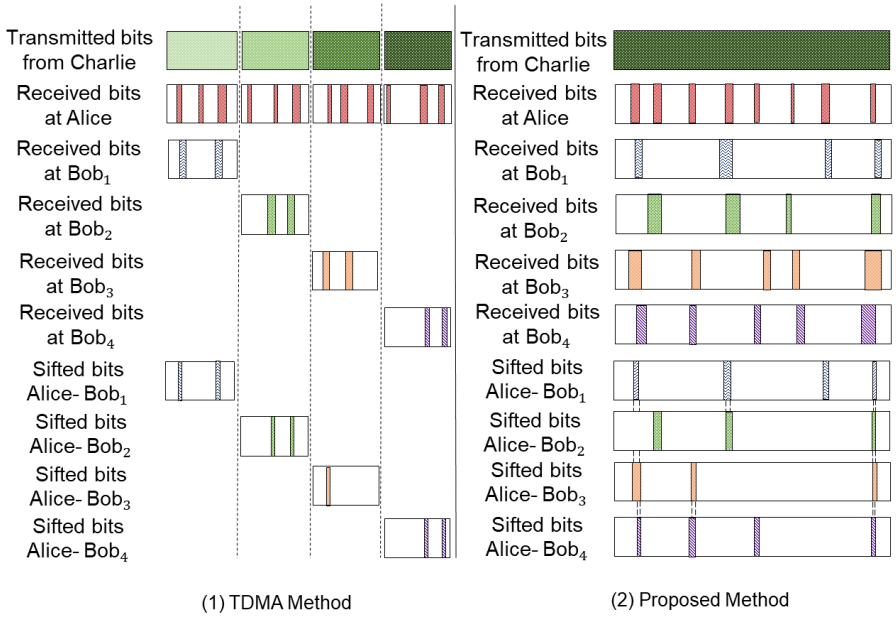


Figure 4.4: Conventional TDMA and our proposed approach for the key distribution with $N = 4$.

4.2.1 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 [112]. In addition, we assume that a fine tracking system with perfect alignment is equipped [111]. 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 [112]. 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 [128]

$$h_G^U = h_{g_1}^U\left(\boldsymbol{r}; L_C\right) = \int_{A_r^Z} I_{beam}\left(\boldsymbol{\rho} - \boldsymbol{r}; L_C\right) d\boldsymbol{\rho}, \tag{4.5}$$

where $I_{beam}\left(.\right)$ is the normalized spatial distribution of the transmitted intensity. $h_{g_1}^U(.)$ denotes the fraction of power collected by each LEO satellite's receiver with the receiving area of $A_r^Z, Z \in \{L_A, L_B\}$. 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 [129].

The approximated result of this integration is given as [115]

$$h_{g_1}^U\left(\boldsymbol{r}; L_C\right) \approx A_0^Z \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega_{L_C,eq}^2}\right), \tag{4.6}$$

where $\|\boldsymbol{r}\|$ is the radial distance from the center of beam footprint, $A_0^Z = [\text{erf}(\nu_Z)]$ 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 tele-

scope aperture, and $\omega_{L_C,eq}^2 = \left(\omega_{L_C}^2 \frac{\sqrt{\pi}\text{erf}(\nu_Z)}{2\nu_Z \exp(-\nu_Z^2)}\right)^{1/2}$ is the equivalent beam radius at distance L_C. ω_{L_C} is the beam radius at distance L_C and is given as $\omega_{L_C} = \omega_{0,C}\left[1 + \left(\frac{L_C\lambda}{\pi\omega_{0,C}^2}\right)^2\right]^{1/2}$, where $\omega_{0,C} = \lambda/2\theta_C$ is the beam waist at the transmitter of C, λ is the operation wavelength, and θ_C is the divergence angle of the transmitted beam. ω_{L_C} is the beam radius at distance L_C and is given as $\omega_{L_C} = \omega_{0,C}\left[1 + \left(\frac{L_C\lambda}{\pi\omega_{0,C}^2}\right)^2\right]^{1/2}$, 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 [116].

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 $h_{g_1}^U(0; L_C) \approx A_0^Z$.

4.2.2 LEO-to-User Channel Model

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

4.2.2.1 Geometric spreading loss

We consider the Gaussian beam model for the laser beam from LEO satellites. With a similar approach in Sec. 4.2.1, the fraction of power collected by the user U's receiver is approximated as

$$h_{g_2}^U(\boldsymbol{r}; L_Z) \approx A_0^U \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega_{L_Z,eq}^2}\right), \tag{4.7}$$

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 [130]. $A_0^U = [\text{erf}(\nu_U)]$ 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 user U's receiver radius. $\omega_{L_Z} = \omega_{0,Z}\left[1 + \left(\frac{L_Z\lambda}{\pi\omega_{0,Z}^2}\right)^2\right]^{1/2}$, 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 [116]. $\omega_{L_Z,eq}^2 = \left(\omega_{L_Z}^2 \frac{\sqrt{\pi}\text{erf}(\nu_U)}{2\nu_U \exp(-\nu_U^2)}\right)^{1/2}$ 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 $h_{g_2}^U(0; L_Z) \approx A_0^U$.

4.2.2.2 Atmospheric attenuation

The attenuation of laser power through the atmosphere is formulated by the exponential Beer-Lambert's law as

$$h_l^U = \exp(-\xi L_U), \tag{4.8}$$

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 [118]. ξ is the attenua-

tion coefficient, and determined as [117]

$$\xi(\lambda) = \frac{3.912}{V[\text{km}]} \left(\frac{\lambda[\text{nm}]}{550} \right)^{-q(V)}, \tag{4.9}$$

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 [121].

4.2.2.3 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 [**?**]. This phenomenon ultimately results in fading of the received optical power, thus leading to system performance degradation. As reported in [112], 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 is set to 30°). Therefore, the distribution of h_a^U can be modeled as a log-normal distribution that suits the weak turbulence regime. It can be formulated as [115]

$$f_{h_a^U}(h_a^U) = \frac{1}{\sqrt{8\pi} h_a^U \sigma_X^U} \exp\left(- \frac{\left[\ln(h_a^U) - 2\mu_X^U\right]^2}{8(\sigma_X^U)^2} \right), \tag{4.10}$$

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 [120]

$$(\sigma_X^U)^2 = 0.56 k^{7/6} \sec^{11/6}(\zeta_U) \int_{H_U}^{H_h} C_n^2(h) (h - H_U)^{5/6} \mathrm{d}h, \tag{4.11}$$

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

4.3 Performance Analysis

This section presents the analytical framework to analyze the performance of the proposed system using 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.

4.3.1 Sift Probabilities

4.3.1.1 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

$$P_{\text{sift}}^{C,U} = P_{C,U}(0,0) + P_{C,U}(0,1) + P_{C,U}(1,0) + P_{C,U}(1,1), \tag{4.12}$$

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 probabilities that Charlie transmits bit "x" when user U detects bit "y" and calculated as [32]

$$P_{U|C}(0|x) = \int_0^\infty Q\left(\frac{i_x^U - d_0^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{4.13}$$

$$P_{U|C}(1|x) = \int_0^\infty Q\left(\frac{d_1^U - i_x^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{4.14}$$

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

$$d_0^U = \mathbb{E}[i_0^U] - \varsigma_U \sigma_N^U, \tag{4.15}$$
$$d_1^U = \mathbb{E}[i_1^U] + \varsigma_U \sigma_N^U, \tag{4.16}$$

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.

4.3.1.2 Multiple-user sift probability

4.3.1.2.1 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

$$P_{AB_i}^{\text{sift}} = P_{AB_i}(0,0) + P_{AB_i}(0,1) + P_{AB_i}(1,0) + P_{AB_i}(1,1), \tag{4.17}$$

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

$$P_{AB_i}(x,y) = P_C(x)P_{A|C}(x|x)P_{B_i|C}(y|x) + P_C(y)P_{A|C}(x|y)P_{B_i|C}(y|y). \tag{4.18}$$

4.3.1.2.2 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. 4.5 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.

$$P_{AB_i}^{\text{sift-excl}} = P(AB_i) - \varepsilon P(AB_i)_{\text{excl}}, \tag{4.19}$$

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

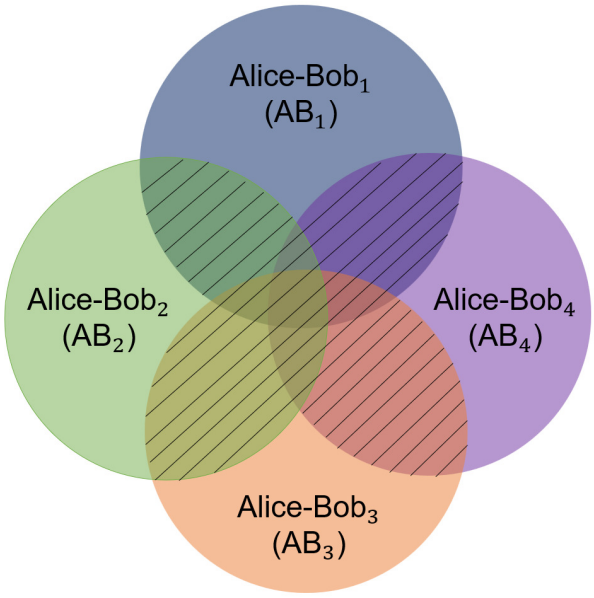


Figure 4.5: Visualization for the relationship of sift probabilities between Alice and Bob$_i$, $i \in \{1,2,3,4\}$. The overlapping region is marked by diagonal stripes.

bits are excluded. $P(AB_i)_{\text{excl}}$ can be calculated as

$$P(AB_i)_{\text{excl}} = \sum_{1\le j\le N} P(AB_i \cap AB_j) - \sum_{1\le j\le k\le N} P(AB_i \cap AB_j \cap AB_k) + (-1)^N P(\bigcap_{i=1}^{N} AB_i), \quad (4.20)$$

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

$$\begin{aligned} P(AB_i \cap AB_j) = & P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(0,0,1) + P_{AB_iB_j}(0,1,0) + P_{AB_iB_j}(0,1,1) \\ & + P_{AB_iB_j}(1,0,0) + P_{AB_iB_j}(1,0,1) + P_{AB_iB_j}(1,1,0) + P_{AB_iB_j}(1,1,1), \end{aligned} \quad (4.21)$$

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

$$\begin{aligned} P_{AB_iB_j}(x,y,z) = & \; P_C(x) P_{A|C}(x|x) P_{B_i|C}(y|x) P_{B_j|C}(z|x) \\ & + P_C(y) P_{A|C}(x|y) P_{B_i|C}(y|y) P_{B_j|C}(z|y). \end{aligned} \quad (4.22)$$

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 $P_{B_j|C}(y|x)$, $x \neq y, x, y \in \{0,1\}$ 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. (5.18) can be rewritten as

$$P(AB_i \cap AB_j) \approx P_{AB_iB_j}(0,0,0) + P_{AB_iB_j}(1,1,1) = P_{A|C}(0|0) \left[P_{B_i|C}(0|0)\right]^2. \quad (4.23)$$

From Eq. (4.23), we can simplify Eq. (5.17) as follows

$$P(AB_i)_{\text{excl}} \approx \sum_{k=0}^{N-2} (-1)^k C_{N-1}^{k+1} P_{A|C}(0|0) \left[P_{B_i|C}(0|0)\right]^{k+2}, \tag{4.24}$$

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.

4.3.2 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 [128]

$$\text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}}. \tag{4.25}$$

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

4.3.2.1 QBER between Charlie and the legitimate user

$$P_{\text{error}} = P_{C,U}(0,1) + P_{C,U}(1,0), \tag{4.26}$$

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

4.3.2.2 QBER between two legitimate users

$$P_{\text{error}} = P_{AB_i}(0,1) + P_{AB_i}(1,0), \tag{4.27}$$

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 (A.1) into (4.12), (4.17), (4.25), (4.26), and (4.27).

4.3.3 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), and Eve$_1$ and Eve$_2$, respectively. All of them can be determined by

$$I(Y;Z) \;=\; \sum_{y,z\in\{0,X,1\}} P_{YZ}(y,z) \log_2 \left[\frac{P_{YZ}(y,z)}{P_Y(y)P_Z(z)}\right], \tag{4.28}$$

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

$$R_i^f = R_i^s [\alpha I(A;B_i) - \max(I(A;E_1), I(B_i;E_2), I(E_1;E_2))] , \tag{4.29}$$

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 paper, we assume perfect error correction efficiency, i.e., $\alpha = 1$, as an upper bound evaluation of the system performance [108].

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

4.4 Two-Layer Satellite FSO/QKD System Design

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

4.4.1 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 [131], is employed as Charlie. Due to the capability of 24/7 global coverage, Starlink satellites are chosen to be the relay nodes [132]. Illustrations of Himawari-8's position and orbits of two Starlink satellites (Starlink-1293 and Starlink-2063) over Japan on December 23$^{\text{rd}}$, 2021 are calculated from the available TLE data in [127] and displayed in Fig. 4.6. All satellites are supposed to be equipped with optical devices necessary for the proposed system shown in Fig. 4.3.

There are seven orbital planes of the Starlink satellite constellation from northwest to southwest of Japan, as shown in Fig. 4.7. 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 Figs. 4.8a and 4.8b, 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. 5.1. 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. 5.1, 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".

Table 4.1: 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
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

4.4.2 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 $d_{\mathrm{t}}^{\mathrm{E}} = 0$[2]. Fig. 4.9 illustrates the error probabilities at Eves as a function of δ for different values of d_{E}. Simulation parameters are listed in Table. 5.1. We consider the worst-case scenario where the relay satellites are closest to legitimate users (i.e., the zenith angle is 0

[2] $P_{\mathrm{error}}^{\mathrm{E}}$ can be derived in the similar way as in [128].

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 $P_{\text{error}}^{\text{E}} > 0.1$ 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 QBER [32]. 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. Figure 4.10 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 the further analysis as the lower bound on the performance of BSA detection.

4.4.3 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.

4.4.3.1 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 Figs. 4.11 (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, Figs. 4.11a, 4.11b, and 4.11c 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 1293s, any value between 0 and 4 can be chosen for ς_A.

In addition to the above requirements, Alice should also 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. 4.12, 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. 4.13 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 (4.12). Thus, according to the central limit theorem [133], $P_{\text{sift}}^{C,A}$ 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 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. 4.14 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. 4.2. Here, it can be seen that increasing d_{BSA} results in higher percentages of 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. 4.12), 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. 4.11a, 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.

Table 4.2: 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%

4.4.3.2 Bob's 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 Figs. 4.15a, 4.15b, and 4.15c, 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. 4.16. Therefore, $\varsigma_{B_i} = 2.25$ is chosen to maximize the sift probability between Alice and Bob$_i$.

4.4.4 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 assume that there are two eavesdroppers performing URAs at Alice's and Bob cluster's locations as depicted in Fig. 4.1. 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. 4.17 illustrates the total final-key creation rates of all users $R^f_{\sum}$ versus the exclusion ratio coefficient ε at different elapsed time instances that Charlie transmits the signal to the relays. The number of users at Bob's cluster is $N = 4$. It is observed that $R^f_{\sum}$ 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., $\varepsilon = 1$). $R^f_{\sum}$ 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, $R^f_{\sum}$ 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. 4.18 investigates $R^f_{\sum}$ 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 $R^f_{\sum}$ keeps unchanged when the number of users increases. In the proposed method, 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. 4.15c, leading to an increase in $R^f_{\sum}$ at the optimal number of users.

4.5 Conclusions

This chapter 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 using DT/DD receivers inspired by the BBM92 protocol for EB scheme were 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.

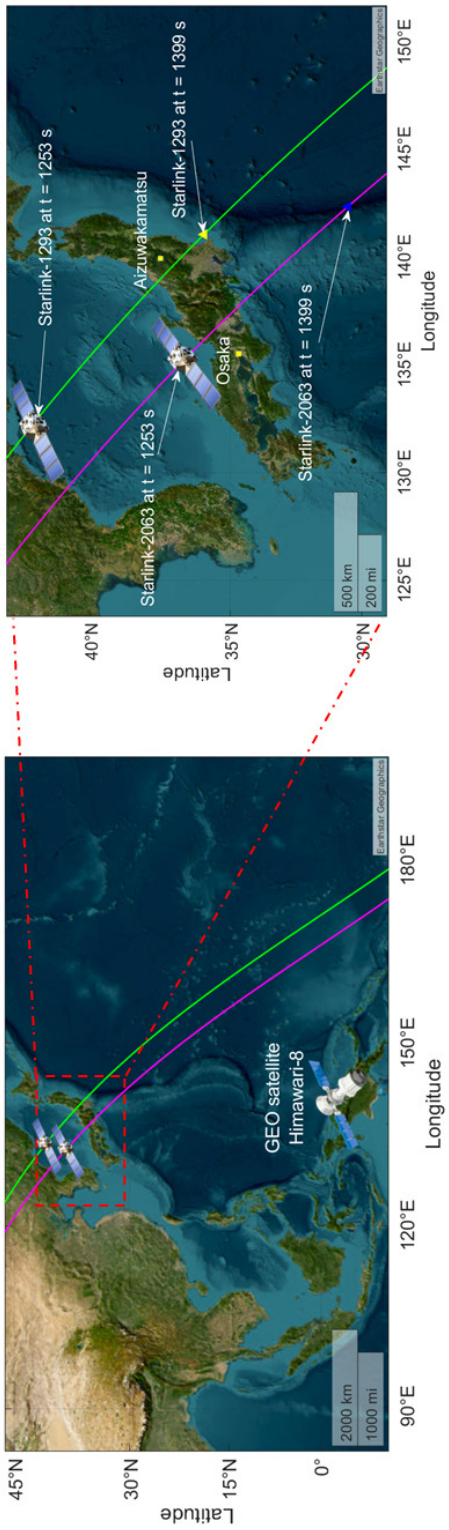


Figure 4.6: Position of GEO satellite on the Earth's surface and ground traces of LEO satellites over Japan observed from 16:09:00 UTC+9 2021/12/23 (Calculated from the collected data in [127])

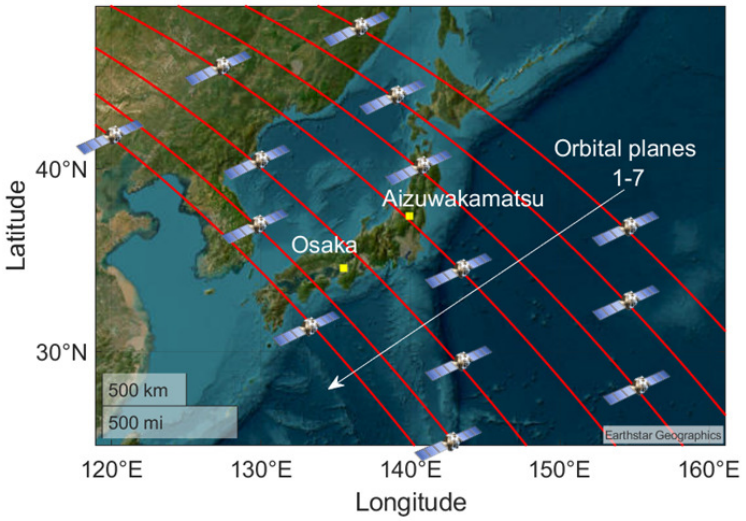
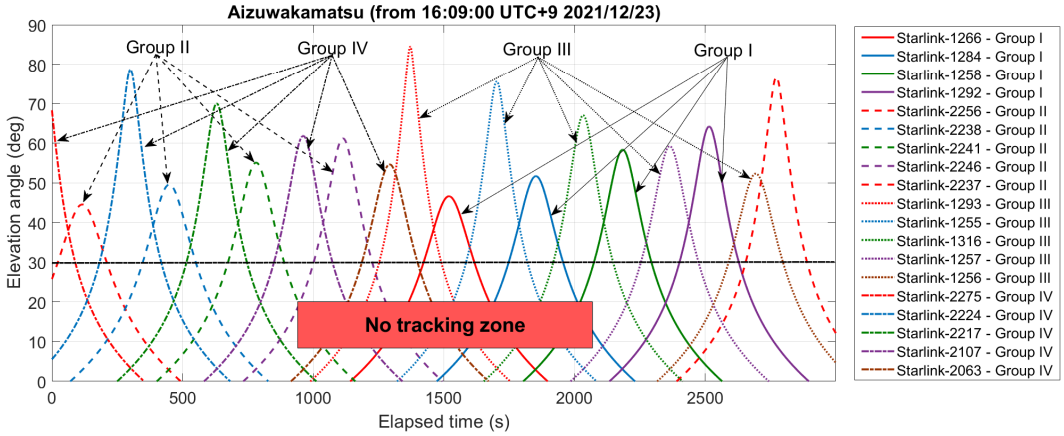
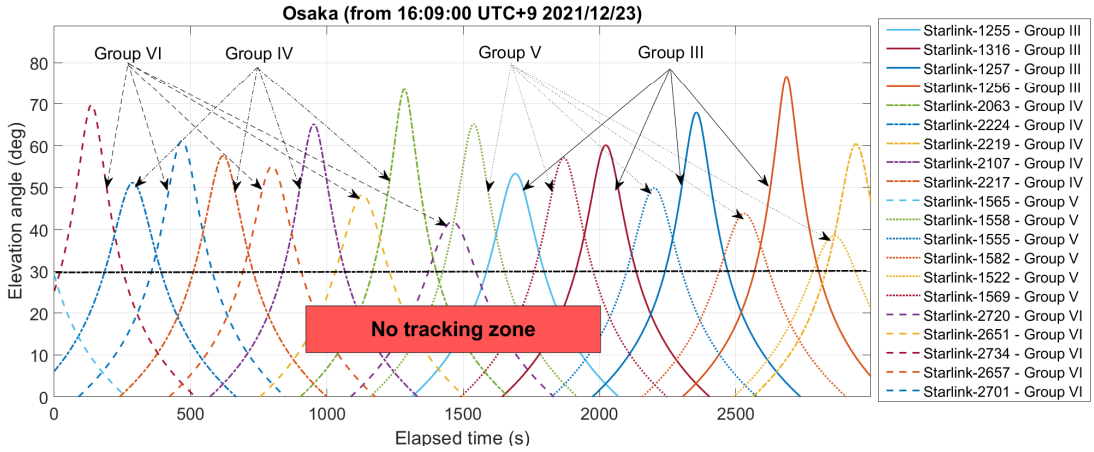


Figure 4.7: Seven orbital planes of Starlink satellite constellation over Japan.



(a) Aizuwakamatsu City



(b) Osaka City

Figure 4.8: An illustration of the visibility of Starlink's LEO satellites in two different cities of Japan.

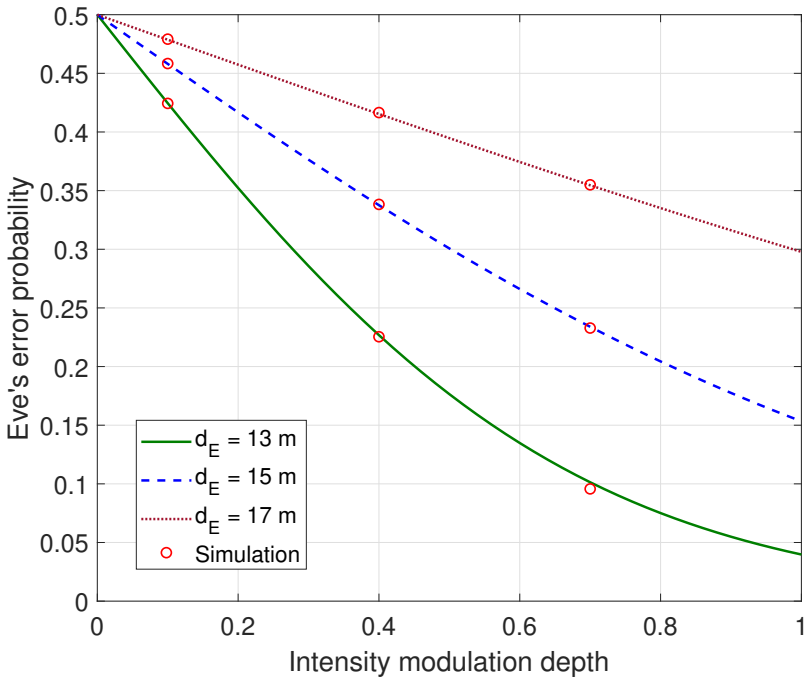


Figure 4.9: Eve's error probability versus intensity modulation depth.

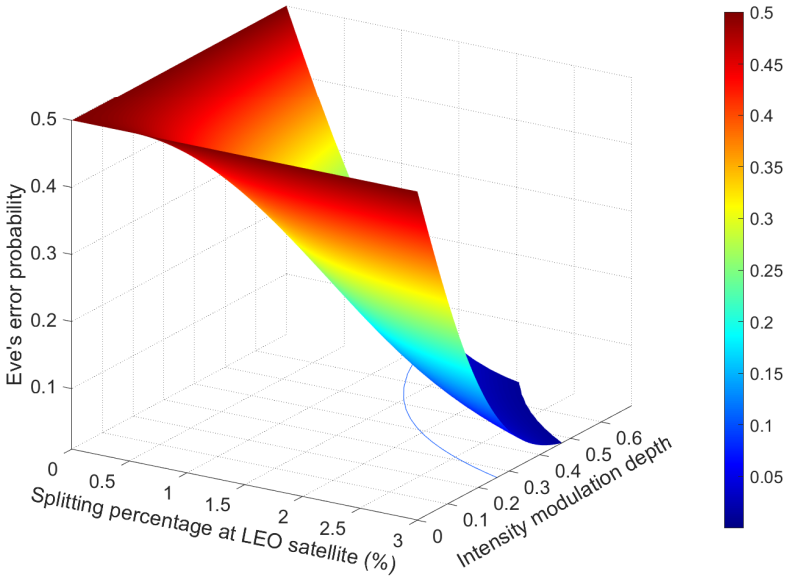
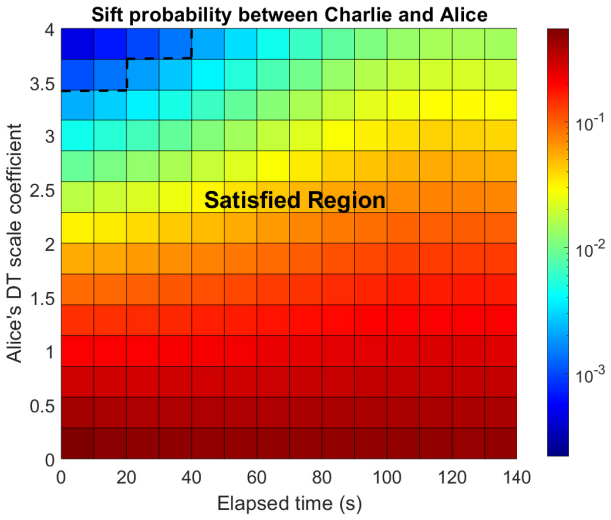
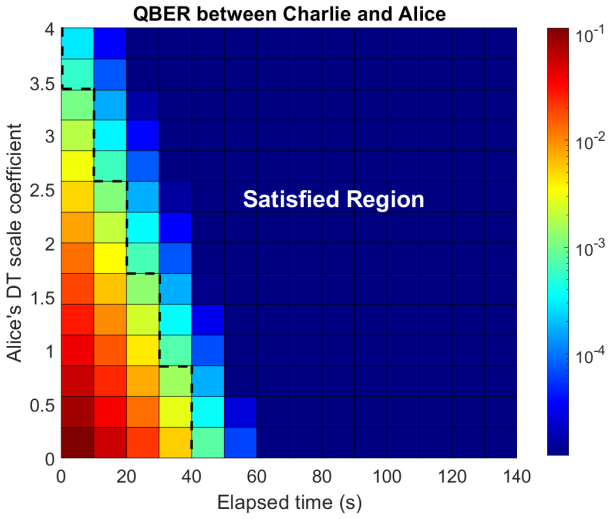


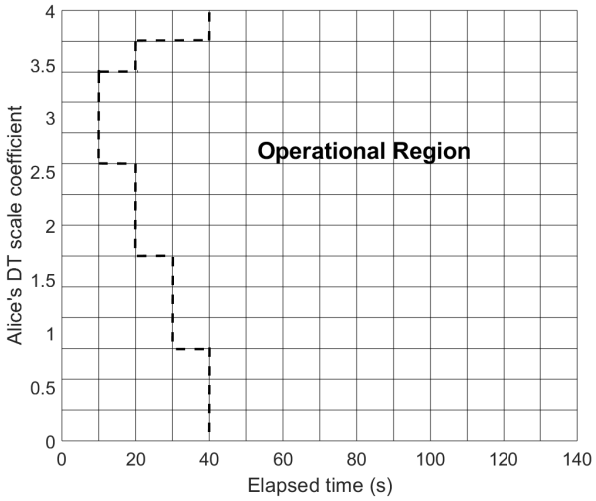
Figure 4.10: Eve's error probability versus the intensity modulation depth and splitting percentage at LEO satellites.



(a) $P_{\text{sift}} \geq 10^{-3}$



(b) QBER$\leq 10^{-3}$



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

Figure 4.11: P_{sift} and QBER between Charlie and Alice versus Alice's DT scale coefficient and the elapsed time

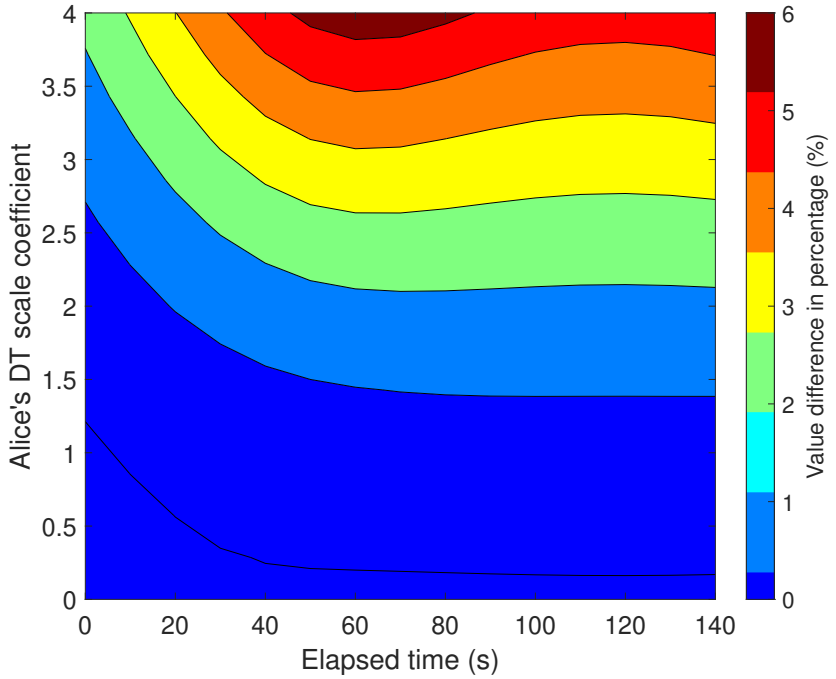


Figure 4.12: The value difference in the sift probability between Alice and Charlie in the case that no BSA and BSA are performed by L_A, SP = 1.5 %.

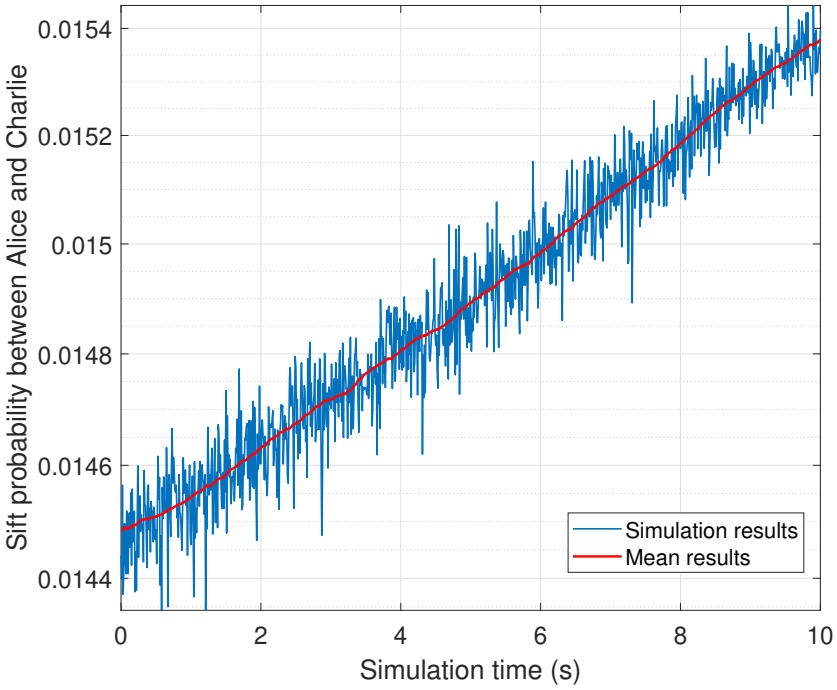


Figure 4.13: Simulation results of the sift probability between Alice and Charlie in the case that BSA is performed by L_A, SP = 1.5%.

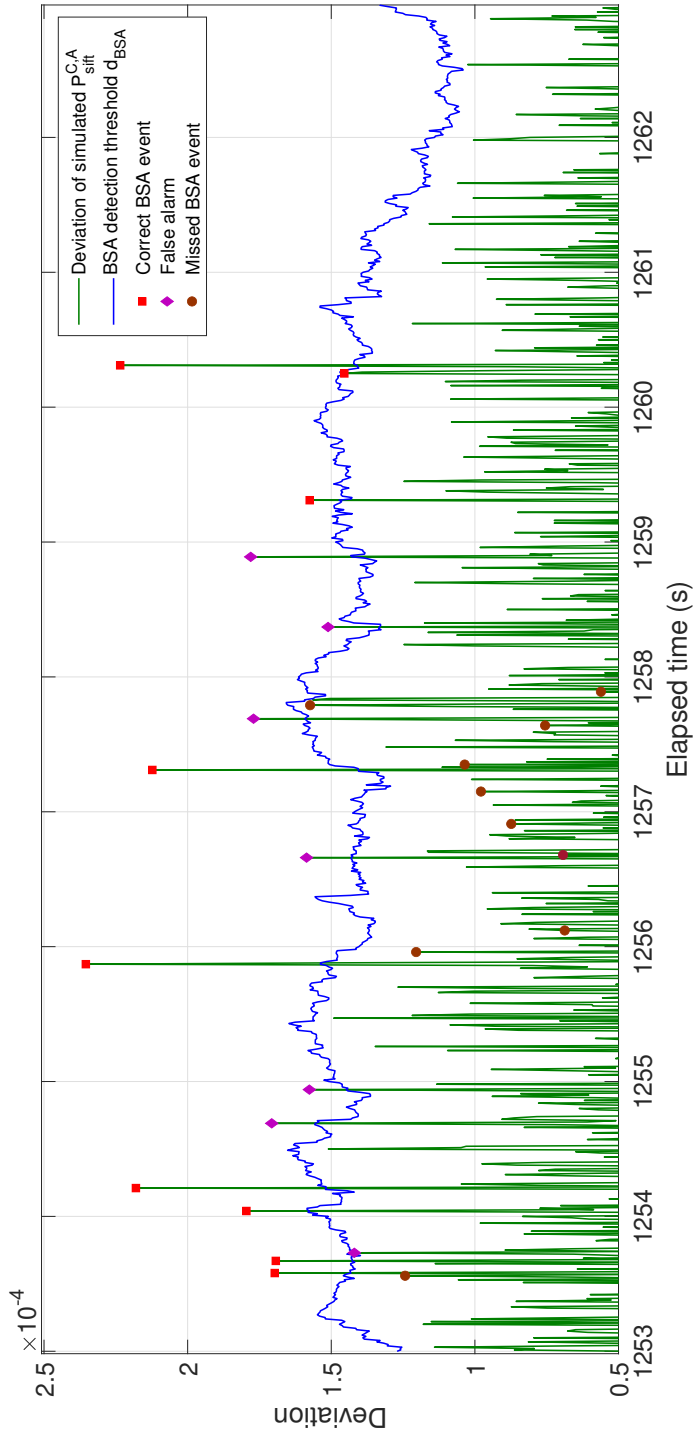
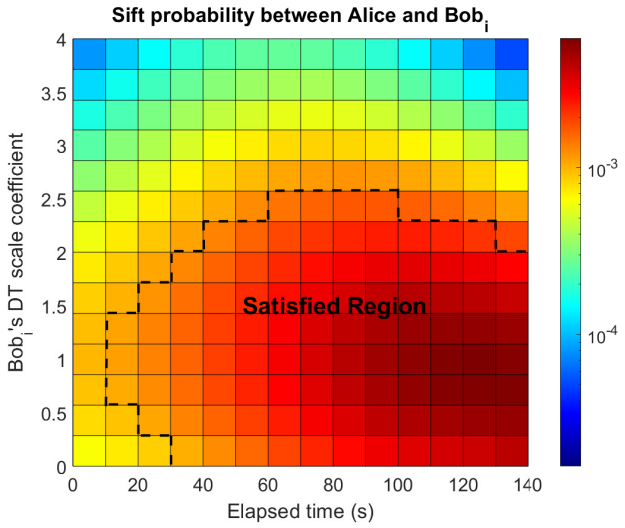
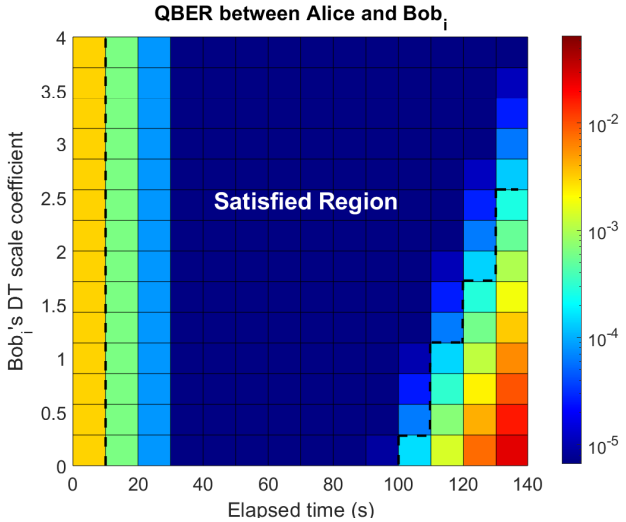


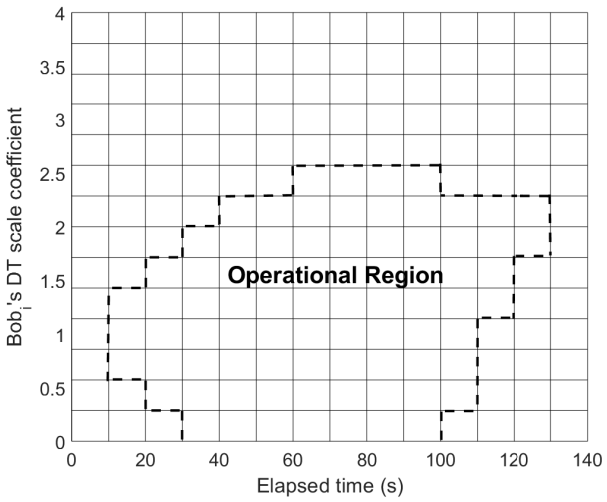
Figure 4.14: BSA detection by comparing the deviation of simulated $P_{\text{sift}}^{C,A}$ and the mean value with the threshold $d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$.



(a) $P_{\text{sift}} \geq 10^{-3}$



(b) QBER$\leq 10^{-3}$



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

Figure 4.15: P_{sift} and QBER between Alice and Bob$_i$ versus Bob$_i$'s DT scale coefficient and the elapsed time.

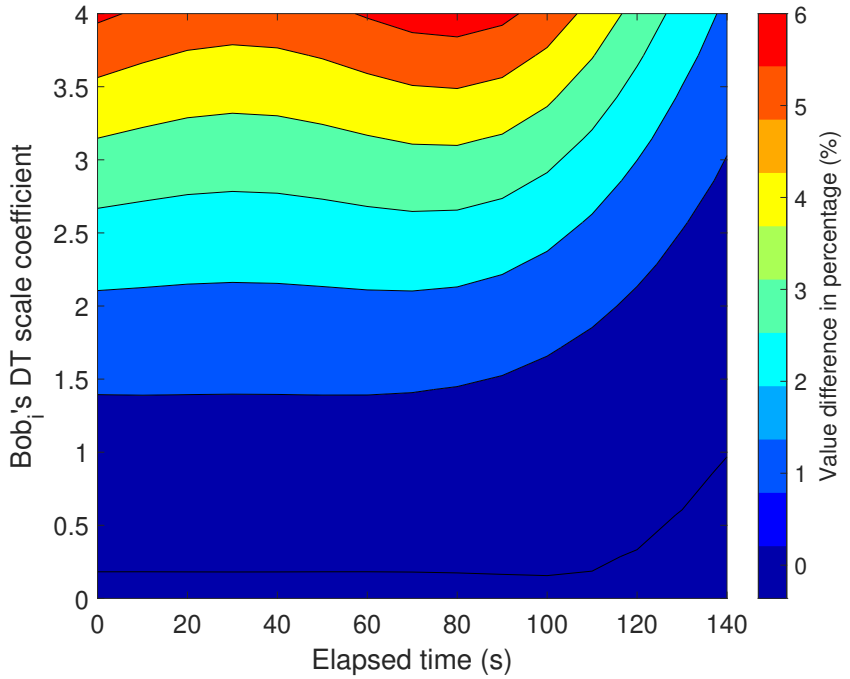


Figure 4.16: The value difference in the sift probability between Alice and Bob$_i$ in the case that no BSA and BSA is performed by L_B, SP = 1.5 %.

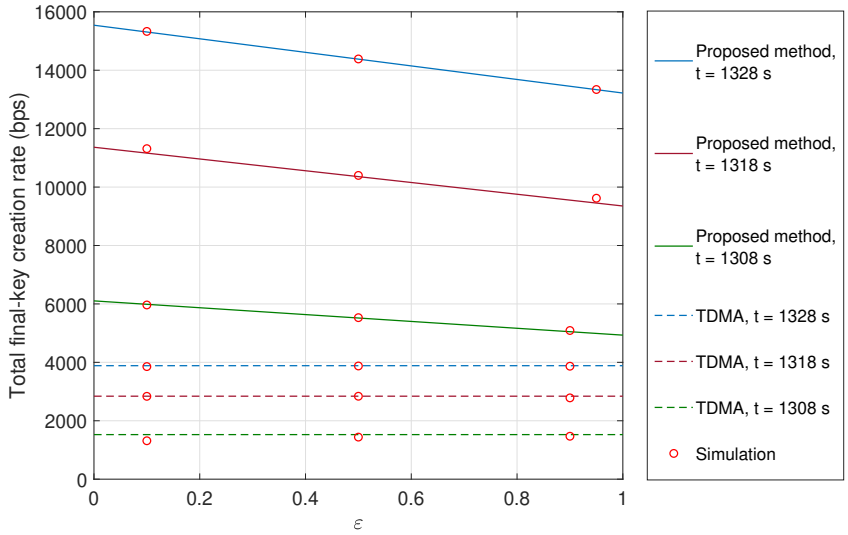


Figure 4.17: Total final-key creation rate versus the exclusion ratio coefficient with $N = 4$: Proposed method versus TDMA method. $\varsigma_{B_i} = 2.25$.

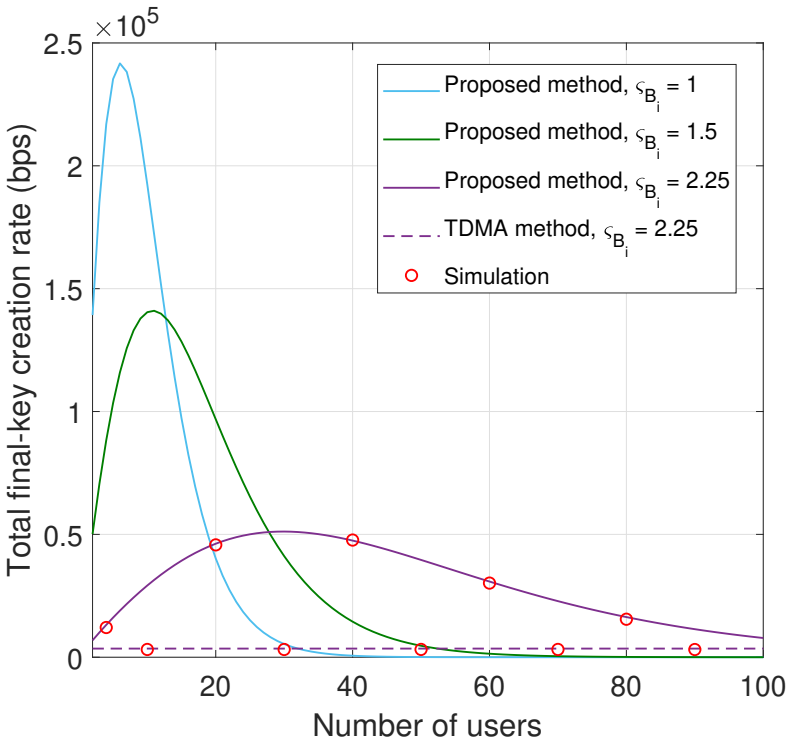


Figure 4.18: Total final-key creation rate versus the number of users at Bob's cluster.

Chapter 5

Design of Hybrid EB/PM Satellite-Based FSO/QKD Systems using GEO/LEOs towards QKD Networks

This chapter[1] focuses on the design of global-scale free-space optics/quantum key distribution (FSO/QKD) networks involving geostationary (GEO) and low-Earth orbit (LEO) satellites. In the approach of the satellite-based FSO/QKD system in chapter 4, the eavesdropper may possess valuable information about the secret keys by analyzing received signals from satellites in the EB scheme. Therefore, in this chapter, we present a novel implementation of network coding-aided hybrid entanglement-based/prepare-and-measure (EB/PM) for satellite continuous-variable QKD (CV-QKD) using dual-threshold/direct-detection (DT/DD) scheme to distribute shared secret keys to multiple users located in distant locations. The purpose of using network coding in this work is to send the key information from GEO satellite to users without sending it directly. Then, the system performance is investigated in terms of final key-creation rates by considering the number of user pairs that the proposed system can support and the effects of the spreading loss, atmospheric attenuation, turbulence, and unauthorized receiver attack (URA) from eavesdroppers. Also, the feasibility of a case study is considered for the existing GEO and LEO satellites from Japan QKD network.

In multiple-user communication scenarios, it is desirable for all users to share their secret keys such that each user can decrypt messages sent by any other users. With distant groups of users, secret key distribution for each pair of users can cope with many security concerns when the secret keys are relayed/routed over many hops [139]. A more efficient alternative is to derive the key from a key source. The key information is then distributed to all users, and each user performs measurement on their own received signal. Each user in each group then performs a post-processing procedure via a public channel with each other to agree on their shared secret key [140]. To implement this method to distribute secret keys for multiple users within distant groups, in this paper, we propose network coding-aided hybrid EB/PM satellite FSO/QKD systems. Both EB and PM schemes are implemented using continuous-variable QKD (CV-QKD). It is realized by transmitting sub-carrier intensity modulation/binary

[1]The content of this chapter was presented in part in

1. Minh Q. Vu *et al.*,"Network coding aided hybrid EB/PM satellite-based FSO/QKD systems," *2023 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC),* Jeju, Korea, Jun. 2023.
2. Minh Q. Vu *et al.*,"Satellite-based quantum key distribution: hybrid EB/PM scheme-assisted multiple users," *Under Review*

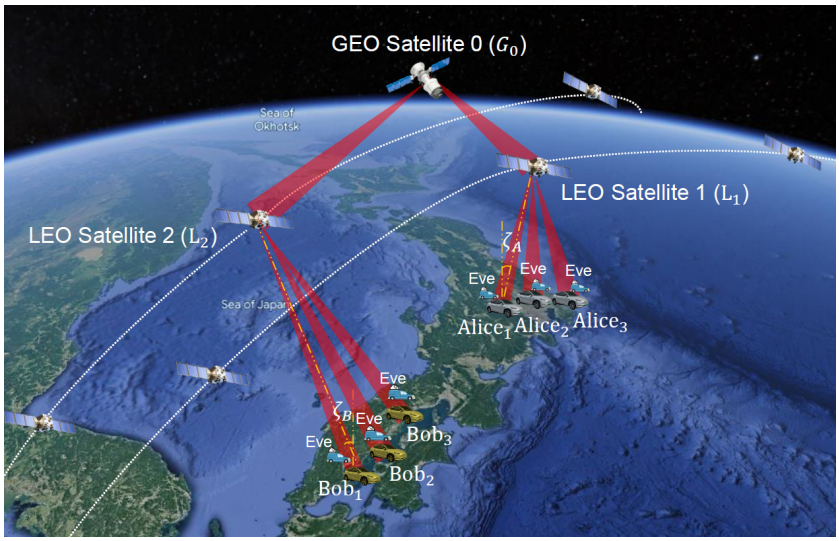


Figure 5.1: Proposed FSO/QKD system using LEO and GEO satellites with $N = 3$. (Maps data: Google Earth)

phase shift keying (SIM/BPSK) signal and equipping dual-threshold direct detection (DT/DD) receivers thanks to its advantages of simple configuration, cost-efficiency, and compatibility with standard optical communication technologies [128]. We also analytically derive the final key-creation rates and investigate the feasibility of the proposed system with practical Japan QKD satellite networks.

5.1 System Description

5.1.1 System Model

Figure 5.1 depicts the proposed two-layer satellite-based FSO/QKD system for multiple wireless users. In this system and in the context of secure vehicle network, we consider N pairs of autonomous vehicles as users in two distant sites (Alice's and Bob's sites). Each user on each site is adjacent to each other and numbered from 1 to N. They are denoted as A_j and B_l with $j, l \in \{1, \ldots, N\}$, respectively. Each user on Alice's site will exchange secret keys with the respective user on Bob's site.

In particular, a GEO satellite (G_0) generates the key K_0 via FSO channels to two LEO satellites[2] ($L_i, i \in \{1, 2\}$). Among G_0 and L_i, EB scheme is applied. After receiving K_0 at L_i, the network coding scheme is employed to distribute the shared key K_0 to multiple legitimate users and is described as follows. Firstly, each L_i uses PM scheme to distribute N different keys to each user by implementing multiple beams over FSO channel at each site. The secret keys shared by PM scheme between L_i and users on Alice's site and on Bob's site are denoted as K_{A_j} and K_{B_l}, respectively. Secondly, meanwhile, the received key K_0 at each L_i is encoded with K_{A_j} (at L_1) or K_{B_l} (at L_2) using XOR operation. Then, the encoding $K_1^j = K_0 \oplus K_{A_j}$ and $K_2^l = K_0 \oplus K_{B_j}$ are shared with A_j and B_l via the public channel, respectively. Thirdly, A_j and B_l then decode respectively received K_1^j and K_2^l by applying the XOR operation with the received K_{A_j} and K_{B_l}. In the perfect case without any errors, each respective pair of users, A_j and B_l, can retrieve the same key K_0, i.e., $(K_0 \oplus K_{A_j}) \oplus K_{A_j} = K_0$ and $(K_0 \oplus K_{B_l}) \oplus K_{B_l} = K_0$. The detailed QKD protocol is further described in Section 5.1.2.

[2] As suggested by NASA, the minimum LEO's elevation angle for system tracking is 30° to avoid the skyscraper's blockage and minimize the impact of atmospheric attenuation/turbulence [146]. Also, this paper considers LEO satellites as trusted nodes.

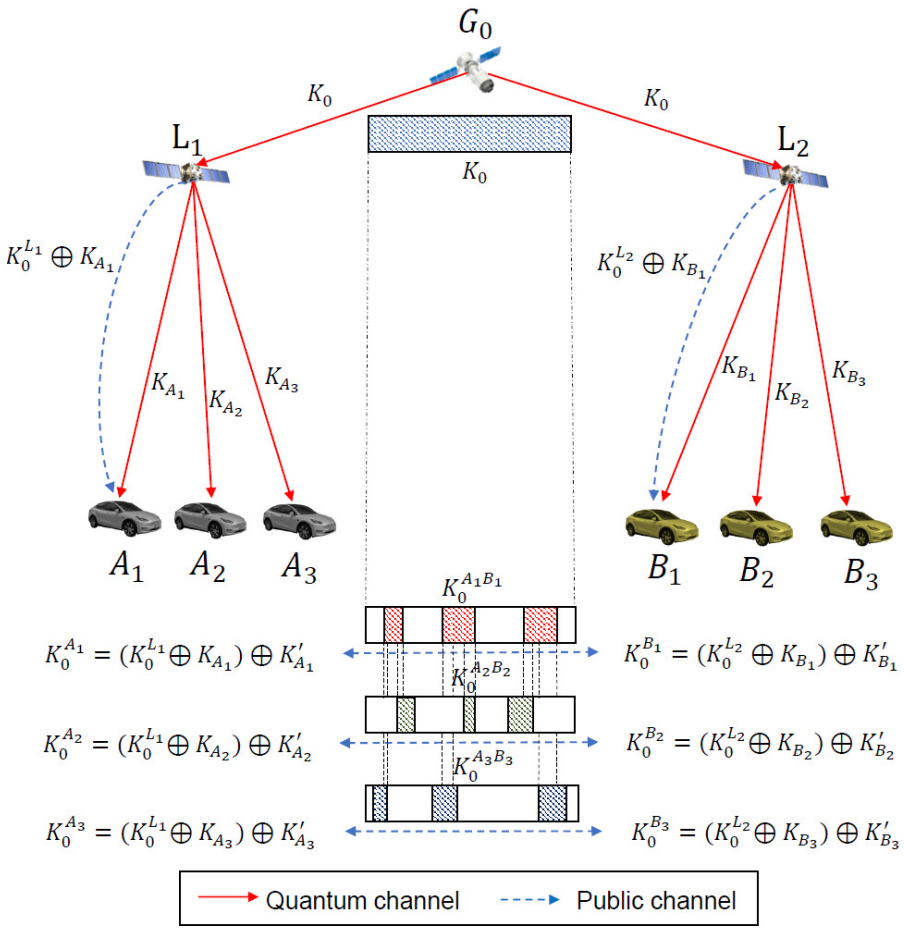


Figure 5.2: Principle of the proposed scheme with $N = 3$.

Moreover, we also consider the scenario where eavesdroppers (Eves) perform an unauthorized receiver attack (URA), the most popular attacking strategy in practical QKD systems. For this attack, Eves, which can be wireless vehicles, try to tap the transmitted signals from L_1 and L_2 by locating their detectors within the beam footprints of each user.

5.1.2 Proposed QKD Protocol for Multiple Wireless Users

The implementation of the proposed QKD protocol of the proposed system can be divided into the following stages.

Stage 1: GEO (G_0) distribute the secret key K_0 to Alice$_j$ and Bob$_l$ using EB scheme over the quantum channel (FSO channel).

- **Signal preparation at** G_0: G_0 generates SIM/BPSK modulated signal representing bit $a \in \{0, 1\}$ of K_0. The value of intensity modulation depth δ_{G_0} ($0<\delta_{G_0}<1$) is adjusted small enough so that the transmitted state cannot be distinguished clearly.

- **Signal transmission and detection at** L_1 **and** L_2: The signal from G_0 is transmitted simultaneously to L_1 and L_2. At each LEO satellite, the received signal is detected individually by its own DT/DD receiver following the detection rule as

$$a_{L_i} = \begin{cases} 0 \text{ if } \left(i_r^{L_i} \leq d_0^{L_i}\right), \\ 1 \text{ if } \left(i_r^{L_i} \geq d_1^{L_i}\right), \\ \text{X otherwise}, \end{cases} \tag{5.1}$$

where a_{L_i} is the detected bit at $L_i, j \in \{1,2\}$, $i_r^{L_i}$ is the detected value of the received current signal at L_i. $d_0^{L_i}$ and $d_1^{L_i}$ are the two levels of DT. X represents the case that L_i creates no bit corresponding to the case of wrong basis selection in QKD [32].

After stage 1, because the random fluctuations in the received signals result in random detection results of "0", "1", and "X", L_1 and L_2 will receive parts of K_0 to form $K_0^{L_1}$ at L_1 and $K_0^{L_2}$ at L_1.

Stage 2: $L_i, i \in \{1,2\}$ implement PM scheme to distribute secret key K_{A_j} with Alice$_j$ and K_{B_l} with Bob$_l$, respectively, over the quantum channel (FSO channel).

- **Signal preparation at** L_i: SIM/BPSK is also generated at L_i with a small modulation depth δ_{L_i} ($0<\delta_{L_i}<1$), corresponding to binary random bit $b \in \{0,1\}$ of K_{A_j} at L_1 and $c \in \{0,1\}$ of K_{B_l} at L_2.

- **Signal transmission and detection at Alice$_j$ (Bob$_l$)**: The signal from L_1 (L_2) is transmitted and detected separately at Alice$_j$ (Bob$_l$). The DT/DD receiver at Alice$_j$ (Bob$_l$) applies the detection rule (5.1) to create bit $b'(c') \in \{0,1\}$ and no bit detected ("X") from the detected signal $i_r^{A_j}$ ($i_r^{B_l}$) with $d_0^{A_j}$ ($d_0^{B_l}$) and $d_1^{A_j}$ ($d_1^{B_l}$) are the two levels of DT at Alice$_j$ (Bob$_l$).

After this stage, Alice$_j$ (Bob$_l$) will receive random detection results of bit "0", "1", and no bit detected (denoted by "X") in K_{A_j} (K_{B_l}) to form K'_{A_j} (K'_{B_l}) due to the random fluctuations in the received signals over the atmospheric channel between L_i and Alice$_j$ (Bob$_l$).

Stage 3: Post-processing procedures using the public channel (e.g., the Internet) to create secret keys between Alice$_j$ and Bob$_l$

- **Key forwarding:** Bit a_{L_i} of $K_0^{L_i}$ is stored at L_i and distributed to Alice$_j$ and Bob$_l$, respectively. The transmitted bit is encoded using XOR operation with bit b of K_{A_j} at L_1 (bit c of K_{B_l} at L_2) and broadcast via the public channel.

  When Alice$_j$ and Bob$_l$ receive the broadcast signal, they decode bit $k_0^{A_j} = (a_{L_1} \oplus b) \oplus b'$ for $K_0^{A_j}$ at Alice$_j$ and bit $k_0^{B_l} = (a_{L_2} \oplus c) \oplus c'$ for $K_0^{B_l}$ at Bob$_l$. The received signal from the broadcast channel is assumed to be error-free. Alice$_j$ and Bob$_l$ then can decode a_{L_i} successfully if b' (c') is detected correctly as transmitted bit b (c) in stage 2 as follows

$$\begin{aligned} k_0^{A_j} &= (a_{L_1} \oplus b) \oplus b = a_{L_1} \\ k_0^{B_l} &= (a_{L_2} \oplus c) \oplus c = a_{L_2}. \end{aligned} \tag{5.2}$$

  If either bit a_{L_1} (a_{L_2}) or b' (c') is detected as X (i.e., no bit is detected), $k_0^{A_j}$ ($k_0^{B_l}$) is assigned to X.

- **Sifting process:** Each pair of Alice$_j$ and Bob$_l$ notify of the time instants that they can receive binary bits from $K_0^{A_j}$ and $K_0^{B_l}$. They will discard bit values at time instants that either $k_0^{A_j}$ or $k_0^{B_l}$ is assigned to X. Alice$_j$ and Bob$_l$ then share an identical bit string, i.e., *sifted key* as the combination of different parts of K_0. The details of the operational scheme are illustrated in Fig. 5.2. The *sifted key* part is illustrated as the rectangular part having the same size with K_0. The colored parts[3] of the received bits at Alice$_j$ and Bob$_l$ denote the instants that Alice$_j$ and Bob$_l$ decode bits. Otherwise, the blank parts represent the time instants that Alice$_j$ and Bob$_l$ decoded "X" (i.e., no bit is detected). The sifted key bits between each pair of Alice$_j$ and Bob$_l$ can be overlapped with each other. With a pair of user Alice$_j$ and Bob$_l$, the knowable sift key parts of other pairs are aligned by dash lines.

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

- **Post-processing:** Error correction and privacy amplification are performed at Alice$_j$ and Bob$_l$ to get the *final shared secret key* from the sifted key $K_0^{A_jB_l}$.

5.2 Channel Models

5.2.1 GEO-to-LEO Channel Model

In the first stage, two LEO satellites L_i receive the signal of K_0 from the GEO satellite via FSO channel. This signal is transmitted through a non-atmospheric region at an altitude above 20 km, therefore, the effect of atmospheric can be imperceptible [141]. All satellites and users are assumed they equipped with fine tracking systems with perfect alignment [142]. Moreover, because the maximum frequency shift in LEO satellite communications is within the capability of the current design for optical satellite communications, the Doppler effect is neglected [112]. Therefore, the geometric spread attenuation of the laser beam modeled by the Gaussian beam becomes the critical impairment.

The attenuation caused by geometric spread for the position vector from the center of the beam footprint $\boldsymbol{r}$ is approximated as [115]

$$h_b^{L_i}\left(\boldsymbol{r}; L_{G_0}\right) \approx A_0^{L_i} \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega_{L_{G_0},eq}^2}\right), \tag{5.3}$$

where $\|\boldsymbol{r}\|$ is the radial distance from the center of the beam footprint. L_{G_0} is the distance between G_0 and L_i. This distance can be calculated from two-line element (TLE) sets of the GEO and LEO satellites and the geometric analysis as in [129]. $A_0^{L_i} = [\text{erf}(\nu_{L_i})]$ is the fraction of the collected power at $\boldsymbol{r} = 0$ with $\nu_{L_i} = \frac{\sqrt{\pi}a_{L_i}}{\sqrt{2}\omega_{L_{G_0}}}$, where a_{L_i} is L_i's receiver radius. $\omega_{L_{G_0}} = \omega_0^{G_0}\left[1 + \left(\frac{L_{G_0}\lambda}{\pi(\omega_0^{G_0})^2}\right)^2\right]^{1/2}$, where $\omega_0^{G_0} = \lambda/2\theta_{G_0}$ is the beam waist at the transmitter of G_0, λ is the operating wavelength, and θ_{L_i} is the divergence angle of the transmitted beam. $\omega_{L_{G_0},eq}^2 = \left(\omega_{L_{G_0}}^2 \frac{\sqrt{\pi}\text{erf}(\nu_{L_i})}{2\nu_{L_i}\exp(-\nu_{L_i}^2)}\right)^{1/2}$ is the equivalent beam radius at distance L_{G_0}. L_i is assumed to be at the center of G_0's beam footprint. Therefore, $h_b^{L_i} = h_b^{G_0}\left(0; L_{G_0}\right) \approx A_0^{L_i}$.

5.2.2 LEO-to-User Channel Model

In the second stage, L_i transmits the signal to user $U \in \{A_j, B_l\}$ over the FSO channel to distribute key K_U. The received signal at user U mainly suffers from three major impairments consisting of the attenuation due to geometric spread h_b^U, atmospheric attenuation h_l^U, and atmospheric turbulence h_a^U. The composite channel between L_i and users is determined as $h_{L_i}^U = h_b^U h_l^U h_a^U$.

5.2.2.1 Geometric spread

We model the transmitted laser beam from LEO satellites as the Gaussian beam. Similar in Sec. 5.2.1, the attenuation due to beam spread at user U is approximated as

$$h_b^U\left(\boldsymbol{r}; L_U\right) \approx A_0^U \exp\left(-\frac{2\|\boldsymbol{r}\|^2}{\omega_{L_U,eq}^2}\right), \tag{5.4}$$

where $L_U = (H_{L_i} - H_U)/\cos(\zeta_U)$ is the distance between the L_i and user U. H_{L_i} and H_U are altitudes of L_i and user U. ζ_U is the zenith angle between L_i and user U, which can

be derived from TLE set of LEO satellites [130]. $A_0^U = [\text{erf}(\nu_U)]$ is the fraction of the collected power at $\boldsymbol{r} = 0$ with $\nu_U = \frac{\sqrt{\pi}a_U}{\sqrt{2}\omega_{L_U}}$ where a_U is the user U's receiver radius. $\omega_{L_U} = \omega_0^{L_i}\left[1+\left(\frac{L_U\lambda}{\pi(\omega_0^{L_i})^2}\right)^2\right]^{1/2}$, where $\omega_0^{L_i} = \lambda/2\theta_{L_i}$ is the beam waist at the laser transmitter of L_i, and θ_{L_i} is the divergence angle of the transmitted beam. $\omega_{L_U,eq}^2 = \left(\omega_{L_U}^2 \frac{\sqrt{\pi}\text{erf}(\nu_U)}{2\nu_U \exp(-\nu_U^2)}\right)^{1/2}$ is the equivalent beam radius at distance L_U. The user U is assumed to be at the center of L_i's beam footprint. The fraction of collected power at user U is thus derived as $h_b^U(0; L_U) \approx A_0^U$. To perform URA, Eve$_j$ and Eve$_l$ locate near Alice$_j$ and Bob$_l$, respectively, and within the beam footprint from L_i. Therefore, the fraction of collected power at them can be determined as $h_b^{E_j}\left(d_{E_j}; L_U\right) \approx A_0^U \exp\left(-\frac{2{d_{E_j}}^2}{\omega_{L_U,eq}^2}\right)$, where $d_{E_j}, j \in \{1, 2, ..., N\}$ is the distance from Eve$_j$ to user U. This formula for E_l is derived in a similar way.

5.2.2.2 Atmospheric attenuation and turbulence

The attenuation of the transmitted laser beam through the atmosphere is calculated by the exponential Beer-Lambert's law as $h_l^U = \exp(-\xi L_U)$, 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 [118]. ξ is the attenuation coefficient, and its value depends on the operating wavelength and the weather conditions [121].

In the Earth's atmosphere, atmospheric turbulence is caused by inhomogeneities in the temperature and pressure of the atmosphere and leads to variations of the refractive index along the transmission path. These index inhomogeneities can cause fluctuations in both the amplitude and the phase of the received signal when the signal propagates through the atmosphere. These fluctuations result in an increase in the link error probability, limiting the performance of the system [121]. When the zenith angles equal to or less than 60° as the requirement for tracking users mentioned in Sec. 5.1.1, the turbulence strength for LEO-to-user link is usually weak [128]. For weak turbulence, the distribution of h_a^U can be modeled as a log-normal distribution as [120]

$$f_{h_a^U}(h_a^U) = \frac{1}{\sqrt{8\pi}h_a^U\sigma_X^U}\exp\left(-\frac{\left[\ln(h_a^U) - 2\mu_X^U\right]^2}{8(\sigma_X^U)^2}\right), \tag{5.5}$$

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 [120]

$$(\sigma_X^U)^2 = 0.56k^{7/6}\sec^{11/6}(\zeta_U)\int_{H_U}^{H_h} C_n^2(h)(h - H_U)^{5/6}\mathrm{d}h, \tag{5.6}$$

where $k = 2\pi/\lambda$ is the wave number, and $\sec(x)$ is the secant function. The refractive index structure parameter $C_n^2(\text{m}^{-2/3})$ can be modeled by Hufnagel-Valley as

$$\begin{aligned} C_n^2(\text{m}^{-2/3}) = 0.00594\left(\frac{w}{27}\right)^2\left(10^{-5}h\right)^{10}\exp\left(-\frac{h}{1000}\right)\exp\left(-\frac{h}{1500}\right) \\ +2.7\times 10^{-16}\exp\left(-\frac{h}{1500}\right) + C_n^2(0)\exp\left(-\frac{h}{100}\right), \end{aligned} \tag{5.7}$$

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 [121].

5.3 Performance Analysis

5.3.1 Sift Probability between Alice$_j$ and Bob$_l$

The sift probability between Alice and Bob ($P^{\text{sift}}_{A_jB_l}$) is the probability that both Alice$_j$ and Bob$_l$ can receive bit "0" or "1" from $k_{0(A_j)}$ and $k_{0(B_l)}$. This probability is calculated as

$$P^{\text{sift}}_{A_jB_l} = P_{A_jB_l}(0,0)+P_{A_jB_l}(0,1)+P_{A_jB_l}(1,0)+P_{A_jB_l}(1,1), \tag{5.8}$$

where $P_{A_j,B_l}(m,n)$, $m,n \in \{0,1\}$ is the probability that Alice$_j$ receives bit $k_{0(A_j)} = m$ coincides with bit $k_{0(B_l)} = n$ at Bob$_l$. $P_{A_j,B_l}(m,n)$ is formulate as as

$$P_{A_jB_l}(m,n) = \sum_{o,p,q,r,s,t\in\{0,1\}} P_{L_1L_2}(o,p)P_{L_1A_j}(q,r)P_{L_2B_l}(s,t), \tag{5.9}$$

where $o \oplus q \oplus r = m$ and $p \oplus s \oplus t = n$. $P_{L_1L_2}(o,p)$ is the probability that L_1's received bit o coincides with L_2's received bit p. $P_{L_1,A_j}(q,r)$ is the probability that L_1 transmits bit q and Alice$_j$ receives bit r. $P_{L_2B_l}(s,t)$ is the probability that L_2 transmits bit s and Bob$_l$ receives bit t. These probabilities can be calculated, in turn as

$$P_{L_1L_2}(o,p) = P_{G_0}(o)P_{L_1|G_0}(o|o)P_{L_2|G_0}(p|o) + P_{G_0}(p)P_{L_1|G_0}(o|p)P_{L_2|G_0}(p|p), \tag{5.10}$$

$$P_{L_1A_j}(q,r) = P_{L_1}(q)P_{A_j|L_1}(r|q), \tag{5.11}$$

$$P_{L_2B_l}(s,t) = P_{L_2}(s)P_{B_l|L_2}(t|s), \tag{5.12}$$

where $P_{G_0}(o)$, $P_{L_1}(q)$, and $P_{L_2}(s)$ are the probabilities that G_0, L_1, and L_2 send bit o, q, and s, respectively. We assume that bits "0" and "1" equally likely to be transmitted; hence, $P_{G_0}(o) = P_{L_1}(q) = P_{L_2}(s) = \frac{1}{2}$.

$P_{L_i|G_0}(z|y), i \in \{1,2\}, y\&z \in \{0,1\}$ is the conditional probabilities that G_0 transmits bit y when L_i detects bit z and calculated as $P_{L_i|G_0}(0|y) = Q\left(\frac{i_y^{L_i}-d_0^{L_i}}{\sigma_N^{L_i}}\right)$, $P_{L_i|G_0}(1|y) = Q\left(\frac{d_1^{L_i}-i_y^{L_i}}{\sigma_N^{U}}\right)$, where $i_0^{L_i} = -i_1^{L_i} = -\frac{1}{4}R_eP_t^{G_0}\delta_{G_0}h_b^{L_i}$ are the received current signals for bit "0" and bit "1" at L_i, respectively. R_e is the responsivity of the photodetector, and $P_t^{G_0}$ is the peak transmitted power at G_0. $Q(\cdot)$ denotes the Q-function. Two thresholds $d_0^{L_i}$ and $d_1^{L_i}$ at the receiver of L_i are determined by $d_0^{L_i} = i_0^{L_i} - \varsigma_{L_i}\sigma_N^{L_i}$ and $d_1^{L_i} = i_1^{L_i} + \varsigma_{L_i}\sigma_N^{L_i}$, where ς_{L_i} is the DT scale coefficient of L_i, $\sigma_N^{L_i}$ is the total noise variance including shot noise, background noise and thermal noise at L_i.

$P_{U|L_i}(z|y), U \in \{A_j, B_l\}$ is the conditional probabilities that L_i transmits bit y when U detects bit z and determined as [128]

$$P_{U|L_i}(0|y) = \int_0^\infty Q\left(\frac{i_y^U - d_0^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{5.13}$$

$$P_{U|L_i}(1|y) = \int_0^\infty Q\left(\frac{d_1^U - i_y^U}{\sigma_N^U}\right) f_{h_a^U}(h_a^U)\mathrm{d}h_a^U, \tag{5.14}$$

where $i_0^U = -i_1^U = -\frac{1}{4}R_eP_t^{L_i}\delta_{L_i}h_{L_i}^U$ are the received current signals for bit "0" and bit "1" at

user U, respectively, and $P_t^{L_i}$ is the peak transmitted power at L_i. Two thresholds d_0^U and d_1^U at the receiver of user U are given by

$$d_0^U = \mathbb{E}[i_0^U] - \varsigma_U \sigma_N^U, d_1^U = \mathbb{E}[i_1^U] + \varsigma_U \sigma_N^U, \tag{5.15}$$

where ς_U is the DT scale coefficient of user U and $\mathbb{E}[\cdot]$ is the expectation operator. We have $\mathbb{E}[i_0^U] = -\frac{1}{4} R_e P_t^{L_i} \delta_{L_i} h_b^U h_l^U$ and $\mathbb{E}[i_1^U] = \frac{1}{4} R_e P_t^{L_i} \delta_{L_i} h_b^U h_l^U$ as $\mathbb{E}[h_{L_i}^U] = \mathbb{E}[h_b^U h_l^U h_a^U] = h_b^U h_l^U$ with $\mathbb{E}[h_a^U] = 1$ as the mean irradiance is normalized to unity.

Because Eve$_j$ cannot obtain the knowledge of user U's DT value, the best choice for her is to use the optimal threshold $d_0^{E_j} = d_1^{E_j} = 0$ to receive as much as key information as possible, however, she will suffer high bit error rate thanks to the small modulation depth δ_{L_i} of transmitted SIM/BPSK signal. The detailed explanation for the security of non-coherent CV-QKD can be found in [128].

On the other hand, as mentioned in Sec. 5.1.2, there are probabilities that the sifted key of Alice$_j$ and Bob$_l$ can have useful bits (i.e., bits "0" and "1") at the same time instants with the sifted key of other pairs as illustrated in Fig. 5.2. Alice$_j$ and Bob$_l$ can know which time instant they and other pairs can decode useful bits based on the information sent via the public channel between each pair. The probability of this event is called *mutual sift probability*. To create independent secret keys with other pairs, Alice$_j$ and Bob$_l$ need to exclude the mutual sifting key information with other pairs. Thus, the sifting probability between Alice$_j$ and Bob$_l$ is continued to calculate as follows

$$P_{A_j B_l}^{\text{sift-excl}} = P(A_j B_l) - \varepsilon P(A_j B_l)_{\text{excl}}, \tag{5.16}$$

where ε ($0 \leq \varepsilon \leq 1$) is the exclusion ratio coefficient; when $\varepsilon = 1$, all mutual bits are excluded. $P(A_j B_l)_{\text{excl}}$ is the mutual sift probability with other pairs and formulated as

$$\begin{aligned} P(A_j B_l)_{\text{excl}} = \sum_{1 \leq j_2, k_2 \leq N} P(A_j B_l \cap A_{j_2} B_{l_2}) - \sum_{1 \leq j_2, l_2, j_3, l_3 \leq N} P(A_j B_l \cap A_{j_2} B_{l_2} \cap A_{j_3} B_{l_3}) \\ + (-1)^N P\Big(\bigcap_{j,k=1}^{N} A_j B_l \Big), \end{aligned} \tag{5.17}$$

where $P(A_j B_l \cap A_{j_2} B_{l_2})$ is denoted for the mutual sift probability between two pairs, $A_j B_l$ and $A_{j_2} B_{l_2}$. This mutual sift probability $P(A_j B_l \cap A_{j_2} B_{l_2})$ is expressed as follows

$$\begin{aligned} P(A_j B_l \cap A_{j_2} B_{l_2}) = & P_{A_j B_l, A_{j_2} B_{l_2}}(0,0,0,0) + P_{A_j B_l, A_{j_2} B_{l_2}}(0,0,0,1) \\ + P_{A_j B_l, A_{j_2} B_{l_2}}(0,0,1,0) & + P_{A_j B_l, A_{j_2} B_{l_2}}(0,0,1,1) + P_{A_j B_l, A_{j_2} B_{l_2}}(0,1,0,0) \\ + P_{A_j B_l, A_{j_2} B_{l_2}}(0,1,0,1) & + P_{A_j B_k, A_{j_2} B_{l_2}}(0,1,1,0) + P_{A_j B_l, A_{j_2} B_{l_2}}(0,1,1,1) \\ + P_{A_j B_l, A_{j_2} B_{l_2}}(1,0,0,0) & + P_{A_j B_l, A_{j_2} B_{l_2}}(1,0,0,1) + P_{A_j B_l, A_{j_2} B_{l_2}}(1,0,1,0) \\ + P_{A_j B_l, A_{j_2} B_{l_2}}(1,0,1,1) & + P_{A_j B_l, A_{j_2} B_{l_2}}(1,1,0,0) + P_{A_j B_l, A_{j_2} B_{l_2}}(1,1,0,1) \\ & + P_{A_j B_l, A_{j_2} B_{l_2}}(1,1,1,0) + P_{A_j B_l, A_{j_2} B_{l_2}}(1,1,1,1) \end{aligned} \tag{5.18}$$

where $P_{A_j B_l, A_{j_2} B_{l_2}}(m,n,o,p)$ with $m,n,o,p \in \{0,1\}$ is the probability that Alice$_j$'s detected bit m coincides with Bob$_l$'s detected bit n, Alice$_{j_2}$'s detected bit o and Bob$_{l_2}$'s detected bit p. $P_{A_j B_l, A_{j_2} B_{l_2}}(m,n,o,p)$ is formulated as

$$\begin{aligned} P_{A_j B_l, A_{j_2} B_{l_2}}(m,n,o,p) = & \sum_{q,r,u_1,v_1,u_2,v_2,y_1,z_1,y_2,z_2 \in \{0,1\}} P_{L_1,L_2}(q,r) P_{L_1,A_j}(u_1,v_1) \\ & \times P_{L_1,A_{j_2}}(u_2,v_2) P_{L_2,B_l}(y_1,z_1) P_{L_2,B_{l_2}}(y_2,z_2), \end{aligned} \tag{5.19}$$

where $m = q \oplus u_1 \oplus v_1$, $n = r \oplus y_1 \oplus z_1$, $o = q \oplus u_2 \oplus v_2$, and $p = r \oplus y_2 \oplus z_2$.

The general formula to calculate the mutual sift probability between N user pairs is given in C.

5.3.2 Quantum Bit Error Rate (QBER)

QBER is used to reflect the bit error rate in the sifted key $K_0^{A_jB_l}$. This metric is formulated as $\text{QBER}_{A_jB_l} = \frac{P^{\text{error}}_{A_jB_l}}{P^{\text{sift-excl}}_{A_jB_l}}$, where $P^{\text{error}}_{A_jB_l}$ is the probability that there is a number of the erroneous bits in the sifted key. These erroneous bits are caused by technical imperfections [94]. The erroneous probability can be determined as

$$P^{\text{error}}_{A_jB_l} = P_{A_jB_l}(0,1) + P_{A_jB_l}(1,0), \tag{5.20}$$

where $P_{A_jB_l}(0,1)$ and $P_{A_jB_l}(1,0)$ are determined as Eqs. (5.11),(5.12).

5.3.3 Final-Key Creation Rate

After performing error correction and privacy amplification in post-processing procedures to exclude the amount of information leaked to eavesdroppers, the final key-creation rate ($R_f^{A_jB_l}$) is a metric to determine the useful bit rate of the key distribution system for a pair of users. $R_f^{A_jB_l}$ is given as

$$R_f^{A_jB_l} = R_s^{A_jB_l}\left[\alpha I(A_j;B_l) - \max(I(A_j;E_j), I(B_l;E_l))\right], \tag{5.21}$$

where $R_s^{A_jB_l} = R_b P^{\text{sift-excl}}_{A_jB_l}$ is the sifted-key rate between Alice$_j$ and Bob$_l$ after mutual sift probability extraction, R_b is the system bit rate. α denotes the error correction efficiency and is assumed to be 1 to evaluate the upper bound of the proposed system's performance [108]. $I(A_j;B_l)$, $I(A_j;E_j)$, and $I(B_l;E_l)$ are the mutual information between Alice$_j$ and Bob$_l$, Alice$_j$ and Eve$_j$, and Bob$_l$ and Eve$_l$. These mutual information formulas are given as

$$I(Y;Z) = \sum_{y,z\in\{0,X,1\}} P_{YZ}(y,z)\log_2\left[\frac{P_{YZ}(y,z)}{P_Y(y)P_Z(z)}\right], \tag{5.22}$$

where $P_{YZ}(y,z)$ with $Y, Z \in \{A_j, B_l, E_j, E_l\}$ 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.

5.4 Numerical Results

5.4.1 Practical Scenarios and Considered Satellites

To investigate the feasibility of the proposed system for Japan QKD network, we consider multiple users Alice$_j$ are located randomly in Aizuwakamatsu City, Japan (longitude: 139.93899°E; latitude: 37.52266°N; elevation: 209.093 m). On the other hand, multiple user Bob$_l$ are located randomly in Osaka City, Japan (longitude: 135.51983°E; latitude: 34.68305°N; elevation: 155.448 m), which is about 500 km southwest of Alice$_j$ location. We select the existing Japanese GEO satellite Himawari-8 ((longitude: 140.66°E; latitude: 0.02°S) employed as G_0 in the proposed system [131]. LEO satellites employed as L_i are chosen from the Starlink constellation thanks to the capability of 24/7 global coverage [132]. The data of satellites were observed at the epoch time of 16:09:00 (UTC+9) on Dec. 23, 2021. After the epoch time, from the elapsed time of $t = 1253$ s to $t = 1399$ s, two available LEO satellites (Starlink-1293 and

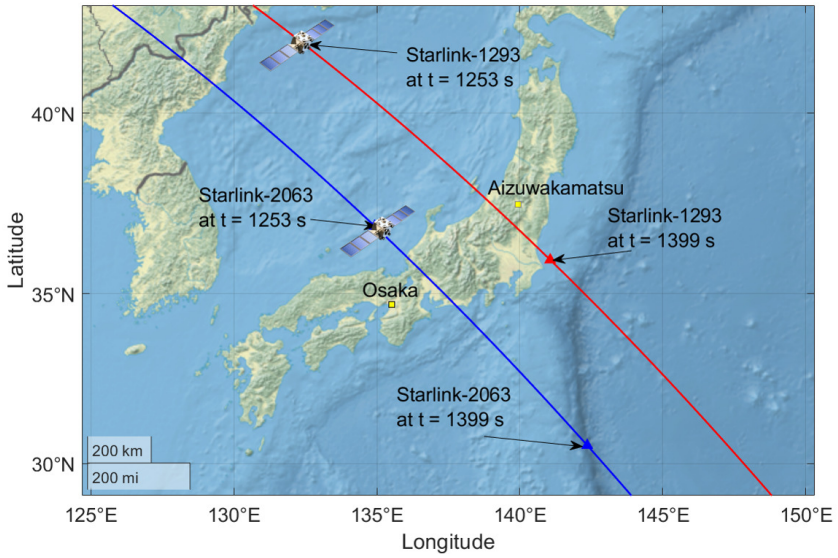


Figure 5.3: Ground traces of LEO satellites over Japan observed from 16:09:00 UTC+9 2021/12/23.

Starlink-2063) can transmit the signal to Alice$_j$ and Bob$_l$ simultaneously, where the zenith angle between a satellite and a legitimate user is below 60° as shown in Fig. 5.3 plotted from the available TLE data in [127].

5.4.2 Secret-key Rate Performance

In this section, we analyze the secret-key rate performance indicated by the final-key creation rate of $R_f^{A_jB_l}$ and the number of user pairs that the proposed system can support under URAs performed by Eve$_j$. Following the design criteria in 4.4.1, our main target is to control: (1) $P_{A_jB_l}^{\text{sift-excl}} \geq 10^{-3}$ to guarantee that Alice$_j$ and Bob$_l$ receives sufficient key information, i.e., to achieve a sifted-key rate at Mbps with the typical transmission rates at Gbps of FSO communications; and (2) $\text{QBER}_{A_jB_l} \leq 10^{-3}$ so that the error is small enough that it can be efficiently corrected at such Mbps of sifted-key rates by error-correcting code. Thus, the parameters can be selected as $\delta_{G_0} = 0.6$, $\delta_{L_i} = 0.6$, $\varsigma_{L_i} = 1$, $\varsigma_{A_j} = 0.25$, $\varsigma_{B_l} = 0.25$. In addition, the other system parameters are shown in Table 5.1.

Figure 5.4 shows the final-key creation rate of one user pair with different numbers of user pairs (N) and the zenith angle between L_i and users as the function of elapsed time. The final-key creation rate of one user pair will achieve maximum value (e.g., $\approx$ 18 kbps when $N = 1$). When the number of user pairs increases, the final-key creation rate of one user pair will decrease.

In Fig. 5.5, the final-key creation rate of one user pair versus the number of user pairs with different exclusion ratio coefficients at a specific time instant $t = 1360$ s are presented. Basically, the final-key creation rate of one user pair will decrease when the number of user pairs increases. When $\varepsilon = 1$ (i.e., 100% mutual sift probabilities are excluded), the final-key creation rate will asymptote to 0 when the number of user pairs increases to 40. In this case, a pair of users can generate different secret keys from other user pairs. The saturated value of the final-key creation rate of one user pair can be increased if more percentages of mutual sift probabilities are kept in the sift probability of Alice$_i$ and Bob$_l$. For example, when $\varepsilon = 0.9$ (i.e., 10% mutual sift probabilities are kept), the saturated value of the final-key creation rate of one user pair is increased to $\approx$ 5 kbps. However, this also increases the knowledge of key information among user pairs. It can lead to reduced security of the proposed system if the trust

Table 5.1: System Parameters

Name	Symbol	Value
GEO Satellite G_0		
Wavelength	λ	1550 nm
Bit rate	R_b	1 Gbps
Altitude	H_{G_0}	35793 km
Divergence angle	θ_{G_0}	10 μrad
Transmitted power	$P_t^{G_0}$	32 dBm
LEO Satellites $L_i, i \in \{1, 2\}$		
Wavelength	λ	1550 nm
Altitude	H_{L_i}	550 km
Divergence angle	θ_{L_i}	50 μrad
Receiving aperture radius	a_{L_i}	10 cm
Transmitted power	$P_t^{L_i}$	30 dBm
FSO Channel		
Sun's spectral irradiance from above the atmosphere at 1550 nm	Ω_{l}	$0.1\ \mathrm{W/cm^2 \cdot \mu m}$
Sun's spectral irradiance from above the Earth at 1550 nm	Ω_{r}	$0.05\ \mathrm{kW/m^2 \cdot \mu m}$
Wind speed	w	21 m/s
The refractive index structure parameter at the ground level	$C_n^2(0)$	$10^{-15}\mathrm{m}^{-2/3}$
Visibility (clear weather condition)	V	30 km
Users A_j, B_l **Eves** E_j, E_l $j, l \in \{1, 2, \ldots, N\}$		
Altitude	H_{U}	2 m
Receiving aperture radius	a_{U}	5 cm
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

relationship among user pairs is broken.

In Fig. 5.6, we investigate the impact of the distance between eavesdroppers and users (d_{E_j}, d_{E_l}) on the final-key creation rate of one pair along with the number of user pairs (N). When eavesdroppers are far away from users, the final-key creation rate of one pair will increase. The distance between eavesdroppers and users has much influence on the final-key creation rate of one pair when there are 1 to 4 pairs of users. For example, in the case $N = 2$, the final-key creation rate of one pair can increase from about 0.4 kbps to 20 kbps when the distance between eavesdroppers and users increases from 22 to 32 meters.

Figure 5.7 illustrates the spatial distribution of the final-key creation rate of one user pair with different numbers of user pairs when multiple users Bob_l are located in Osaka City. From this figure, we can observe the possible location for multiple users Alice_j and the final-key creation rate at the respective location. The value of final-key creation rates of one user pair also decreases when the number of user pairs is increased.

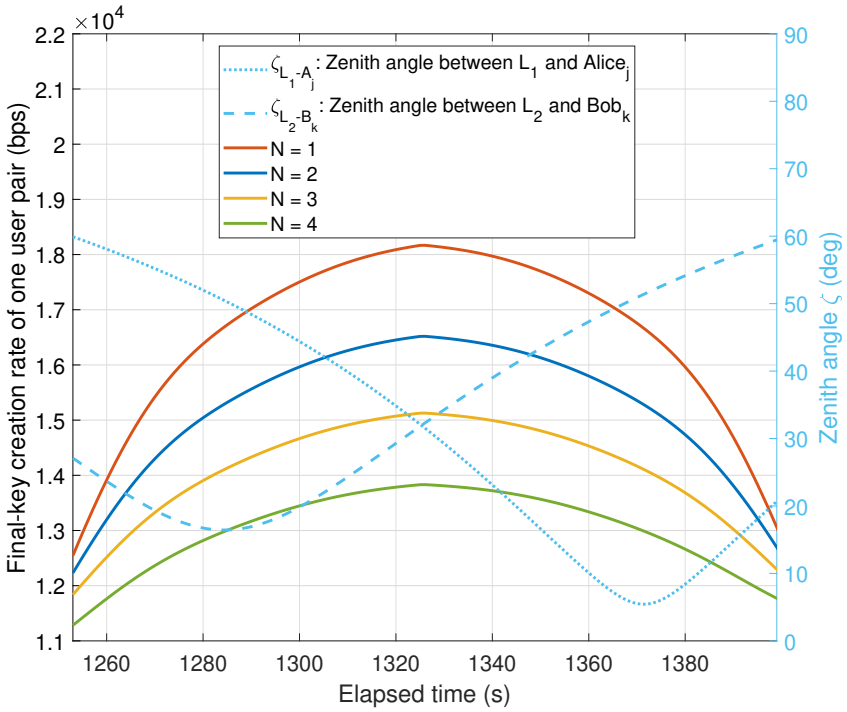


Figure 5.4: Final-key creation rate of one user pair with different numbers of user pairs (N) and zenith angle between L_i and users versus elapsed time from the epoch time, d_{E_j}=d_{E_l}=25 m, $\varepsilon = 1$.

5.5 Conclusions

In this paper, we presented a novel design for a global-scale FSO/QKD network based on a GEO satellite as the secret key source and LEO satellites as intermediate nodes for multiple wireless users. Network coding combined with the entanglement-based and prepare-and-measure CV-QKD protocol and DT/DD receivers are employed to reduce the number of transmission phases and increase the security of the proposed system. The system performance was analyzed in terms of final-key creation rates, and the number of user pairs that the proposed system can support, considering the spreading loss, atmospheric attenuation, and turbulence. We investigated the case study for the Japan QKD network, taking into consideration URA from eavesdroppers.

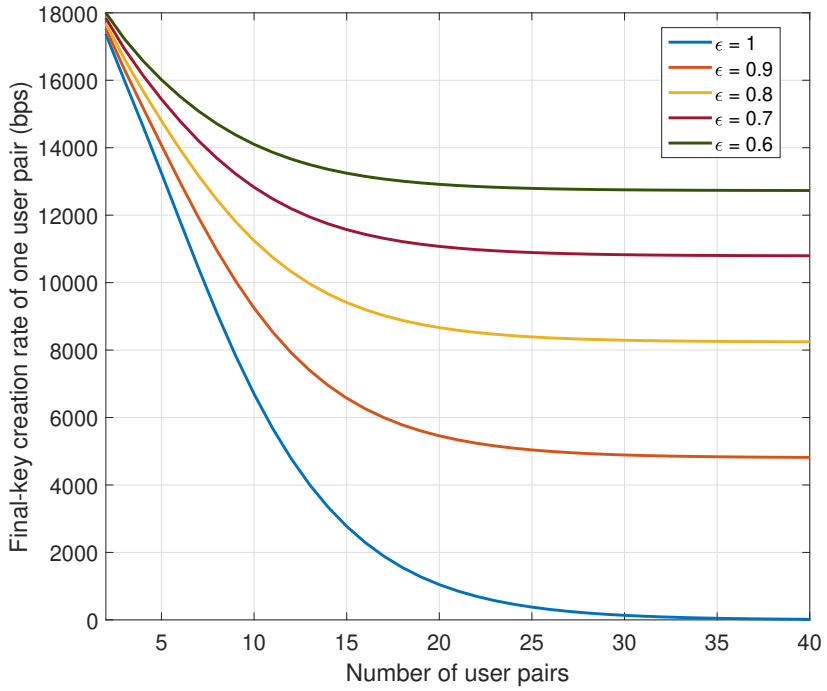


Figure 5.5: Final-key creation rate of one user pair versus the number of user pairs (N) with different exclusion ratio coefficients (ε). $t = 1360$ s, d_{E_j}=d_{E_l}=25 m.

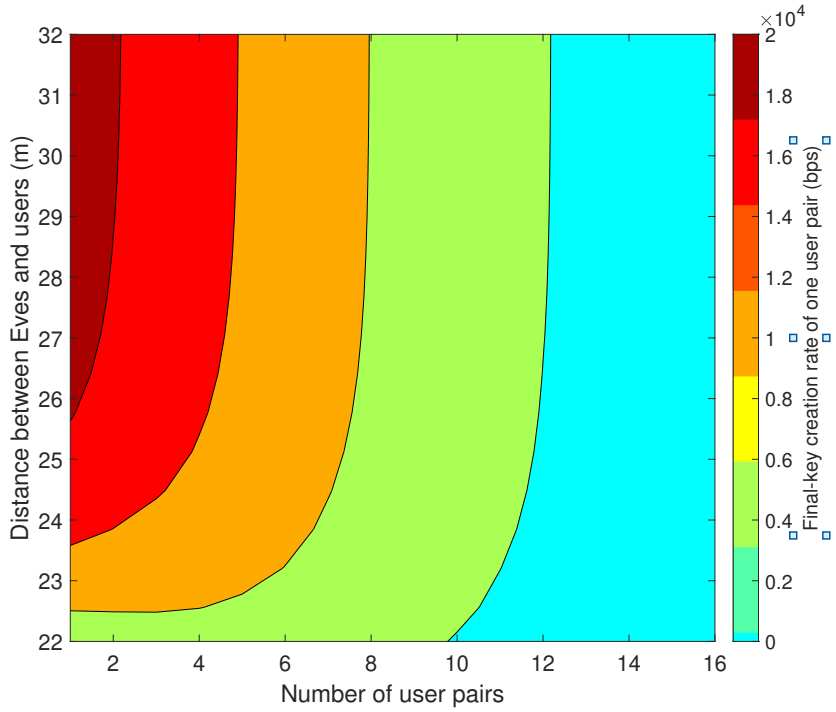
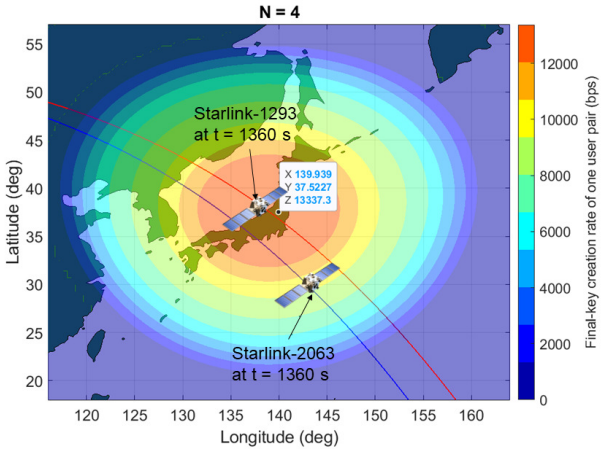
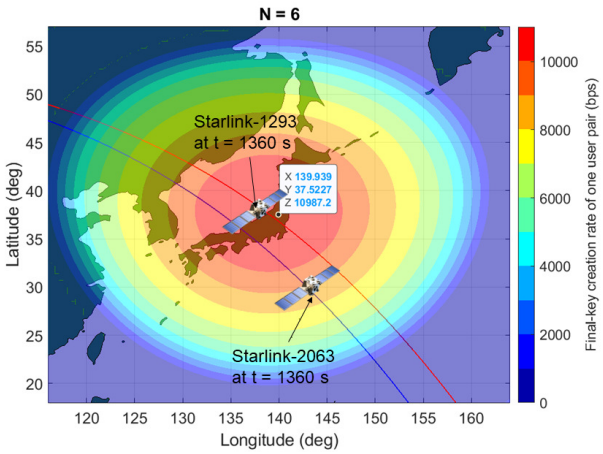


Figure 5.6: Final-key creation rate of one pair versus the distance between eavesdroppers and users (d_{E_j},d_{E_l}) and the number of user pairs (N), $t = 1360$ s, ε = 1.



(a) N = 4



(b) N = 6

Figure 5.7: The spatial distribution of the final-key creation rate of one user pair with different numbers of user pairs, $t = 1360$ s. (Bob_l are located in Osaka City).

Chapter 6

Summary and Future Research

6.1 Summary

QKD is a practical application of quantum mechanics, which exploits the fundamental principles of physics to exchange cryptographic keys between legitimate parties. It can guarantee unconditional communication security because the security of the protocol does not depend on the complexity of some mathematical problem; thus, the computational power of a possible adversary does not have to be bounded. QKD systems using optical fiber and FSO as the quantum channel has been demonstrated. Due to the limitation in the distance of the terrestrial-based system, a viable solution is using satellites that distribute secure keys to ground stations via FSO links.

Satellite-based FSO/QKD can work in two different schemes: PM scheme and EB scheme. In the former, the satellite acts as a trusted relay node for legitimate parties (Alice and Bob). The secret keys are distributed from Alice to Bob via the relay node. The disadvantages of this scheme include complexity and inefficiency, as we need more than one phase to distribute a key ultimately. In the latter, the satellite acts as the central source and sends two beams of entangled quantum states to Alice and Bob simultaneously. They then make independent measurements of received quantum states and define the secret key without the involvement of the satellite. Neither Alice nor Bob needs to trust the satellite anymore. Compared to the PM scheme, this scheme is more efficient and can potentially implement a global-scale QKD network.

Depending on how quantum states are represented, in each scheme, there are two main approaches to implement QKD systems, including DV-QKD and CV-QKD. The deployment of DV-QKD is limited by the difficulty in generating entangled photon pairs and the expense of single-photon detectors. Moreover, DV-QKD is incompatible with the standard optical communication technology. Compared to DV-QKD, CV-QKD is capable of supporting higher key rates than DV-QKD. Recall that CV-QKD can be implemented by modulating both the amplitude and phase quadratures of a coherent laser and can be subsequently measured in the receivers using homodyne/heterodyne detectors, which operate faster and more efficiently than single-photon detectors. CV-QKD are more compatible with standard optical communication technology. However, the weakness of CV-QKD is the requirement of a sophisticated phase-stabilized local light for coherent detection. It leads to a high cost for deploying CV-QKD systems.

Considering the future scenario where QKD would be implemented globally for a wide range of applications, including mobile users like autonomous vehicles and unmanned aerial vehicles, it is necessary to find a less complex and low-cost QKD implementation. To do so, in chapter 3, we consider non-coherent CV-QKD by employing DT/DD at receivers for the EB scheme. Specifically, we present a new design concept for satellite-based FSO/QKD by applying non-coherent detection for the EB scheme based on the BBM92 protocol. This protocol is the most popular EB DV-QKD, which is also used in Micius's satellite-based FSO/QKD system. In the system model and analysis, the atmospheric channel between satellites and legitimate

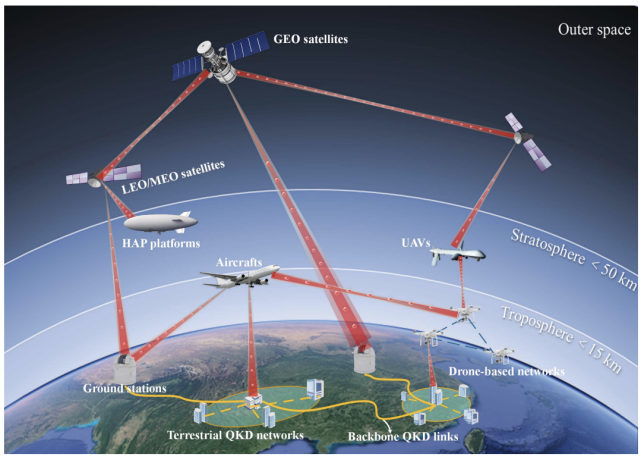


Figure 6.1: Hierachical quantum network operating in different atmospheric layers [136]

users is characterized by considering the geometric spreading loss, atmospheric attenuation, and atmospheric turbulence-induced fading. The numerical results support the parameter selection of transmitter and receiver, which allows the proposed QKD system to work effectively. We also analyze the normalized secret key rate, which is the rate of secure key bits that can be transmitted over a given bandwidth of a communication channel, to confirm the effectiveness of our proposed system. We further investigate the feasibility of a case study for the Japan QKD network using the existing Starlink LEO satellite constellation.

From the beginning of satellite-based FSO/QKD, LEO satellites have recently attracted QKD studies and experiments. LEO satellites benefit from the low channel loss; however, their coverage is limited. The distributing secret keys for two distant ground stations can be implemented by multiple LEO satellites organized into a constellation. Nevertheless, the key relaying/routing in the network of satellites would bring new security concerns. While a GEO satellite with an altitude of 35,768 km can solve the coverage problem, the system suffers from a high path loss and limited key rates. Therefore, combining GEO and LEO satellites is a promising solution for the global-scale QKD network. In chapter 4, we present a novel entanglement-based FSO/QKD system that uses LEO and GEO satellites. Moreover, we focus on designing a system that can support multiple mobile users, which opens the potential to establish a global-scale QKD network in chapter 5. 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. The secret key performance of the proposed system is also given based on the design criteria of transmitters and receivers. M-C simulations are performed to verify analytical results.

6.2 Future Research

We finish this dissertation by briefly discussing some potential areas of future work.

- Firstly, the research on the proposed satellite-based FSO/QKD systems can be extended to remove some simplifications and approximations. Post-processing algorithms for error estimation, error correction, and privacy amplification need to be standardized and validated. Key generation rates of the system can be improved by finding new approaches for the classical optical issues of pointing stabilization, overcoming atmospheric losses, turbulence, and suppressing background noise.

- Secondly, satellite-based FSO/QKD constellation design is an attractive research field. The constellation design problem can be interpreted as a multiple-objective optimization

problem [138]. A constellation of satellites for QKD design needs to maximize the final key creation rates, maximize the availability of satellites for each station, and minimize the cost.

- Thirdly, to expand the coverage and increase the mobility of the global-scale QKD, airborne platforms or high-altitude platforms (HAPs) are ideal mobile nodes that can cooperate with terrestrial-based and satellite-based FSO/QKD to build a global quantum network as shown in Fig. 6.1. Similar to the satellite-based FSO/QKD, diverse flying vehicles have different characteristics and optimum application scenarios. Off-the-shelf drones commonly fly below 500 m under normal conditions. The manned/unmanned aircraft fly in the 5-15 km region while floating vehicles such as HAPs work above 15 km [137]. These vehicles could serve as temporary relays to solve the last-mile quantum key exchange for an inner-city or a field network benefiting from their rapid deployment capabilities. In general, airborne systems present a flexible approach for expanding the scope of quantum communications in time and space.

Appendix A

Approximate expressions for (4.13) and (4.14)

Approximate expressions for (4.13) and (4.14) can be derived by using the Gauss-Hermite quadrature. Particularly, by making a change of variable $y = \frac{\ln\left(h_a^U\right)+(\sigma_X^U)^2}{\sqrt{8\pi}h_a^U\sigma_X^U}$, (4.13) and (4.14) are written in the form $\int_{-\infty}^{\infty} g(y)\exp(-y^2)\mathrm{d}y$, where $g(y)$ is a function of the variable y [32]. Then, using the Gauss-Hermite quadrature, this integral is approximated as [121]

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

where n is the order of approximation, while ω_i and x_i are weight factors and zeros of the Hermite polynomial, respectively. It is worth noting that the Gauss-Hermite used for (4.13) and (4.14) quickly converges to the exact-form expressions for a finite value of n, i.e., n = 20 terms.

Appendix B

Proof of the Equation (5.17)

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

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

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

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

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} = & P(AB_i) - \sum_{1 \leq j \leq N} P(AB_i \cap AB_j) + \sum_{1 \leq j \leq k \leq N} P(AB_i \cap AB_j \cap AB_k) + \ldots \\ & -(-1)^N P(\bigcap_{i=1}^{N} AB_i). \end{aligned} \tag{B.2}$$

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

$$P_{AB_i}^{\text{sift-excl}} = P(AB_i \cap (AB_1)^C \cap (AB_2)^C) = P(AB_i) - P(AB_1 \cap AB_2) \text{ with } i \in \{1, 2\}. \tag{B.3}$$

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

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} &= P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C \\ &\cap (AB_{N+1})^C) \\ &= P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C) \\ &- P(\, AB_i \cap (AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C \\ &\cap (AB_{N+1})) \\ &= S_1 - S_2. \end{aligned} \tag{B.4}$$

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

$$S_1 = P(AB_i) - \sum_{1 \leq j \leq N} P(AB_i \cap AB_j) + \sum_{1 \leq j \leq k \leq N} P(AB_i \cap AB_j \cap AB_k) + \ldots - (-1)^N P(\bigcap_{i=1}^{N} AB_i). \tag{B.5}$$

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

$$\begin{aligned} S_2 &= P(AB_i \cap AB_{N+1} \cap [(AB_1)^C \cap (AB_2)^C \ldots \cap (AB_N)^C]) \\ &= P(AB_i \cap AB_{N+1}) \\ &- P[(AB_i \cap AB_{N+1} \cap AB_1) \cup (AB_i \cap AB_{N+1} \cap AB_2) \\ &\ldots \cup (AB_i \cap AB_{N+1} \cap AB_N)]. \end{aligned} \tag{B.6}$$

Applying inclusion-exclusion principle [135] for the second term of S_2, it is continued to calculate as

$$\begin{aligned} S_2 = P(AB_i \cap AB_{N+1}) &- \sum_{1 \le j \le N} P(AB_i \cap AB_{N+1} \cap AB_j) \\ &+ \sum_{1 \le j \le k \le N} P(AB_i \cap AB_{N+1} \cap AB_j \cap AB_k) - \ldots - (-1)^{N+1} P(\bigcap_{i=1}^{N+1} AB_i). \end{aligned} \tag{B.7}$$

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

$$\begin{aligned} P_{AB_i}^{\text{sift-excl}} = P(AB_i) &- \sum_{1 \le j \le N+1} P(AB_i \cap AB_j) + \sum_{1 \le j \le k \le N+1} P(AB_i \cap AB_j \cap AB_k) \ldots \\ &- (-1)^N P(\bigcap_{i=1}^{N} AB_i) + (-1)^{N+1} P(\bigcap_{i=1}^{N+1} AB_i) \end{aligned} \tag{B.8}$$

The equation for $N+1$ also holds true, establishing the induction step. The equation (5.17) 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.

Appendix C

The Mutual Sift Probability between N User Pairs (In Chapter 5)

In this appendix, the formulas to calculate $P(\bigcap_{j,k=1}^{N} A_j B_l)$ are given. The system parameters are set so that the error probabilities at L_i ($P_{L_1L_2}(0,1)$ and $P_{L_1L_2}(0,1)$) are small enough to neglect (e.g., below 10^{-6}).

Moreover, 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 Alice$_j$ Bob$_l$ are located in adjacent locations in respective cities. The joint probabilities are assumed to be the same for Alice$_j$ and Bob$_l$, respectively. These formulas to calculate $P(\bigcap_{j,k=1}^{N} A_j B_l)$ are listed as follows

$$\begin{aligned} P_1 = & P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^N [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^N \dots \\ & + P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^N [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^N, \end{aligned} \tag{C.1}$$

$$\begin{aligned} P_2 = & \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^N [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{(N-i)} \dots \\ & \times C_{N-1}^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^i + P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^N \dots \\ & \times [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N-i} C_{N-1}^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^i, \end{aligned} \tag{C.2}$$

$$\begin{aligned} P_3 = & \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^N [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)] \dots \\ & \times [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{(N-1-i)} C_{N-1}^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^i \dots \\ & + P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^N [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)] \dots \\ & \times C_{N-1}^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^i [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N-1-i}, \end{aligned} \tag{C.3}$$

$$P_4 = \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{N-i} C_{N-1}^{i} [P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{i} \ldots$$
$$\times [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{N} + P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{N-i} \ldots$$
$$\times C_{N-1}^{i} [P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N}, \tag{C.4}$$

$$P_5 = \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{N-i} C_{N-1}^{i} [P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{i} \ldots$$
$$\times [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)][P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{N-1} \ldots$$
$$+ P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{N-i} \ldots$$
$$\times C_{N-1}^{i} [P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)][P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N-1}, \tag{C.5}$$

$$P_6 = \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{N-i} C_{N-1}^{i} [P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{i} \ldots$$
$$\times [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)][P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{N-i} C_{N-1}^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{i} \ldots$$
$$+ P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{N-i} C_{N-1}^{i} [P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{i} \ldots$$
$$\times [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N-i} C_{N-1}^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{i}, \tag{C.6}$$

$$P_7 = \sum_{i=1}^{N-1} \{P_{L_1L_2}(0,0)[P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{N-i} C_{N-1}^{i} [P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{i} \ldots$$
$$\times [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)][P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{(N-1-i)} \ldots$$
$$\times C_{N-1}^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{i} + P_{L_1L_2}(1,1)[P_{L_1A_j}(0,1) + P_{L_1A_j}(1,0)]^{N-i} \ldots$$
$$C_{N-1}^{i} [P_{L_1A_j}(0,0) + P_{L_1A_j}(1,1)]^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)] \ldots$$
$$\times C_{N-1}^{i} [P_{L_2B_l}(0,0) + P_{L_2B_l}(1,1)]^{i} [P_{L_2B_l}(0,1) + P_{L_2B_l}(1,0)]^{N-1-i}, \tag{C.7}$$

where $P_{L_1,L_2}(o,p)$ is the probability that L_1's received bit o coincides with L_2's received bit p. $P_{L_1,A_j}(q,r)$ is the probability that L_1 transmits bit q and Alice$_j$ receives bit r. $P_{L_2,B_l}(s,t)$ is the probability that L_2 transmits bit s and Bob$_l$ receives bit t. C_{N-1}^{i} is the number of combinations of i users from a set with $N-1$ users.

Finally, the mutual sift probability between N user pairs is calculated as

$$P(\bigcap_{j,l=1}^{N} A_j B_l) = 2\sum_{i=1}^{7} P_i. \tag{C.8}$$

Appendix D

Earth-Satellite Geometry

There is a wide variety of geometric problems in connection with communication satellites. They range from the simple to the extremely complicated. The calculation of link performance (including the effects of atmospheric attenuation, and the calculation of coverage area) and the prediction of the satellite visibility passes all required the solution of some geometric problem. Satellite ground traces and the coverage patterns provided by multiple-satellite constellations also involve an analysis of the earth-satellite geometry [143].

D.1 Orbital Elements and Coordinates Systems

The position in space of a satellite is necessarily determined by four fundamental elements: the orbital plan orientation in space, orbit orientation in that plane, dimensions and shape of orbit and the position of the satellite in its orbit as illustrated in Fig. D.1.

These elements are defined by the orbital parameters, which are semi-major axis a, eccentricity e, inclination i, argument of perigee ω, right ascension of ascending node (RAAN) Ω, true anomaly ν, and mean anomaly M.

In particular, i is the tangle at which the orbit is tilted out of the equatorial plane. Ω is the angle of rotation around Earth spin axis referenced by convention to the direction of Sun at the vernal equinox. ω describes the position of the perigee point relative to the point on the orbit which ascends across the equator. ν is the angle in the orbit plane between the satellite at an instant in time and perigee. M is the angle from perigee through which the satellite would have moved if its motion about Earth had uniform angular velocity.

In a satellite movement around Earth, orbit calculation uses four different Cartesian coordinates:

- Orbital coordinates (O): determine the movement of the satellite in its own orbital plane. The x_0-axis is along the major axis of the orbit. The satellite is following a circle or an ellipse in the (x_o,y_o) plane.

- Inertial coordinates (I): the origin is at the center of Earth, the z_i-axis is along the axis of rotation and the x_i pointing toward the vernal equinox γ

- Greenwich coordinates (G): these coordinates are fixed to Earth and rotating with x_g-axis pointing the Greenwich meridian.

- Topocentric coordinates (H): the origin is at the ground station position with (x_h,y_h) plane tangent to the terrestrial sphere.

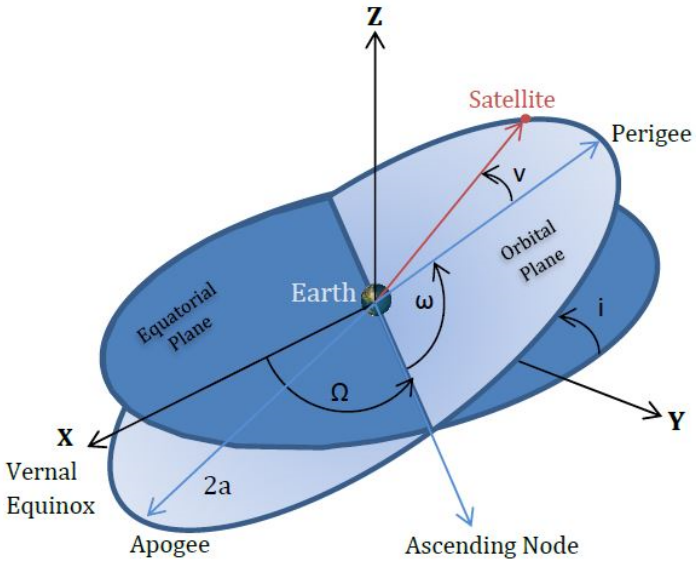


Figure D.1: The orbital plane coordinates [144].

D.2 Orbit Calculation Methodology

The methodology followed in order to calculate the visibility parameters of the satellite is summarized in the following steps:

1. Express satellite position in the orbital plane
2. Transformation to inertial coordinates
3. Transformation to Greenwich coordinates
4. Transformation to topocentric coordinates
5. Computation of elevation angle and slant range

D.2.1 Satellite Orbital Coordinates

The first step is to determine the position of the satellite. For a given orbit semi-major axis a, the period of revolution is

$$T = \frac{2\pi}{n} = 2\pi\sqrt{\frac{a^3}{\mu}}, \tag{D.1}$$

where $\mu = GM = 398600.5km^3/s^2$ is the gravitational constant of Earth and $n = 2\pi/T$ is the mean motion. The mean anomaly at time t is

$$M = n(t - t_e) + M_0, \tag{D.2}$$

where M_0 is the mean anomaly at the specified initial time (epoch) t_e. The eccentric anomaly E is found from Kepler's equation

$$M = E - e\sin E, \tag{D.3}$$

where e is the orbit eccentricity and the true anomaly ν is finally calculated from E using Gauss' equation

$$\tan\frac{\nu}{2} = \left(\frac{1+e}{1-e}\right)^{1/2} \tan\frac{E}{2}. \tag{D.4}$$

The frequently useful magnitude of the radius vector r is given by

$$r = \frac{a(1-e^2)}{1+e\cos\nu} = a(1-e\cos E). \tag{D.5}$$

The coordinates (r,ν) specify the position of the satellite in its own orbital plane. M_0, t_e and n in addition to other parameters are extracted from the satellite ephemeris file published daily by North American Aerospace Defense Command (NORAD).

Then, the satellite coordinates (x_o,y_o,z_o) are given by

$$x_o = r\cos\nu = a(\cos E - e) \tag{D.6}$$

$$y_0 = r\sin\nu = a\sqrt{1-e^2}\sin E \tag{D.7}$$

$$z_0 = 0 \tag{D.8}$$

D.2.2 Transformation to Inertial Coordinates

Once the satellite orbital coordinates are obtained, the next step is a transformation to inertial coordinates. This transformation is done by means of rotations using inclination i, argument of perigee ω and RAAN Ω angles. Using the transformation matrix, the satellite inertial coordinates (x_i,y_i,z_i) are given by

$$\begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} = \begin{bmatrix} \cos\omega\cos\Omega - \sin\omega\sin\Omega\cos i & -\sin\omega\cos\Omega - \cos\omega\sin\Omega\cos i & \sin\Omega\sin i \\ \cos\omega\sin\Omega + \sin\omega\cos\Omega\cos i & -\sin\omega\sin\Omega + \cos\omega\cos\Omega\cos i & -\cos\Omega\sin i \\ \sin\omega\sin i & \cos\omega\sin i & \cos i \end{bmatrix} \times \begin{bmatrix} x_o \\ y_o \\ z_o \end{bmatrix} \tag{D.9}$$

D.2.3 Transformation to Greenwich Coordinates

To obtain the Greenwich coordinates, the inertial coordinates reference frame is rotated using the Greenwich Mean Sideral Time (GMST) angle which is the angle between the vernal equinox and the Greenwich meridian as shown in Fig. D.2.

The Greenwich coordinates (x_g,y_g,z_g) are given by

$$\begin{bmatrix} x_g \\ y_g \\ z_g \end{bmatrix} = \begin{bmatrix} \cos GMST & \sin GMST & 0 \\ -\sin GMST & \cos GMST & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} \tag{D.10}$$

At time t, the $GMTS$ angle is given by

$$GMTS = GMTS_0 + \omega_e t, \tag{D.11}$$

where ω_e is the rate of rotation of Earth and $GMTS_0$ is the Greenwich mean sideral time at midnight Universal Time (UT). The value of $GMST_0$ in degrees may be calculated from the expression

$$GMTS_0 = 24110.^s54841 + 8640184.^s812866T + 0.^s093104T^2 - 0.000006210T^3, \tag{D.12}$$

where T is the time elapsed since January 0, 1900, 12^h UT measured in Julian centuries of

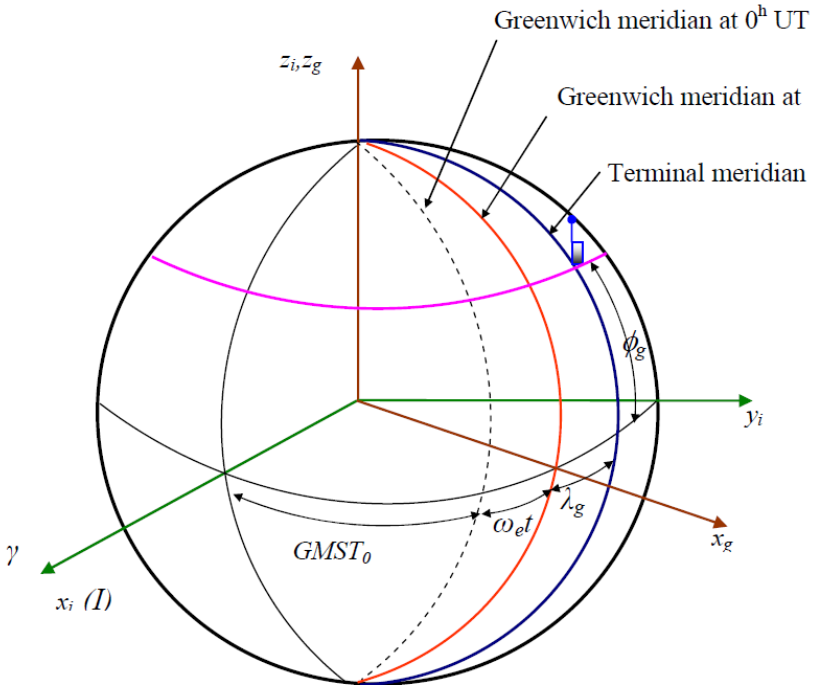


Figure D.2: The geometry of the Greenwich meridian [130]

36525 days of Universal Time. The time T is given by

$$T = \frac{JD - 2451545}{36525} = \frac{d}{365425}, \tag{D.13}$$

where JD is the Julian day number and d is the number of days from the reference date, which itself is Julian day number 2451545 at noon (d is negative before the year 2000).

D.2.4 Ground Station-Satellite Vector in Greenwich Coordinates

The ground station-satellite vector $\vec{\rho_g}$ coordinates in the Greenwich coordinates (ρ_{gx},ρ_{gy},ρ_{gz}) are obtained by subtracting the terminal coordinates from the satellite coordinates

$$\begin{cases} \rho_{gx} = x_g - x'_g \\ \rho_{gy} = y_g - y'_g \\ \rho_{gz} = z_g - z'_g \end{cases}. \tag{D.14}$$

The terminal coordinate (x'_g,y'_g,z'_g) are calculated using the geocentric latitude and longitude of the station. Earth has an equatorial radius R_E of 6378.137 km and a polar radius R_P of 6356,755 km. We have ϕ_g, λ_g and h are respectively the geographic latitude, the longitude and the altitude of the station, then the geocentric latitude ϕ_{gc} and the earth radius r_t at the station position are calculated from the expressions:

$$\phi_{gc} = \arctan\left(\frac{R_P}{R_E}\tan\phi_g\right) \tag{D.15}$$

$$r_t = h + \frac{R_E R_P}{\sqrt{(R_E \sin\phi_g c)^2 + (R_P \cos\phi_{gc})}} \tag{D.16}$$

Then, the coordinates of the ground station in the Greenwich system are given by

$$\begin{cases} x'_g &= r_t \text{cos}\lambda_g \text{cos}\phi_{gc} \\ y'_g &= r_t \text{sin}\lambda_g \text{cos}\phi_{gc} \\ z'_g &= r_t \text{sin}\phi_{gc} \end{cases}. \tag{D.17}$$

D.2.5 Ground Station-Satellite Vector in Topocentric Coordinates

The next step is to transform the ground station-satellite vector to the topocentric coordinates. This is achieved by rotating the Greenwich system using the station geocentric latitude ϕ_{gc} and longitude λ_g. Therefore, the $\vec{\rho_t}$ vector coordinates are given by the transformation

$$\begin{bmatrix} \rho_t x \\ \rho_t y \\ \rho_t z \end{bmatrix} = \begin{bmatrix} \text{sin}\phi_{gc}\text{cos}\lambda_g & \text{sin}\phi_{gc}\text{cos}\lambda_g & -\text{cos}\phi_{gc} \\ -\text{sin}\phi_g & \text{cos}\phi_g & 0 \\ \text{sin}\phi_{gc}\text{cos}\lambda_g & \text{cos}\phi_{gc}\text{sin}\lambda_g & \text{sin}\phi_{gc} \end{bmatrix} \times \begin{bmatrix} \rho_{gx} \\ \rho_{gy} \\ \rho_{gz} \end{bmatrix} \tag{D.18}$$

D.2.6 Calculating Elevation Angle and Slant Range between the Satellite and the Ground Station

The elevation angle El and the slant range d of the satellite are computed using the ground station-satellite vector coordinates in the topocentric coordinates as follow

$$d = \sqrt{\rho_{tx}^2 + \rho_{ty}^2 + \rho_{ty}^2} \tag{D.19}$$

$$El = \text{arcsin}\left(\frac{\rho_{tz}}{d}\right) \tag{D.20}$$

Appendix E

NORAD Two-Line Element Set Format

Data for each satellite consists of three lines in the format as shown in Fig. E.1.

Line 0 is a twenty-four character name (to be consistent with the name length in the NORAD Satellite Catalog (SATCAT)).

Line 1 and 2 are the two-line orbital element set format which consists of two 69-character lines of data which can be used to determine the position of the associated satellite. The only valid characters in a two-line element set are the numbers 0-9, the capital letters A-Z, the period, the space, and the plus and minus signs.

All other columns are blank or fixed.

An example of two-line element set for a satellite in Starlink constellation is given in Fig. E.2.

Tables E.1 and E.2 define each of the individual fields for lines 1 and 2, respectively.

```
AAAAAAAAAAAAAAAAAAAAAAA
1 NNNNNU NNNNNAAA NNNNN.NNNNNNNN +.NNNNNNNN +NNNNN-N +NNNNN-N N NNNNN
2 NNNNN NNN.NNNN NNN.NNNN NNNNNNN NNN.NNNN NNN.NNNN NN.NNNNNNNNNNNNN
```

Figure E.1: Two-line element set format [145].

```
Starlink-2166
1 48558C 21041F   21357.16057992  .00002702  00000-0  18107-3 0  3574
2 48558  53.0520 193.8605 0002488  81.6392 166.2671 15.06384617    11
```

Figure E.2: An example two-line element set for a satellite in Starlink constellation.

Table E.1: Two-Line Element Set Format Definition, Line 1

Field	Column	Description	Example
1.1	01	Line Number of Element Data	1
1.2	03-07	Satellite Number	48558
1.3	08	Classification	C
1.4	10-11	International Designator (Last two digits of launch year)	21
1.5	12-14	International Designator (Launch number of the year)	041
1.6	15-17	International Designator (Piece of the launch)	F
1.7	19-20	Epoch Year (Last two digits of year)	21
1.8	21-32	Epoch (Day of the year and fractional portion of the day)	357.16057992
1.9	34-43	First Time Derivative of the Mean Motion	.00002702
1.10	45-52	Second Time Derivative of the Mean Motion (decimal point assumed)	00000-0
1.11	54-61	BSTAR drag term (decimal point assumed)	18107-3
1.12	63	Ephemeris type	0
1.13	65-68	Element number	357
1.14	69	Check sum (Modulo 10) (Letters, blanks, periods, plus signs = 0; minus signs =1)	4

Table E.2: Two-Line Element Set Format Definition, Line 2

Field	Column	Description	Example
2.1	01	Line Number of Element Data	2
2.2	03-07	Satellite Number	48558
2.3	09-16	Inclination [Degrees]	53.0520
2.4	18-25	Right Ascension of the Ascending Node [Degrees]	193.8605
2.5	27-33	Eccentricity (decimal point assumed)	0002488
2.6	35-42	Argument of Perigee [Degrees]	81.6392
2.7	44-51	Mean Anomaly [Degrees]	166.2671
2.8	53-63	Mean Motion [Revs per day]	15.063894617
2.9	64-68	Revolution Number at Epoch [Revs]	1
2.10	69	Checksum (Modulo 10)	1

References

[1] I. Khan *et al.,* "Satellite-based QKD," *Optics & Photonics News,* Feb. 2018.

[2] C. Bennett, and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing.", *International Conference on Computers, Systems & Signal Processing,* Bangalore, India, pp. 175-179, Dec. 1984.

[3] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," *in 2012 IEEE Conference on Technologies for Homeland Security (HST),* 2012, pp. 156–161.

[4] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.,* vol. 88, pp. 3762-3764, Mar. 2004.

[5] A. Poppe *et al.*, "Practical quantum key distribution with polarization entangled photons," *Opt. Exp.,* vol. 12, no. 16, pp. 3865-3871, 2004.

[6] P. A. Hiskett *et al.*, "Long-distance quantum key distribution in optical fibre," *New J. Phys.,* vol. 8, Art. no. 193, Sep. 2006.

[7] J. Lodewyck *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, no. 4, Art. no. 042305, Oct. 2007.

[8] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A.,* vol. 76, no. 5, Art. no. 052323, Nov. 2007.

[9] W. Buttler *et al.*, "Free-space quantum-key distribution," *Phys. Rev. A,* vol. 57, no. 4, pp. 2379–2382, Apr. 1998.

[10] W. Buttler *et al.*, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.,* vol. 81, no. 15, pp. 3283-3286, Oct. 1998.

[11] W. Buttler *et al.*, "Daylight Quantum Key Distribution over 1.6 km," *Phys. Rev. Lett.,* vol. 84, no. 24, pp. 5652-5655, Jun. 2000.

[12] J. Rarity, P. M. Gorman, and P. R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography," *Electronics Letters,* vol. 37, no. 8, pp. 512-514, Apr. 2001.

[13] R. Hughes *et al.*, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.,* vol. 4, pp. 43, Jan. 2002.

[14] B.-X. Wang, Y. Mao, L. Shen, L. Zhang, X.-B. Lan, D. Ge, Y. Gao, J. Li, Y.-L. Tang, S.-B. Tang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber," *Opt. Express,* vol. 28, no. 9, pp. 12 558–12 565, Apr 2020. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-28-9-12558

[15] Y.-H. Gong, K.-X. Yang, H.-L. Yong et al., "Free-space quantum key distribution in urban daylight with the spgd algorithm control of a deformable mirror," *Opt. Express,* vol. 26, no. 15, pp. 18 897–18 905, Jul. 2018.

[16] Y. Cao, H. Liang, J. Yin, H.-L. Yong, F. Zhou, Y.-P. Wu, J.-G. Ren, Y.-H. Li, G.-S. Pan, T. Yang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Entanglement-based quantum key distribution with biased basis choice via free space," *Opt. Express,* vol. 21, no. 22, pp. 27 260–27 268, Nov 2013. [Online]. Available: https://opg.optica.org/oe/abstract.cfm?URI=oe-21-22-27260

[17] S. K. Liao *et al.,* "Satellite-to-ground quantum key distribution," *Nature,* vol. 549, pp. 44-47, Aug. 2017.

[18] J. G. Ren *et al.,* "Ground-to-satellite quantum teleportation," *Nature,* vol. 549, pp. 70-73, Sep. 2017.

[19] J. Yin *et al.,* "Satellite-based entanglement distribution over 1200 kilometers," *Science,* vol. 356, no. 6343, pp. 1140-1144, Jun. 2017.

[20] N. Hosseinidehaj and R. Malaney, "CV-MDI quantum key distribution via satellite," *Quantum Inf. Comput.,* vol. 17, nos. 5-6, pp. 361-379, 2017.

[21] D. Oi *et al.,* "CubeSat quantum communications mission," *EPJ Quantum Technology,* vol. 4, Art. no. 6, Apr. 2017.

[22] J. Grieve *et al.,* "SpooQySats: CubeSats to demonstrate quantum key distribution technologies," *Acta Astronautica,* vol. 151, pp. 103-106, Oct. 2018.

[23] E. Kerstel *et al.,* "Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration," *EPJ Quantum Technology,* vol. 5, Art. no. 6, Jun. 2018.

[24] S. Neumann *et al.,* "Q3Sat: quantum communications uplink to a 3U CubeSat—feasibility & design," *EPJ Quantum Technology,* vol. 5, Art. no. 4, Apr. 2018.

[25] D. Dequal *et al.,* "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information,* vol. 7, Art. no. 3, 2021.

[26] 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, Art. no. 090302, 2017.

[27] S. K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Art. no. 030501, Jan. 2018.

[28] R. Bedington, X. Bai, E. Truong-Cao, Y. Tan, K. Durak, A. Villar Zafra, J. Grieve, D. Oi, and A. Ling, "Nanosatellite experiments to enable future space-based qkd mission," *EPJ Quantum Technology,* vol. 3, p. 12, Dec. 2016.

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

[30] J. Yin *et al.,* "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature,* vol. 582, pp. 501-505, Jun. 2020.

[31] N. Hosseinidehaj, Z. Babar, R. Malaney et al., "Satellite-based continuous variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys Tutorials,* vol. 21, no. 1, pp. 881–919, 2019.

[32] 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.

[33] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npi Quantum Information*, vol. 2, Art. no. 16025, Nov. 2016.

[34] N. Wang *et al.,* "Long-distance continuous-variable quantum key distribution with entangled states," *Phys. Rev. Applied,* vol. 10, no. 6, Art. no. 064028, Dec. 2018.

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

[36] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.,* vol. 68, no. 5, pp. 557-559, Feb. 1992.

[37] D. Dieks, "Communication by EPR devices," *Phys. Lett. A,* vol. 92, no. 6, pp. 271-272, Nov. 1982.

[38] H. K. Lo, M. Curty, and K. Tamaki, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050-2056, Mar. 1999.

[39] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441-444, Jul. 2000.

[40] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351-406, May 2001.

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

[42] C. H. Bennett, F. Bessette, G. Brassard *et al.*, "Experimental quantum cryptography," *J. Cryptography*, vol. 5, pp. 3-28, Jan. 1992.

[43] T. Ralph, "Continuous variable quantum cryptography," *Phy. Rev. A,* vol. 61, no. 1, Art. no. 010303, Dec. 1999.

[44] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A,* vol. 61, no. 2, Art. no. 022309, Jan. 2000.

[45] N. Cerf *et al.,* "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A,* vol. 63, no. 5, Art. no. 052311, Apr. 2001.

[46] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.,* vol. 88, no. 5, Art. no. 057902, Jan. 2002.

[47] A. Muller *et al.*, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *Europhysics Letters (EPL),* vol. 23, no. 6, pp. 383–388, 1993.

[48] A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding," *Nature* vol. 378, 449, Nov. 1995

[49] P. Townsend, "Quantum cryptography on optical fiber networks," *Proc. SPIE 3385, Photonic Quantum Computing II,* Jul. 1998.

[50] J. P. Chen *et al.*, "Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, Art. no. 070501, Feb. 2020.

[51] X. T. Fang *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nat. Photonics,* vol. 14, pp. 422-425, Mar. 2020.

[52] S. K. Joshi *et al.*, "Space QUEST mission proposal: experimentally testing decoherence due to gravity," *New J. Phys.,* vol. 20, Art. no. 063016, Jun. 2018.

[53] H. Podmore *et al.*, "Optical Terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat)," *2019 IEEE International Conference on Space Optical Systems and Applications (ICSOS),* Portland, OR, USA, pp. 1-5, Oct. 2019.

[54] L. Mazzarella *et al.*, "QUARC: Quantum Research Cubesat—A constellation for quantum communication," *Cryptography 2020,* vol. 4, no. 1, Feb. 2020

[55] H. Takenaka *et al.*, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photon.,* vol. 11, pp. 502-508, Jul. 2017.

[56] P. Marks, "Quantum cryptography to protect Swiss election," *New Scientist*, Oct. 2007. [Online]. Available: https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

[57] H. Johnston, "Encryption kicks off in the quantumStadium," *Physics World,* May 2010. [Online]. Available: https://physicsworld.com/a/playing-in-the-quantumstadium/

[58] V. Scarani *et al.*, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301-1350, Sep. 2009.

[59] S. L. Braunstein, and P. V. Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, no. 77, no. 2, pp. 513-577, Jun. 2005.

[60] F. Karinou *et al.,* "Toward the integration of CV quantum key distribution in deployed optical networks," *IEEE Photon. Technol. Lett.,* vol. 30, no. 7, pp. 650-653, Apr. 2018.

[61] T. Hirano *et al.*, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Science and Technology,* vol. 2, no. 2, Art.no. 024010, Jun. 2017.

[62] D. Gottesman, and J. Preskill, "Secure quantum key distribution using squeezed states," *Phys. Rev. A*, vol. 63, no. 2, Art.no. 022309, Jan. 2001.

[63] F. Grosshans *et al.*, "Quantum key distribution using gaussian-modulated coherent states," *Nature,* vol. 421, pp. 238-241, Jan. 2003.

[64] C. Weedbrook *et al.*, "Quantum cryptography without switching," *Phys. Rev. Lett.,* vol. 93, no. 17, Art. no. 170504, Oct. 2004.

[65] A. M. Lance *et al.*, "No-switching quantum key distribution using broadband modulated coherent light," *Phys. Rev. Lett.,* vol. 95, no. 18, Art. no. 180503, Oct. 2005.

[66] R. G. Patron and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," *Phys. Rev. Lett.,* vol. 102, no. 13, Art. no. 130501, Mar. 2009.

[67] Y. B. Zhao, M. Heid, J. Rigas, and N. Lutkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," *Phys. Rev. A,* vol. 79, no. 1, Art. no. 012307, Jan. 2009.

[68] K. Bradler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Phys. Rev. A,* vol. 97, no. 2, Art. no. 022310, Feb. 2018.

[69] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Phys. Rev. Lett.,* vol. 102. no. 18, Art. no. 180504, May 2009.

[70] X. Ma, C. H. F. Fung, and H. K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, no. 1, Art. no. 012307, Jul. 2007.

[71] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite" *Phys. Rev. A,* vol. 91, no. 2, Art. no. 022304, Feb. 2015.

[72] N. Hosseinidehaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," in *Proc. IEEE International Conference on Communications (ICC),* London, pp. 7413-7419, Sep. 2015.

[73] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," Opt. Express, vol. 16, no. 21, pp. 16840-16853, 2008.

[74] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.,* vol. 74, no. 1, pp. 145-195, Mar. 2002.

[75] D. Rosenberg *et al.*, "Practical long-distance quantum key distribution system using decoy-levels," *New J. Phys.,* vol. 11, Art. no. 045009, Apr. 2009.

[76] Q. D. Xuan, Z. Zhang, and P. L. Voss, "A 24-km fiber-based discretely signaled continuous variable quantum key distribution system," *Opt. Exp.,* vol. 17, no. 26, pp. 24244-24249, Dec. 2009.

[77] P. Jouguet *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photon.*, vol. 7, no. 5, pp. 378-381, Apr. 2013.

[78] D. Stucki *et al.*, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New J. Phys.,* vol. 11, no. 7, Jul. 2009.

[79] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.,* vol. 9, no. 3, pp. 163-168, Feb. 2015.

[80] H. L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.,* vol. 117, no. 19, Nov. 2016.

[81] C. Peng *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Phys. Rev. Lett.,* vol. 94, no. 15, Art. no. 150501, Apr. 2005.

[82] K. J. Resch *et al.*, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Opt. Exp.,* vol. 13, no. 1, pp. 202-209, Jan. 2005.

[83] I. Marcikicm, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," *Appl. Phys. Lett.,* vol. 89, no. 10, Art. no. 101122, Sep. 2006.

[84] R. Hughes *et al.*, "Free-space quantum key distribution in daylight," *Journal of Modern Optics,* vol. 47, pp. 549-562, 2000.

[85] J. Yin *et al.*, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature* vol. 488, pp. 185-188, 2012.

[86] B. Hem *et al.*, "Atmospheric continous-variable quantum communication," *New J. Phys.,* vol. 16, Art. no. 113018, 2015.

[87] S. K. Liao *et al.,* "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics,* vol. 11, pp. 509-513, Jul. 2017.

[88] M. Aspelmeyer *et al.*, "Long-distance quantum communication with entangled photons using satellites," *IEEE Journal of Selected Topics in Quantum Electronics,* vol. 9, no. 6, pp. 1541-1551, 2003.

[89] M. Pfennigbauer *et al.*, "Satellite-based quantum communication terminal employing state-of-the-art technology," *J. Opt. Netw.*, vol. 4, pp. 549-560, 2005.

[90] C. Bonato *et al.*, "Feasibility of satellite quantum key distribution," *New Journal of Physics,* vol. 11, no. 4, Art. no. 045017, 2009.

[91] L. Sanchez *et al.*, "Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links," *IEEE Journal on Selected Areas in Communications,* vol. 27, no. 9, pp. 1582-1590, 2009.

[92] 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.

[93] M. Q. Vu, N. T. Dang, and A. T. Pham, "HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks," *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, pp. 1-6, Apr. 2019.

[94] 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.

[95] Ch. Silberhorn, N. Korolkova, and G. Leuchs, "Quantum key distribution with bright entangled beams," *Phys. Rev. Lett.,* vol. 88, no. 16, Art. no. 167902, Apr. 2002.

[96] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A,* vol. 91, no. 2, Art. no. 022304, Feb. 2015.

[97] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and non-Gaussian entangled states over satellite-based channels," *2016 IEEE Global Communications Conference (GLOBECOM),* Washington, DC, pp. 1-7, Dec. 2016.

[98] N. Hosseinidehaj and R. Malaney, "Quantum entanglement distribution in next-generation wireless communication Systems," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, pp. 1-7, Jun. 2017.

[99] N. Walk *et al.,* "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," *Optica,* vol. 3, no. 6, pp. 634-642, Jun. 2016.

[100] M. Mehic, M. Niemiec, S. Rass, J. Ma et al., "Quantum key distribution: A networking perspective," *ACM Comput. Surv.,* vol. 53, no. 5, Sep. 2020, Art. no. 96.

[101] Y. Cao *et al.,* "Long-distance free-space measurement-device-independent quantum key distribution," *Phys. Rev. Lett.,* vol. 125, no. 26, Art. no. 260503, Dec. 2020.

[102] P. Villoresi *et al.,* "Experimental verification of the feasibility of a quantum channel between space and the Earth," *New J. Phys.,* vol. 10, Art. no. 33038, 2008.

[103] G. Vallone *et al.,* "Experimental satellite quantum communications," *Phys. Rev. Lett.,* vol. 115, no. 4, Art. no. 040502, Jul. 2015.

[104] S. K. Liao *et al.,* "Ground test of satellite constellation based quantum communication," arXiv preprint:1611.09982, 2016

[105] D. Dequal *et al.,* "Experimental single photon exchange along a space link of 7000 km," *Phys. Rev. A,* vol. 93, Art. no. 010301, 2016.

[106] L. Calderaro *et al.,* "Towards quantum communication from global navigation satellite system," *Quantum Sci. Technol.,* vol. 4, Art. no. 015012, 2019.

[107] K. Gunthner *et al.,* "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica,* vol. 4, Art. no. 611, 2017.

[108] 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.

[109] F. Yu. *ScienceNet.cn, China. Accessed:* Aug. 10, 2017. [Online]. Available: http://news.sciencenet.cn/htmlnews/2017/8/384831.shtm?id=384831

[110] D. Huang, Y. Zhao, T. Yang et al., "Quantum key distribution over double layer quantum satellite networks," IEEE Access, vol. 8, pp. 16 087–16 098, 2020.

[111] Le, Hoang D. and Trinh, Phuc V. and Pham, Thanh V. and Kolev, Dimitar R. and Carrasco-Casado, Alberto and Kubo-Oka, Toshihiro and Toyoshima, Morio and Pham, Anh T., "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.

[112] Hoang D. Le and Anh T. Pham, "Level crossing rate and average fade duration of satellite-to-uav fso channels," IEEE Photonics Journal, vol. 13, no. 1, pp. 1–14, 2021.

[113] Li, Jinye and Yao, Yuan and Wu, Guozhang and Hou, Jiaqing and Yu, Wenqi and Liu, Bo and Liu, Jianguo, "Broadband laser Doppler frequency shift emulator for satellite laser communication," *IEEE Photonics Journal,* vol. 11, no. 6, pp. 1–12, 2019.

[114] Bahaa E. A. Saleh, Malvin Carl Teich, *Beam Optics.* JohnWiley & Sons, Ltd, 1991, ch. 3, pp. 80–107.

[115] A. A. Farid and S. Hranilovic, "Outage capacity optimization for freespace optical links with pointing errors," *Journal of Lightwave Technology,* vol. 25, no. 7, pp. 1702–1710, 2007.

[116] Larry C. Andrews and R. L. Phillips, *Laser beam propagation through random media,* 2nd ed. Bellingham, Washington USA: SPIE Press Book, 2005.

[117] J. L. Green, B. W. Welch, and R. M. Manning, "Optical communication link atmospheric attenuation model," *National Aeronautics and Space Administration,* Feb. 2019. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190001012.pdf

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

[119] H. Hemmati, *Near-Earth laser communication,* 2nd ed. Boca Raton, FL, USA: CRC Press, 2009.

[120] Hemani Kaushal, V.K. Jain, Subrat Kar, *Free space optical communication,* 1st ed. New Delhi, India: Springer, 2017.

[121] Z. Ghassemlooy, W. Popoola, S. Rajbhandari, *Optical wireless communication: system and channel modeling with MATLAB,* 1st ed. Boca Raton, FL USA: CRC Press, 2013.

[122] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of fso communications over málaga channels," *IEEE Photonics Journal,* vol. 12, no. 6, pp. 1–17, 2020.

[123] Pham, Thanh V. and Thang, Truong C. and Pham, Anh T., "Average achievable rate of spatial diversity mimo-fso over correlated gamma–gamma fading channels," *Journal of Optical Communications and Networking,* vol. 10, no. 8, pp. 662–674, 2018.

[124] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal,* vol. 27, no. 4, pp. 623–656, 1948.

[125] T. Duan and V. Dinavahi, "Starlink space network-enhanced cyberphysical power system," *IEEE Transactions on Smart Grid,* vol. 12, no. 4, pp. 3673–3675, 2021.

[126] S. Clark, "Spacex launches more starlink satellites, beta testing well underway." [Online]. Available: http://spaceflightnow.com 2020/09/03/spacex-launches-more-starlink-satellites-beta-testing-well-underway/

[127] CelesTrak, "Celestrak orbit visualization." [Online]. Available: https://celestrak.com/

[128] M. Q. Vu *et al.*, "Toward Practical Entanglement-Based Satellite FSO/QKD Systems Using Dual-Threshold/ Direct Detection," in IEEE Access, vol. 10, pp. 113260-113274, 2022.

[129] Z. Yong Wang, J. Lin Li, Q. Guo, and X. Mai Gu, "Analysis on connectivity of inter-orbit-links in a meo/leo double-layer satellite network," Chinese Journal of Aeronautics, vol. 19, no. 4, pp. 340–345, 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1000936111603385

[130] E. B. Zantou, A. Kherras, and A. Addaim, "Orbit calculation and doppler correction algorithm in a leo satellite small ground terminal," 2005.

[131] K. Bessho, K. Date, M. Hayashi, *et al.*, "An introduction to himawari-8/9— japan's new-generation geostationary meteorological satellites," J. Meteorol. Soc. Jpn., vol. 94, pp. 151– 183, 04 2016.

[132] S. Cakaj, "The parameters comparison of the "starlink" leo satellites constellation for different orbital shells," Frontiers in Communications and Networks, vol. 2, 2021. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frcmn.2021.643095

[133] A. Lyon, "Why are normal distributions normal?" The British Journal for the Philosophy of Science, vol. 65, no. 3, pp. 621–649, 2014. [Online]. Available: https://www.jstor.org/stable/26398398

[134] L. J. Kazmier, "Schaum's outline of business statistics," 1976.

[135] E. W. Weisstein, "Inclusion-exclusion principle. From MathWorld—A Wolfram Web Resource," last visited on 12/25/2022. [Online]. Available: `https://mathworld.wolfram.com/Inclusion-ExclusionPrinciple.html`

[136] Y. Xue, W. Chen, S. Wang, Z. Yin, L. Shi, and Z. Han, "Airborne quantum key distribution: a review [Invited]," *Chin. Opt. Lett.* 19, Art. No. 122702- (2021).

[137] M. Sharma, D. Chadha, and V. Chandra, "High-altitude platform for free-space optical communication: performance evaluation and reliability analysis," *J. Opt. Commun. Netw.* vol. 8, pp. 600–609, 2016.

[138] M. Asvial, R. Tafazolli, and B. Evans, "Satellite constellation design and radio resource management using genetic algorithm." *In IEE Proc. Commun.*, vol. 153, pp. 633–638, 2004.

[139] G. Murta, F. Grasselli, H. Kampermann, D. Bruß, "Quantum conference key agreement: a review. advanced quantum," *Advanced Quantum Technologies*, vol. 338, no.11, Art. no. 2000025.

[140] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik and A. Fedrizzi, "Experimental quantum conference key agreement," *Science Advances*, vol. 7, no. 23, Art. no. eabe0395, 2021.

[141] D. Giggenbach and A. Shrestha, "Atmospheric absorption and scattering impact on optical satellite-ground links," *International Journal of Satellite Communications and Networking*, vol. 40, no. 2, pp. 157–176, 2022.

[142] Y. Teng, M. Zhang, and S. Tong, "High precision implementation with design considerations and experimental tracking results for single-sensor optical communication terminal," *IEEE Photonics Journal*, vol. 11, no. 4, pp. 1–9, 2019.

[143] W. L. Pritchard, H. G. Suyderhound, R. A. Nelson, *Satellite communication systems engineering,* 2nd ed., Prentice Hall, 1993.

[144] "Orbital elements and unity's left handed co-ordinate system," [Online]. Available: https://nbodyphysics.com/blog/gravity-engine-doc-1-3-2-2-2/orbital-elements-and-unitys-left-handed-co-ordinate-system/

[145] T. S. Kelso, "Frequently asked questions:Two-line element set format." [Online]. Available: https://celestrak.com/

[146] H. Donovan, "Reduction of the minimum elevation angle for NASA satellite laser ranging tracking operations," MD, USA: Honeywell, 2001. [Online].