hv photonics

IMPACT FACTOR 1.9

CITESCORE 3.5

Article

Quantum-Enhanced Security Framework for Next-Generation Space–Terrestrial Networks

Chengbin Huang, Jiangang Tong, Shengkai Liao, Jinhua Wang, Fei Zhou, Weiwen Kong, Yan Jiang, Yang Xie, Qianran Wang, Yue Zhang et al.

Special Issue

Advanced Optical Transmission Techniques

Edited by

Dr. Zhipei Li, Dr. Xishuo Wang and Dr. Weiwen Kong

MDPI

https://doi.org/10.3390/photonics12121182

photonics

MDPI

Article

Quantum-Enhanced Security Framework for Next-Generation Space–Terrestrial Networks

Chengbin Huang [1,*], Jiangang Tong [1], Shengkai Liao [2,3], Jinhua Wang [1], Fei Zhou [4], Weiwen Kong [1], Yan Jiang [1], Yang Xie [1], Qianran Wang [1], Yue Zhang [1] and Jinhui Li [1]

[1] China Telecom Research Institute, Shanghai 201315, China
[2] Hefei National Laboratory, University of Science and Technology of China, Hefei 230026, China
[3] Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China
[4] Jinan Institute of Quantum Technology, Jinan 250101, China
* Correspondence: huangchb@chinatelecom.cn

Abstract

Advancements in Non-Terrestrial Network (NTN) technology facilitate ubiquitous network access for users, whereas satellite-based Quantum Key Distribution (QKD) offers a viable solution for long-distance quantum key exchange in scenarios lacking terrestrial network infrastructure. This study explores the feasibility and practical utility of integrating NTN technology with satellite-based QKD and proposes a novel quantum-enhanced security framework for next-generation space–terrestrial networks. We have developed and deployed the first-of-its-kind 5G-enabled (fifth generation mobile communication) NTN prototype system leveraging satellite-based QKD key encryption. This system comprises a quantum satellite system, a communication satellite system, a 5G network infrastructure, and end-to-end encryption/decryption modules, aiming to validate the feasibility and usability of the proposed quantum-encrypted NTN security framework. Comprehensive tests and performance evaluations were carried out on the testbed constructed based on this prototype system, which collected critical Quality of Experience (QoE) metrics, including Round-Trip Time (RTT) and jitter, during user-plane ping measurements. Experimental results demonstrate that the integration of quantum encryption capabilities incurs an RTT overhead of 5 ms (0.75%), a necessary trade-off for systems incorporating supplementary quantum-encrypted transmission. Concurrently, the deployment of Virtual Private Network (VPN) infrastructure mitigates network jitter by 50%. These results hold critical theoretical and practical implications for the development of next-generation NTN security frameworks enabled by satellite-based QKD.

Keywords: quantum key distribution (QKD); satellite-based QKD; quantum-enhanced security framework; quantum encrypted NTN

Received: 7 November 2025
Revised: 23 November 2025
Accepted: 27 November 2025
Published: 30 November 2025

Citation: Huang, C.; Tong, J.; Liao, S.; Wang, J.; Zhou, F.; Kong, W.; Jiang, Y.; Xie, Y.; Wang, Q.; Zhang, Y.; et al. Quantum-Enhanced Security Framework for Next-Generation Space–Terrestrial Networks. *Photonics* **2025**, *12*, 1182. https://doi.org/10.3390/photonics12121182

1. Introduction

In recent years, quantum technology has emerged as a frontier domain in the global technological revolution and industrial transformation. Current research focuses on three principal areas: quantum computing, quantum communication, and quantum precision measurement. Among these, quantum communication demonstrates the highest technological maturity, having achieved significant breakthroughs in technical feasibility verification, practical device development, and industrial ecosystem cultivation [1]. Worldwide, nations are actively engaged in the research and deployment of both terrestrial and

satellite-based QKD networks. To date, China has established the world's most extensive quantum-secure communication network. The landmark satellite-based QKD experiment has extended QKD capabilities from thousands to tens of thousands of kilometers, enabling secure Quantum Key Distribution to achieve broader geographic coverage [2,3].

Traditional terrestrial mobile communication systems face limitations imposed by base station placement and optical fiber deployment constraints. The advancement of mobile satellite communication technology addresses these challenges by providing coverage to remote areas and enabling emergency communications where conventional 5G networks prove inadequate [4]. Ensuring space–terrestrial link security is vital for maritime missions and connectivity-deprived regions.

With the advancement of satellite technology, High Throughput Satellite (HTS) communication systems have emerged as a critical complement to terrestrial mobile communication networks. Characterized by extensive coverage, high-bandwidth capacity, and cost-effectiveness, HTS systems now represent a predominant developmental trajectory in satellite communications. Standardization bodies, including the International Telecommunication Union (ITU) and Third Generation Partnership Project (3GPP), have initiated the standardization process for 5G-enabled satellite communications, thereby facilitating the establishment of an integrated space–terrestrial communication architecture [5,6]. Concurrently, global initiatives are actively deploying emergency communication infrastructure in remote regions to strengthen the resilience of regional communication networks. The global satellite communication market size was estimated at USD 90,299.1 million in 2024 and is projected to reach USD 159,599.2 million by 2030, growing at a Compound Annual Growth Rate (CAGR) of 10.2% from 2025 to 2030 [7].

Recent years have witnessed a surge in sophisticated cyberattacks targeting Critical Information Infrastructure (CII), with evolving attack vectors demonstrating increased technical complexity. Statistical data reveal exponential growth in cyber threats against CII, constituting significant risks to national security and societal stability globally. The operational integrity of CII now confronts unprecedented security challenges, as exemplified by *The New York Times*' documented breach of SpaceX's Starlink network by Russian actors [8], which has precipitated legitimate concerns regarding the system's security assurances among stakeholders.

This work aims to integrate satellite-based QKD into next-generation NTN, thereby enabling users in regions beyond the coverage of terrestrial networks to securely distribute quantum keys and to achieve satellite communications based on quantum encryption, so as to safeguard user privacy and data security. We developed a 5G-enabled satellite communication testbed incorporating satellite-based QKD and validated the feasibility of the integrated architecture through testing user experience metrics such as RTT and jitter.

To the best of our knowledge, this study advances the exploration of a quantum-encrypted NTN integration architecture through investigating the implementation of satellite-based QKD in the NTN framework—an approach that remains unprecedented to date. We propose a testbed implemented using a suite of devices, encompassing the "Jinan-1" quantum satellite, "Chinasat-26" communication satellite, 5G network, ground stations, and IP Sec VPNs, with the employed satellite networks being commercial off-the-shelf systems, thereby constructing an experimental environment for quantum-encrypted NTN. From this testbed, we collected both the time metrics of conventional 5G NTN and those of quantum-encrypted 5G NTN to evaluate the overall system performance, and the obtained results offer valuable implications for the development of potential next-generation NTN systems based on satellite-based QKD. However, it is important to note that while the integration of external commercial services into the testbed enables the

acquisition of more realistic data metrics, its intrinsic black-box characteristics inevitably incur numerous assumptions and technical constraints.

In this experiment, we adopted GEO-based NTN links to verify the feasibility of the proposed scheme. Geostationary Earth Orbit (GEO) satellites feature lower deployment costs and network complexity, with only three satellites required to achieve global coverage. Notably, Low Earth Orbit (LEO) satellite constellations are developing rapidly, and we plan to conduct follow-up experiments based on LEO constellations to meet the demands of low-latency communication scenarios (e.g., Sixth-Generation Mobile Communication Technology, 6G). Based on this, we anticipate that GEO-based NTN and LEO-based NTN will coexist for a prolonged period. Furthermore, this experiment utilized a single standalone LEO quantum satellite (rather than a satellite constellation). For a specific ground station, the quantum satellite only passes overhead once per night— the daytime pass is unavailable due to intense solar background light, which interferes with the ground station's reception of optical signals transmitted by the quantum satellite. Consequently, we could conduct at most one experiment per day. Additionally, LEO satellites fly at extremely high speeds, resulting in a time window of only approximately 10 min when passing a single ground station. The ground station must maintain high stability during satellite tracking to ensure continuity of communication. Since only one quantum satellite was used in this experiment, it can dock with only one ground station in the same region within a single orbit. To address the aforementioned two limitations, viable solutions include establishing a quantum satellite constellation or deploying Medium Earth Orbit (MEO)/GEO quantum satellites.

2. Analysis of the Application Scheme of Satellite-Based QKD in 5G-Enabled NTN

In this section, we first analyze the situation and architecture of satellite-based QKD and 5G-enabled NTN. Secondly, we propose a satellite-based QKD encryption solution for 5G-enabled NTN. Finally, we theoretically analyze the impact on the 5G-enabled NTN after adding quantum encryption.

2.1. State of the Art in Satellite-Based QKD Communications: Architecture and Developments

2.1.1. Developments of Satellite-Based QKD

The global development of satellite-based quantum communication has achieved significant milestones since 2016. In August 2016, China successfully deployed the world's first quantum science satellite, "Micius", establishing a pioneering satellite-to-ground quantum secure communication system that accomplished the first intercontinental QKD demonstration [2,3,9,10]. This was followed by the September 2016 launch of the "Tiangong-2" space laboratory carrying quantum communication payloads, which advanced satellite-ground QKD experiments [11]. A subsequent breakthrough occurred in July 2022 with the "Jinan-1" microsatellite, achieving real-time QKD operations and marking a crucial step toward practical implementation [12]. According to the report, Canada has outlined the Quantum EncrYption and Science Satellite (QEYSSat) mission expected to be launched in 2026 and its anticipated outcomes [13]. QEYSSat is a technology demonstration platform aimed at studying the ground-to-space quantum uplink channel using satellite-based quantum receivers, including photon polarization analyzers and single-photon detectors [14]. Germany has launched "QUBE" and "QUICK 3" quantum satellites in 2024 [15,16]. It is planned to launch the "QUBE-II" quantum satellite in 2025, equipped with dual-wavelength Discrete Variable (DV) QKD transmission modules at 850 nm and 1550 nm, Quantum Random Number Generators (QRNG), and high-precision laser communication terminals [17]. The EU plans to launch the "Eagle-1" quantum satellite between the end of 2025 and 2026,

integrating QKD payloads to verify and demonstrate the European cross-border quantum secure communication network [18]. At the same time, the EU plans to launch the "IRIS2" quantum satellite in 2027, which will adopt a multi-orbit QKD architecture combining LEO and MEO, integrating 5G standards and government-level encryption technology [19]. In addition, the EU also plans to launch the "SAGA 1G" quantum satellite, using the Prepare-and-Measure (PM) Discrete Variable QKD protocol, through the C-band quantum signal downlink [20].

2.1.2. Architecture of Satellite-Based QKD

A QKD system typically consists of a quantum transmitter and a quantum receiver, which are connected through a quantum channel and a classical channel. QKD systems typically use the BB84 protocol to implement QKD. The system generates random numbers and randomly selects either the "+" basis (horizontal and vertical polarization) or the "$\times$" basis (45° and $-45°$ polarization) based on the bits. The quantum signal modulation module modulates the quantum signal into the corresponding quantum state, which is transmitted to the QKD receiver through a quantum channel. The QKD receiver's quantum signal demodulation module randomly selects either the "+" basis or the "$\times$" basis for each quantum bit, demodulates and measures the quantum signal, and after obtaining the measurement result, both parties compare the basis vectors through a classical channel to negotiate and form the final quantum key [2,21,22].

Currently, there are two common implementations of QKD: The first is QKD transmitted through fiber-optic networks, which can provide a relatively high secret key generation rate and strong system reliability. The second is QKD based on Free-Space Optical (FSO) has advantages in flexible infrastructure deployment [23,24]. Moreover, satellite-based QKD systems that rely on FSO can distribute secret keys to much farther locations.

Due to the signal attenuation problem of optical quantum transmission in optical fibers, in formally applied QKD networks, the transmission distance between two QKD nodes is usually controlled within 100 km. In order to achieve long-distance transmission of quantum keys, multiple trusted relay nodes need to be set up on the transmission path between the starting node and the target node [21]. A QKD sending device and a QKD receiving device need to be deployed at each node along the entire transmission path. A point-to-point QKD link is established between each group of adjacent nodes to generate a relay quantum key. Based on this key, a "one-time password" method is used to relay the key to the next node [21].

One important role of quantum satellites is to serve as relay nodes to expand the scope of QKD, distributing quantum keys to two nodes that do not have ground-based QKD connection capabilities. A free-space quantum channel is constructed between quantum satellites and ground stations through laser communication technology for satellite-ground QKD [2,22,25].

Deployment of Quantum Ground Stations (QGS) at communication sites lacking ground-based QKD networks is used to dock with quantum satellites and receive optical quantum signals. The BB84 protocol is used between the quantum satellites and ground stations to distribute quantum keys to the quantum encryption and decryption devices of both communication parties [2,11,12,21].

FSO-based satellite-ground communication can operate independently of terrestrial networks, thereby enhancing the flexibility of network deployment. Satellite relay-based QKD networks enable the long-distance transmission of quantum keys, allowing quantum keys to be delivered to any remote areas.

2.2. Analysis of 5G-Enabled NTN Architecture

As a core implementation of 5G-enabled NTN, 5G satellite communications primarily operate through three fundamental architectural paradigms: (1) satellite-based relaying, (2) transparent payload forwarding, and (3) regenerative on-board processing.

2.2.1. Architecture of Satellite-Based Relaying Network

The satellite-based relaying architecture represents a conventional implementation in 5G-enabled NTN systems, where satellites function as transparent backhaul carriers between the next-generation NodeB (gNB) and the core network (CN) of 5G or 6G. This topology maintains minimal on-board signal processing, limiting satellites to basic frequency conversion and signal amplification functions.

As illustrated in Figure 1, the satellite-based relaying architecture demonstrates protocol-transparent coupling with 5G terrestrial networks and enables flexible topology reconfiguration by utilizing established satellite communication infrastructure. However, this implementation mandates the co-located deployment of gNBs and satellite ground stations (e.g., VSAT terminals) at user-side premises.

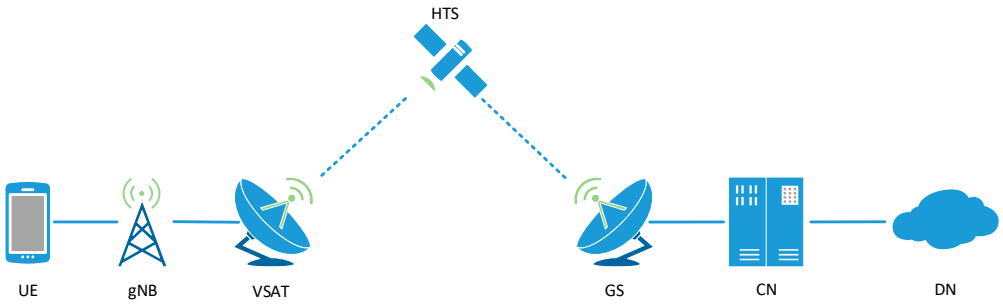

Figure 1. Architecture of a satellite-based relaying network. UE (User Equipment), VSAT (Very Small Aperture Terminal), GS (Gateway Station), and DN (Data Network).

The architecture of a satellite-based relaying network applies to areas with no terrestrial networks at all and where users are relatively concentrated in clusters [26].

2.2.2. Architecture of Satellite-Based Transparent Forwarding Network

Transparent forwarding mode, as standardized in 3GPP Release 17, constitutes a foundational 5G-enabled NTN architecture where satellites and gateway stations operate as Radio Frequency (RF) repeaters. This implementation enables signal propagation to remote regions (e.g., maritime and arid zones) through regenerative RF chain processing. UE achieves direct satellite access via transparent payloads while maintaining terrestrial-grade QoS (Quality of Service) through gateway-anchored gNBs [5,27].

As shown in Figure 2, in the satellite-based transparent forwarding network, the satellite and GS function as signal extensions of the gNB, necessitating support for the NR-Uu (The NR-Uu interface connects the UE to the gNB) radio interface and employing transparent signal relaying techniques that maintain protocol stack integrity without on-board baseband processing. Concurrently, the satellite payload must additionally support RF signal transmission to accommodate NTN requirements [5,26,27].

The architecture of a satellite-based transparent forwarding network is suitable for mobile terminals without fixed operating locations, enabling terminals supporting satellite communication to access the satellite without the need to deploy dedicated devices such as VSAT.

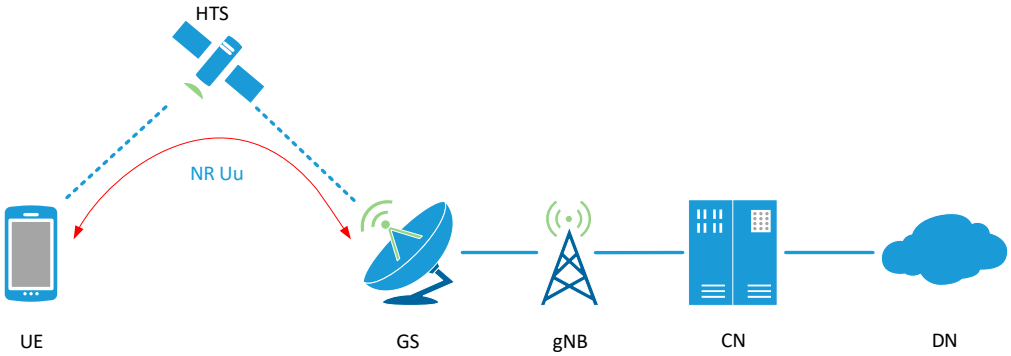

Figure 2. Architecture of a satellite-based transparent forwarding network. In this mode, HTS functions solely as a relay for RF signals and cooperates with GS to transmit gNB signals to more distant locations.

2.2.3. Architecture of Regenerative Satellite-Based Network

A regenerative satellite-based network is an NTN networking mode proposed by 3GPP in R18, shown in Figure 3. In this mode, the main feature of the gNB will be transferred to the satellite, also known as the base station in satellite mode. The satellite still provides the NR-Uu radio interface to ground terminals, and user terminals can directly access the satellite. Unlike the transparent forwarding mode, the on-board regeneration mode layers the base station protocol with the underlying link between the satellite and the GS using Satellite Radio Interface (SRI), and the upper layer protocol is directly transmitted transparently by the GS [5,27].

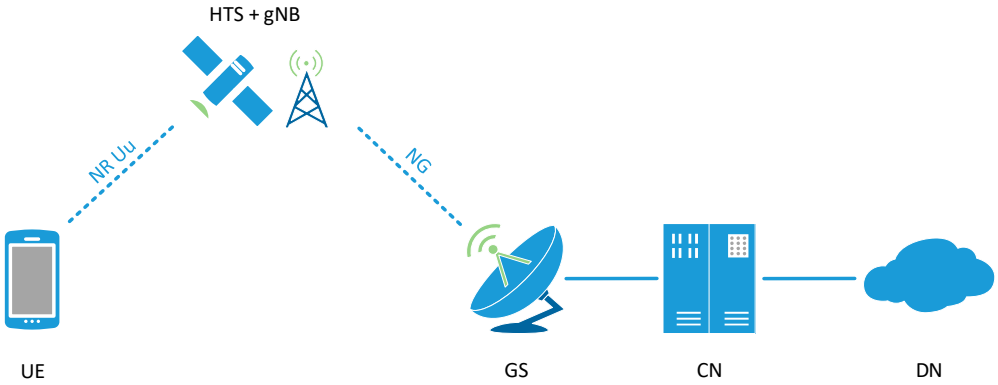

Figure 3. Architecture of a regenerative satellite-based network. In this mode, the gNB function is integrated into the satellite. Beyond transmitting RF signals, the satellite is fully equipped with the core capabilities of a gNB, including baseband signal processing and spectrum resource allocation.

In the regenerative satellite-based network, the satellite is deeply integrated with the gNB, and most of the functions of the gNB need to be integrated into the satellite for direct processing, reducing space–ground interaction, lowering time delay, and improving system reliability.

The application scenarios of the regenerative satellite network architecture are similar to those of the satellite-based transparent forwarding network architecture, and it is also applicable to mobile terminals without fixed operating locations. The biggest difference between the two lies in the different deployment locations of base stations. For the regenerative satellite network architecture, because the distance between base stations and users is shorter, the system processing efficiency is higher.

3. Analysis of Security Frameworks for Converged Applications

Satellite communication has gradually matured, especially with the rapid development of high-throughput satellites. High-throughput satellites provide greater throughput than conventional communication satellites, and satellite Internet demonstrates strong application potential. User terminals can communicate with satellites through ground stations, while some satellite phones support direct satellite connectivity.

For scenarios involving densely concentrated user populations in specific areas, we propose deploying gNBs on the user-side. This approach enables signal coverage via user-side gNB deployment, allowing standard UE to access the network without satellite communication capabilities. The solution effectively addresses diverse connectivity demands while maintaining terminal cost-effectiveness.

Quantum satellites enable secure Quantum Key Distribution between communication parties. The QGS integrates multiple subsystems, including optical receivers, precision turntables, quantum optical processors, and key generation modules. Through the efforts of the industry, the weight of QGS has been successfully reduced from 13 tons to less than 100 kg through miniaturization [12]. Following quantum satellite docking, the QGS stores generated keys in a tamper-resistant local Key Management System (KMS), with on-demand retrieval by application systems. To ensure key security, we propose collocating QGSs with application systems within a shared secure domain, utilizing wired network connections for encapsulated key transmission.

Considering the usage characteristics of the terminal and the networking architecture of the mobile network, the quantum key equipment is recommended to be deployed at the exit of the gNB and the entrance of the CN. Therefore, in the satellite communication network, we suggest applying QKD technology to the satellite communication system in satellite relay mode.

3.1. Converged Architecture

The quantum-encrypted satellite communication scheme involves deploying additional QGS and Encryption Gateways on both the user side and the net side of the satellite-based relaying network to establish a secure, encrypted communication network.

As shown in Figure 4a, the user side consists of UE, gNB, VSAT, QGS, and Encryption Gateway, while the network-side comprises CN, QGS, and Encryption Gateway, which interfaces with the high-throughput satellite GS. The CN further connects to the DN.

The high-throughput satellite network, composed of high-throughput satellites, ground stations (GSs, and the core network, provides satellite-based broadband communication capabilities to users. It serves as a backhaul network to enable data transmission between gNBs and the CN in satellite communication systems, delivering the signal coverage to terrestrial network-inaccessible areas and meeting conventional users' communication requirements.

The ground station interfaces with the high-throughput satellite, responsible for transmitting uplink data from gNBs to the high-throughput satellite and simultaneously receiving downlink data from the high-throughput satellite for forwarding to gNBs. The GS connects to the high-throughput satellite, receives gNB data relayed by the high-throughput satellite, and transmits the data to CN via a dedicated network line.

The satellite-based QKD network, composed of quantum satellites, QGS, and Quantum Satellite Operation and Control Centers (QSOCC), enables intercontinental QKD through FSO-QKD technology. This network provides quantum keys for Encryption Gateways on both the gNB and CN sides, ensuring the security of gNB backhaul links.

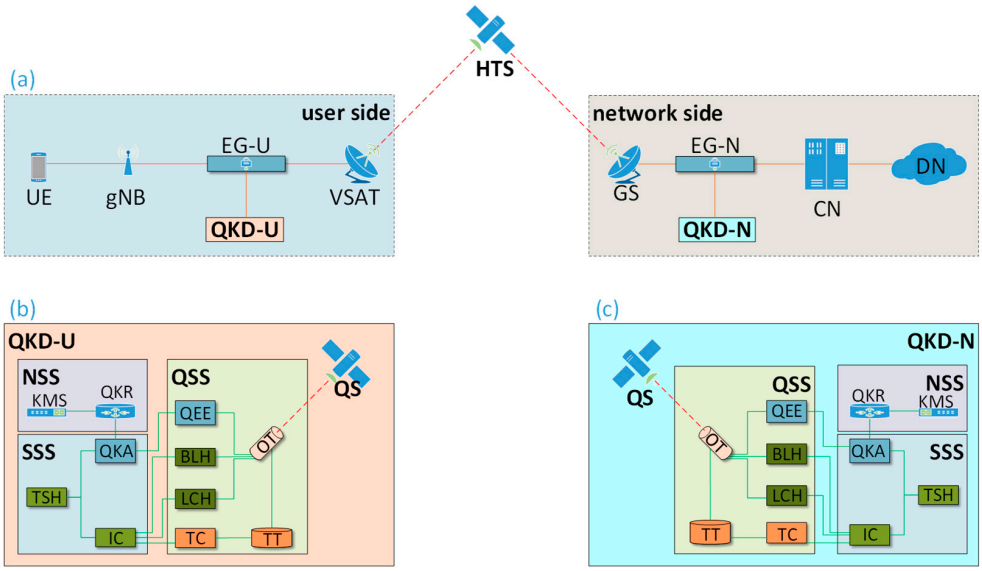

Figure 4. Experimental setup of quantum-encrypted satellite communication network. (**a**) System architecture. (**b**,**c**) are the schematics of QKD-U (QKD on Uer side) and QKD-N (QKD in the Network-side). (**b**) During the first orbit, QKD is performed between the QS (Quantum Satellite) and the user-side ground station. (**c**) During the second orbit, QKD is performed between the QS and the network-side ground station. EG-U (Encryption Gateway in user side), GS, EG-N (Encryption Gateway in network side), CN, OT (Optical Terminal), TT (Tracking Turntable), TC (Tracking Controller), BLH (Beacon Light Host), LCH (Laser Communication Host), QEE (QKD Electronic Equipment), TSH (Task Scheduling Host), QKA (Quantum Key Adapter), IC (Integrated Controller), QKR (Quantum Key Router). QSS (Quantum SubSystem), SSS (Service SubSystem), NSS (Network SubSystem).

As shown in Figure 4b,c, the QKD-U and QKD-N systems implement identical QKD protocols and function as ground-based quantum signal receivers for single-photon signals transmitted from quantum satellites. The fundamental distinction resides in their network deployment: QKD-U is typically co-located with end-user devices, whereas QKD-N functions as an intermediate node within the network infrastructure.

The QGS interfaces with the quantum satellite to implement QKD. Generated quantum keys are securely stored in the QGS's KMS and are then delivered to the Encryption Gateways on the gNB and CN sides via standardized interfaces. These Encryption Gateways utilize these keys to encrypt transmission links between gNBs and the CN.

During system operation, the satellite-based QKD and satellite communication systems operate asynchronously. The Encryption Gateway consumes quantum keys when encrypting satellite communication links. To maintain sufficient available quantum keys between ground stations, the quantum satellite and QGS trigger QKD sessions periodically or on demand based on real-time key consumption rates.

The QKD process is dynamically scheduled to ensure continuous key replenishment between QGSs, thereby guaranteeing sustained encryption capability for the Encryption Gateway-secured backhaul links between gNBs and the CN.

The proposed integrated architecture obtains quantum keys by deploying Quantum Ground Stations on both the user-side and the core-network-side of the NTN. Meanwhile, it deploys quantum encryption and decryption gateways to perform quantum encryption for NTN links, thus constructing an NTN security architecture based on quantum encryption.

3.2. Principle of Satellite-Based QKD

A satellite-based QKD system requires at least one QS and two QGSs. The QS enables QKD and relay between the two QGS units, which are deployed on the infor-

mation transmission and reception sides, respectively, to provide quantum keys for the information systems.

During scheduled overflight windows, the QS passes over the QGS units, which then acquire and maintain continuous tracking of the satellite. Within a single orbital period, the QS continuously transmits single-photon signals to the ground stations. The QKD process between the QS and each QGS is implemented using the BB84 protocol, establishing a shared key K at both ends.

As illustrated in Figure 5, when long-distance Quantum Key Distribution is required between QGS 1 and QGS 2, satellite-ground docking missions are initiated through the quantum satellite operation and control center. The missions are dispatched to the quantum satellite, QGS 1, and QGS 2, respectively. During the docking with QGS 1, the quantum satellite establishes a QKD link based on the BB84 protocol, generating a shared key K_1 stored in both entities. Similarly, during the docking with QGS 2, another shared key K_2 is produced through the BB84 protocol and stored in the quantum satellite and QGS 2.

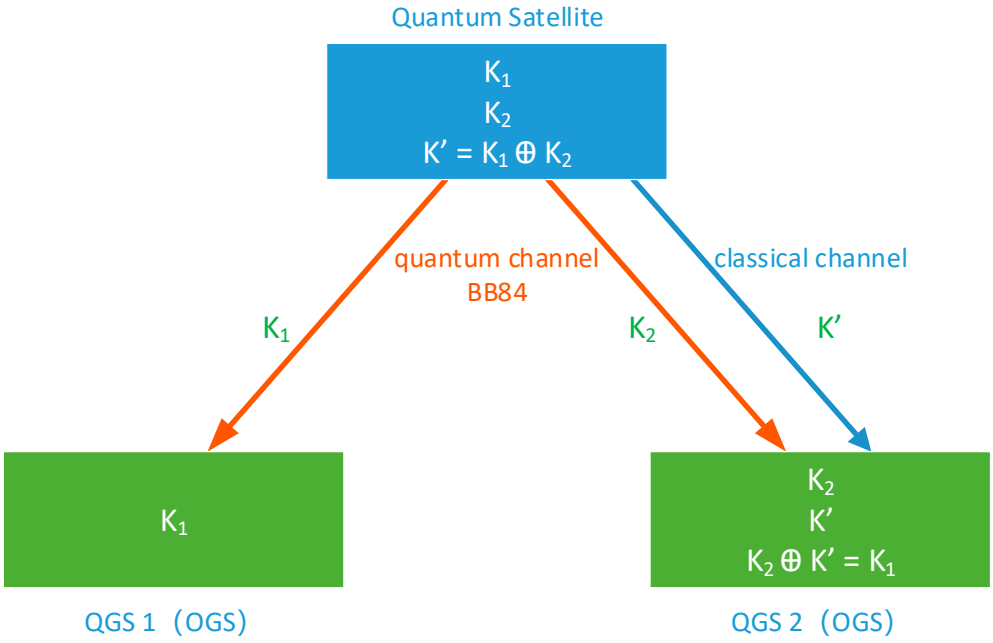

Figure 5. Principle of the satellite-to-ground QKD. QGS is an Optical Ground Station (OGS). A quantum channel is established between the quantum satellite and the ground station for key distribution, and the keys from QGS 1 are relayed to QGS 2 via a classical channel.

Upon completing the QKD process with QGS 2, the quantum satellite encrypts K_1 with K_2 to obtain K', which is transmitted to QGS 2. QGS 2 then decrypts K' using K_2 to recover K_1, enabling secure key sharing between the two ground stations. This process ensures that K_1 is securely distributed without direct transmission between QGS 1 and QGS 2.

The shared key K_1 can now be utilized by both ground stations for end-to-end encryption of transmitted data. QGS 1 and QGS 2 provide K_1 to their local application systems, respectively, enabling secure communication between the two locations. This method leverages the quantum satellite as a trusted intermediary for key distribution [3,21].

The use of the BB84 protocol ensures the security of the key generation process, as any attempt to intercept the quantum signals would introduce detectable disturbances. The encryption of K_1 with K_2 further enhances security during the key sharing phase, ensuring that K_1 remains confidential until it reaches QGS 2.

The core function of satellite-based QKD lies in key relay. A quantum satellite establishes shared quantum keys with each ground station via separate quantum secure

channels. When a specific ground station requests to share keys with another ground station, the quantum satellite encrypts the key of the target ground station using the shared quantum key between itself and the requesting ground station, and then distributes the encrypted key. The OTP encryption method, which offers the highest security, is adopted in this process.

3.3. Quantum-Encrypted NTN Workflow

The quantum-encrypted NTN comprises a foundational infrastructure of high-throughput satellites, ground stations, and GSs.

In an encrypted transmission channel, the user-side Encryption Gateway and network-side Encryption Gateway establish an end-to-end encrypted tunnel over the satellite network. This tunnel serves as the underlying secure transport layer, connecting gNBs to the CN to form the encrypted NTN system.

Figure 4 details the communication workflow. In uplink data transmission, the UE sends data to the gNB. The gNB forwards the data to the EG-U, which encrypts it using quantum keys. The encrypted data is then transmitted via the satellite network to the EG-N. The EG-N decrypts the data using quantum keys and forwards it to the CN, which delivers it to the data network. In downlink data transmission, the reverse path is followed for downlink data (DN → CN → EG-N → HTS → EG-U → gNB → UE). The EG-N encrypts downlink data, while the EG-U decrypts it [28].

3.4. Performance Evaluation

In satellite communication networks, communication delay stands as the most significant factor affecting overall system availability. The variation in satellite altitude directly impacts communication delay, with higher altitudes resulting in greater delays. Based on orbital altitude, satellites are typically categorized into three classifications: GEO, MEO, and LEO. Specifically, GEO satellites operate at an altitude of 36,000 km, MEO satellites function within the altitude range of 5000–20,000 km, while LEO satellites maintain orbital heights between 500 and 1200 km.

As shown in Figure 6, the propagation delay Δ_t for signals transmitted from a satellite to a ground station can be calculated based on the signal propagation distance and the speed of light. Mathematically, it is expressed as [29,30]:

$$\Delta_t = \frac{1}{c} \cdot \sqrt{R^2 + r^2 - 2R \cdot r \cdot \left[\sin\phi_s \cdot \sin\phi_{gs} + \cos\phi_s \cdot \cos\phi_{gs} \cdot \cos\left(\lambda_s - \lambda_{gs}\right)\right]} \quad (1)$$

where R denotes the Earth's equatorial radius (the distance from the Earth's surface at the equator to its center), r represents the satellite's orbital radius (the distance from the satellite to the Earth's center), ϕ_s and λ_s indicate the satellite's latitude and longitude in the geocentric coordinate system, respectively, while ϕ_{gs} and λ_{gs} correspond to the latitude and longitude of the ground station.

As depicted in Figure 7, the RTT (T) of satellite communication services comprises not only the propagation delay between the Shanghai VSAT and the Chengdu GS, but also the access latency from the UE to the VSAT, and the core network transmission delay from the GS to the DN [29,30].

$$\begin{aligned} T = {} & d_{UE-gNB} + d_{gNB-VSAT} + d_{VSAT-HTS} + d_{HTS-GS} + d_{GS-CN} + d_{CN-DN} + d_{DN-CN} \\ & + d_{CN-GS} + d_{GS-HTS} + d_{HTS-VSAT} + d_{VSAT-gNB} + d_{gNB-UE} \end{aligned} \quad (2)$$

Satellite communication networks exhibit multiple intermediate nodes and are susceptible to weather-induced impairments in space-to-ground links. To ensure statistical

validity of the time delay, we conducted n times (n = 100) delay measurement trials and calculated the mean delay using the following equation:

$$\mu = \frac{\sum_{i=1}^{n} T_i}{n} \tag{3}$$

where T_i denotes the RTT of the i-th communication and μ denotes the mean time delay.

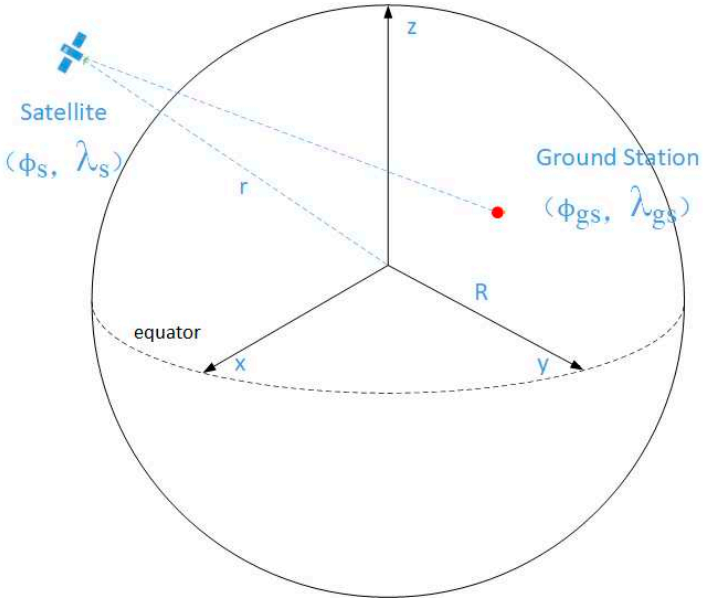

Figure 6. Correlation factors of the time delay between satellite and ground station.

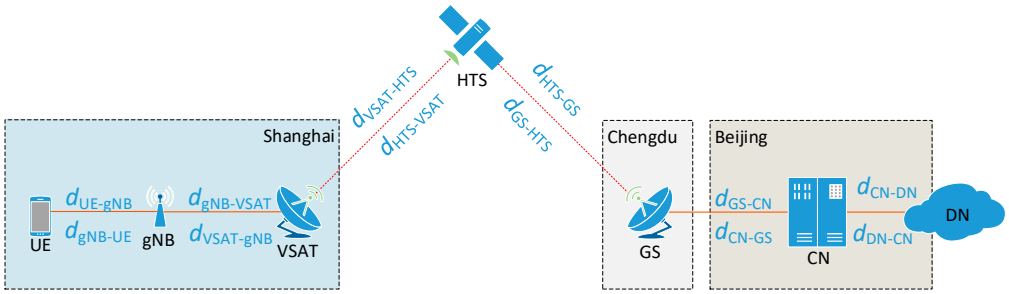

Figure 7. Composition of communication delay of quantum encryption satellite communication, $d_{\text{UE-gNB}}$ and $d_{\text{gNB-UE}}$ denote the delay between UE and gNB, $d_{\text{gNB-VSAT}}$ and $d_{\text{VSAT-gNB}}$ denote the delay between gNB and VSAT, $d_{\text{VSAT-HTS}}$ and $d_{\text{HTS-VSAT}}$ denote the delay between VSAT and HTS, $d_{\text{HTS-GS}}$ and $d_{\text{GS-HTS}}$ denote the delay between HTS and GS, $d_{\text{GS-CN}}$ and $d_{\text{CN-GS}}$ denote the delay between GS and CN, $d_{\text{CN-DN}}$ and $d_{\text{DN-CN}}$ denote the delay between CN and DN.

In assessing network availability between nodes, in addition to average RTT, network jitter serves as a critical stability metric. This parameter σ quantifies temporal delay variation and is calculated as follows:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (T_i - \mu)^2}{n}} \tag{4}$$

where T_i represents the i-th time delay measurement.

To quantify network stability with higher precision, we propose analyzing the temporal dynamics of network jitter through standardized measurement intervals using the following equation:

$$J_i = |T_i - T_{i-1}| \tag{5}$$

4. Experimental Setup and Results

To validate the feasibility of integrating satellite-based QKD into 5G satellite communication systems, we constructed a satellite-relayed encrypted 5G network using the following components:

- QS: "Jinan-1";
- HTS: "Chinasat-26";
- QGS: CASQN SIWS-1000;
- VSAT: KeyCSat PB60A-S4;
- GS: CSC Chengdu GS;
- 5GC: GENEW 5GC;
- IPSec VPN: CASQN CSL-VPN-1000;
- gNB: CTIBS5421 5G small cell;
- UE: HUAWEI Mate 30 Pro 5G.

Subsequently, we conducted satellite-based QKD experiments to provide quantum keys for IPSec VPNs located in Beijing and Shanghai. Based on these keys, we further implemented a quantum-encrypted 5G satellite communication test.

In Shanghai and Beijing, shown in Figure 8, QGS were deployed and connected to the quantum satellite to establish a satellite-to-ground QKD network. In Shanghai, a VSAT and 5G small cell were installed to provide 5G signal coverage for scenarios lacking terrestrial network infrastructure (e.g., maritime vessels, deserts, and remote areas). In Beijing, a 5GC was implemented and interfaced via dedicated fiber-optic lines with the GS in Chengdu, which connects to the HTS.

Figure 9 presents a satellite-based QKD-encrypted 5G-enabled NTN between Shanghai and Beijing nodes.

As depicted in Figure 10, the experimental campaign achieved critical milestones in satellite-based QKD: On 22 November 2024 (22:40:01–22:47:29 UTC+08:00), the QGS in Beijing successfully established a quantum optical link with the "Jinan-1" and performed QKD, generating quantum-secured keys. On 29 November 2024, these keys were relayed to the QGS in Shanghai via the "Jinan-1". These keys, managed by the integrated KMS of the QGS's QKD system, are utilized to secure satellite communications. When encrypted 5G satellite communication is required, the VPN gateways can request and obtain these QKD-derived keys from the QGS's KMS to negotiate strong session keys for protecting the IPSec VPN tunnels.

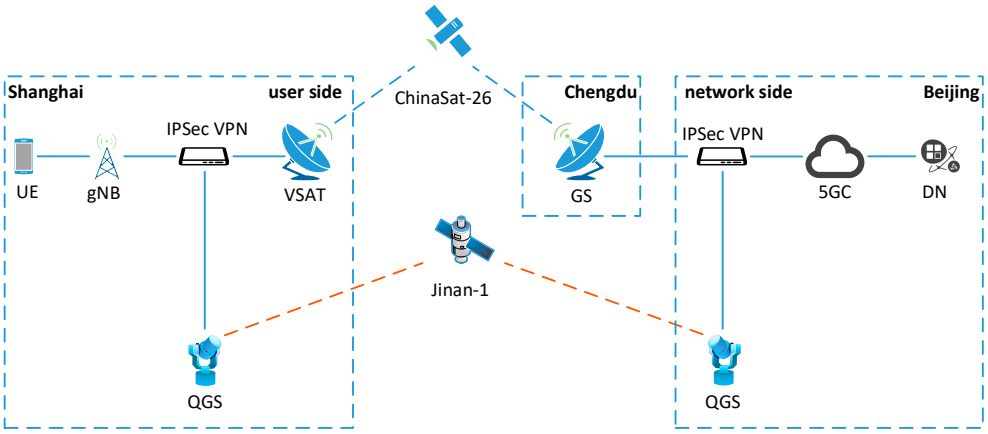

Figure 8. Architecture of quantum-encrypted 5G satellite communication network.

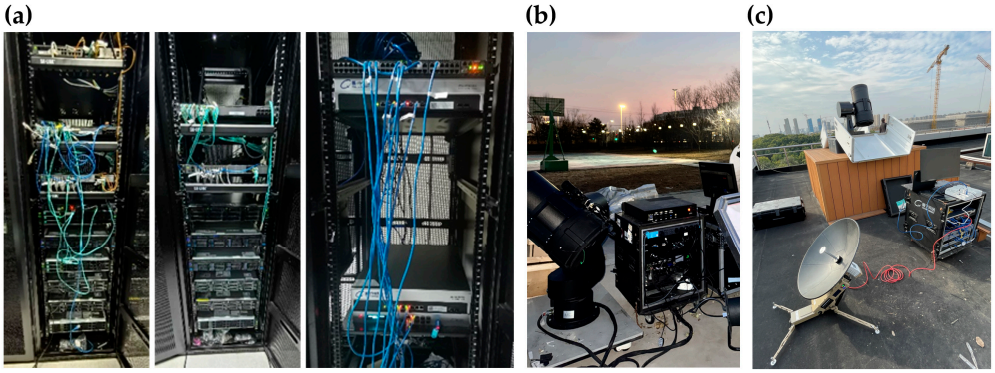

Figure 9. Experimental installation. (**a**) GENEW 5GC and CASQN CSL-VPN-1000 IPSec VPN (Beijing indoor). (**b**) CASQN SIWS-1000 QGS (Beijing outdoor). (**c**) KeyCSat PB60A-S4 VSAT and CASQN SIWS-1000 QGS and CASQN CSL-VPN-1000 and CTIBS 5421 gNB (Shanghai outdoor).

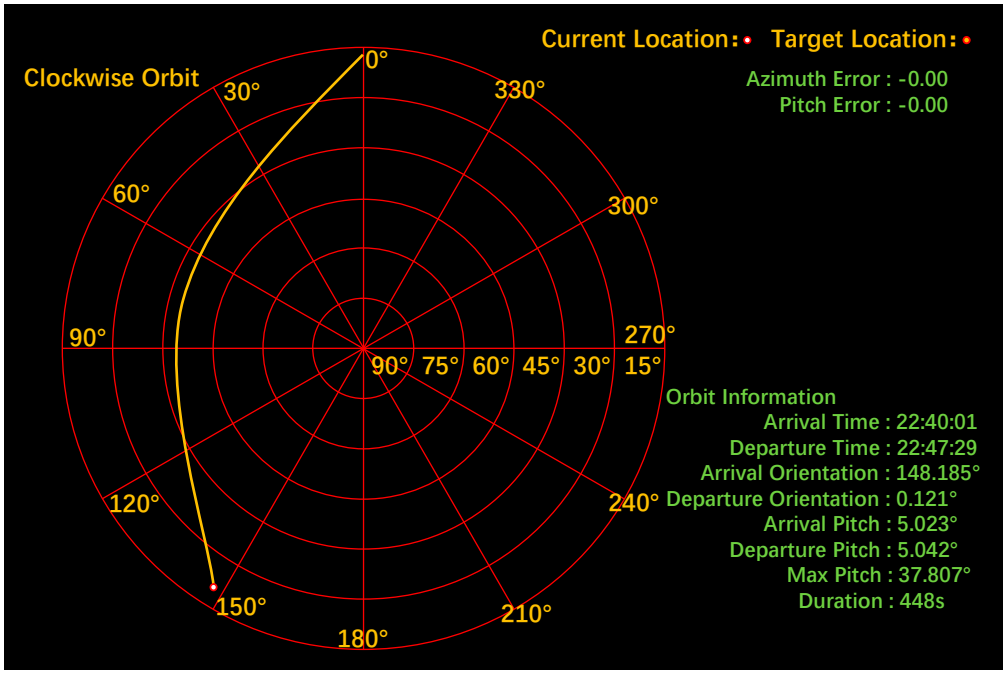

Figure 10. The monitoring image from the integrated control software of QGS depicts the operational trajectory of the "Jinan-1" Quantum Satellite during this space—ground docking process.

When encrypted data transmission is required in 5G satellite networks, the IPSec VPN dynamically acquires fresh quantum keys from the local KMS, implementing end-to-end quantum-secured communication via 128-bit SM4 or AES encryption algorithms.

In this experiment, shown in Figure 11, the "ChinaSat-26" satellite is positioned directly above the equator (i.e., $\phi_s = 0^\circ$), which simplifies the trigonometric terms to $\sin \phi_s = \sin 0^\circ = 0$ and $\cos \phi_s = \cos 0^\circ = 1$. Consequently, the propagation delay Equation (1) reduces to

$$\Delta_t = \frac{1}{c} \cdot \sqrt{R^2 + r^2 - 2R \cdot r \cdot \cos \phi_{gs} \cdot \cos(\lambda_s - \lambda_{gs})} \quad (6)$$

The parameters are substituted as follows:

- Speed of light c = 299,792.458 km/s;
- Earth's equatorial radius R = 6378 km;
- Satellite orbital radius r = 42,164 km;
- Longitude difference = $\lambda s - \lambda gs = 125^\circ - 121^\circ 30' = 3^\circ 30'$.

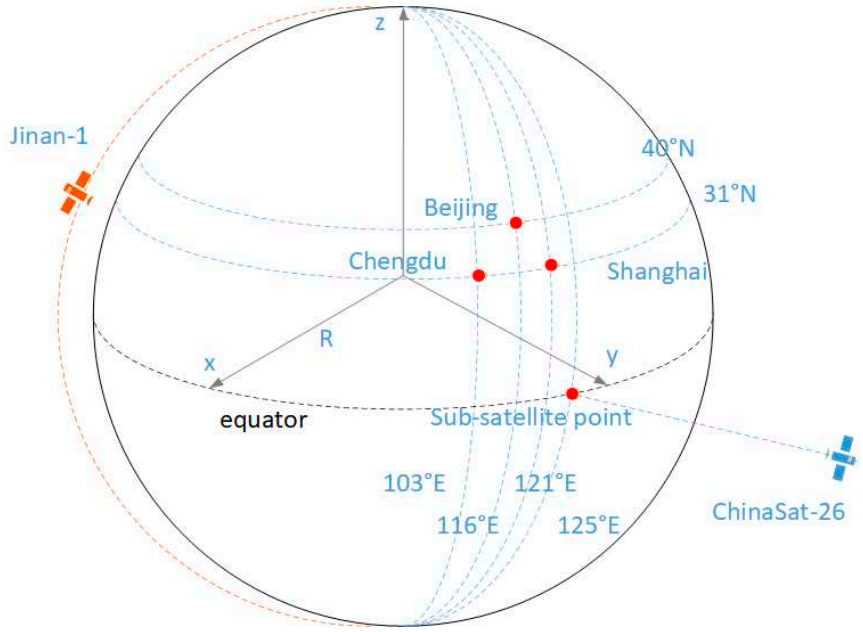

Figure 11. The geographic positions of the satellites and ground stations. The coordinates of the experimental sites are as follows: Shanghai: 31°6′ N, 121°30′ E, Beijing: 40°6′ N, 116°30′ E, Chengdu GS: 31° N, 103°36′ E. The "ChinaSat-26" satellite, a GEO satellite, is positioned at 125°E longitude over the equator. Its sub-satellite point is located at 0° N, 125° E, with an orbital altitude of 42,164 km. The "Jinan-1" quantum satellite, classified as a LEO satellite, operates in a Sun-synchronous orbit (SSO) with no fixed geographic position.

The theoretical propagation delay from the satellite to the Shanghai ground station is calculated as $\Delta_{ts} = 123$ ms, and to the Chengdu GS as $\Delta_{tc} = 124$ ms. Therefore, the total theoretical propagation delay between the Shanghai ground station and the Chengdu GS approximates 247 ms.

The leased line transmission delay from the Chengdu GS to the Beijing 5GC is approximately 20 ms. The total delay from the Shanghai VSAT to the Beijing DN is 267 ms, yielding a RTT of 534 ms.

We first conducted RTT tests on the high-throughput satellite link between the Shanghai VSAT and the Beijing 5GC entry point. As shown in Figure 12a, the measured RTT consistently remained below 600 ms, with a minimum RTT of 562 ms, a maximum RTT of 586 ms, and an average RTT of 576 ms. Compared to the theoretical RTT of 534 ms, the measured results exhibited an average increase of approximately 42 ms, indicating limited overall RTT variation.

To evaluate the impact of quantum encryption implementation on 5G satellite communication services, we conducted RTT tests using a real UE in a non-IPSec VPN environment. As depicted in Figure 12b, the measured RTT ranged from 600 ms to 765 ms with an average value of 660 ms.

Subsequently, we deployed IPSec VPN within the experimental environment. As illustrated in Figure 13, the network architecture was augmented with a pair of IPSec VPN tunnels, and bidirectional delay measurements were systematically conducted.

As shown in Figure 12c, in quantum-encrypted 5G satellite communication scenarios, the RTT between UE and DN remains predominantly below 700 ms, with a minimum RTT of 617 ms, a maximum RTT of 713 ms, and an average RTT of 665 ms. The comparative analysis of RTT can refer to Figure 12d.

Detailed jitter dynamics are illustrated in Figure 14. Experimental results demonstrate that the high-throughput satellite link exhibits minimal network jitter, with an average value of 6 ms. In contrast, the non-encrypted 5G satellite communication network shows

significantly higher jitter, averaging 38 ms. Following the implementation of quantum IPSec VPN, the 5G satellite communication network achieves a substantial 50% reduction in jitter, lowering the average to 19 ms. This provides evidence that quantum IPSec VPN markedly enhances network stability.

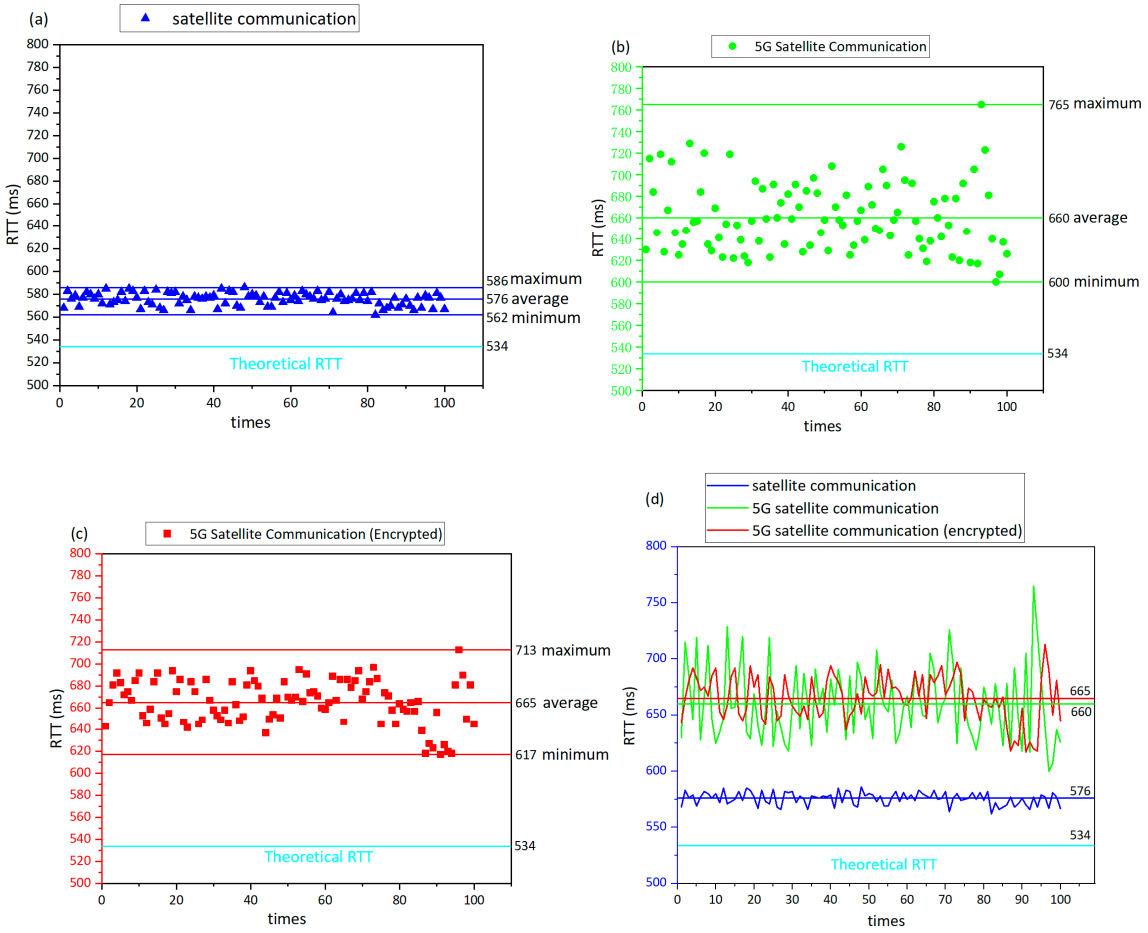

Figure 12. (**a**) RTT of satellite communication (between VSAT and GS). (**b**) RTT of 5G satellite communication (between UE and DN). (**c**) RTT of encrypted 5G satellite communication (between UE and DN). (**d**) Line chart of RTT and comparison chart of average RTT for satellite communication, 5G satellite communication, and 5G satellite communication (encrypted).

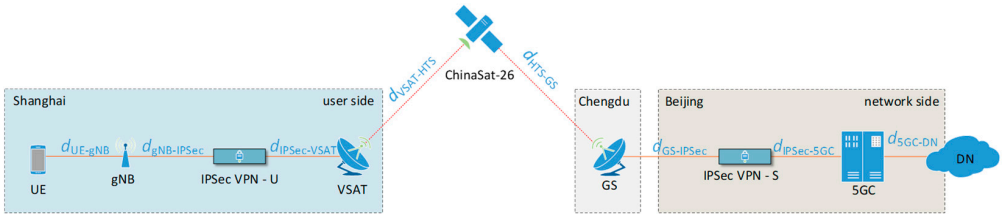

Figure 13. The delay components of quantum-encrypted 5G satellite communications, defined as follows: $d_{\text{UE-gNB}}$—time delay between 5G UE and gNB; $d_{\text{gNB-IPSec}}$—time delay between gNB and user-side IPSec VPN; $d_{\text{IPSec-VSAT}}$—time delay between user-side IPSec VPN and VSAT; $d_{\text{VSAT-HTS}}$—time delay between VSAT and HTS; $d_{\text{HTS-GS}}$—time delay between HTS and GS; $d_{\text{GS-IPSec}}$—time delay between GS and network-side IPSec VPN; $d_{\text{IPSec-5GC}}$—time delay between IPSec VPN and 5GC; $d_{\text{5GC-DN}}$—time delay between 5GC and DN.

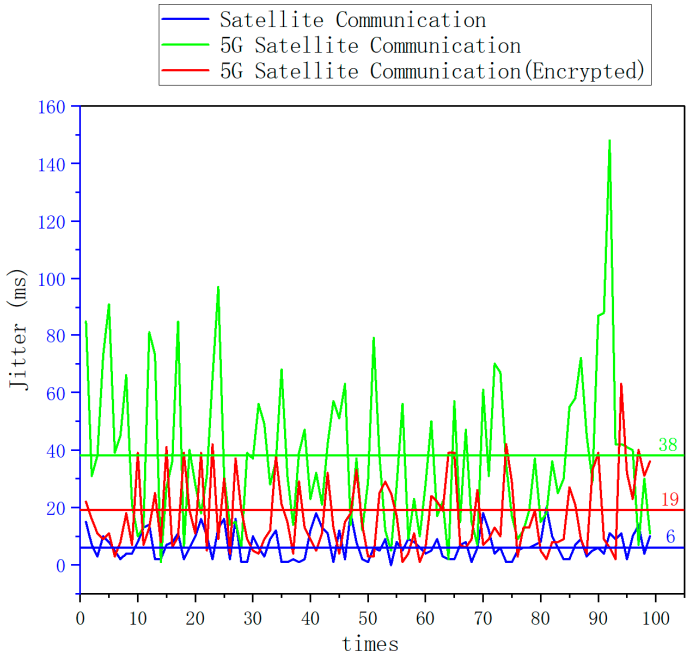

Figure 14. Line chart and average values of jitter test data under three scenarios.

Furthermore, we conducted comprehensive testing of quantum-encrypted 5G services, including Voice over New Radio (VoNR), messaging, and data communications. All services operated seamlessly, with VoNR—the most delay-sensitive application—delivering excellent audio quality. Under the Mean Opinion Score (MOS) evaluation framework, all testers rated the voice quality above 4.0 (categorized as "good" to "excellent").

5. Discussion

This paper systematically examines the feasibility of 5G-enabled NTN and satellite-based QKD technology, proposing an integrated application framework for spaceborne QKD in 5G satellite systems. In terms of results, this study not only experimentally validates the technical feasibility of integrating of 5G-enabled NTN with satellite-based QKD in 5G networks, but also achieves enhanced communication, as well as providing RTT and jitter metrics to assess end-user experience performance. These findings may inspire the research community to further explore security while expanding solutions for next-generation NTN based on satellite-based QKD encryption, as well as their potential applications.

The security framework presented in this work exhibits both strengths and limitations. First, 5G-enabled NTNs operating in satellite relay mode deliver reliable 5G signal coverage to remote areas, eliminating the need for wired connections between gNB and 5GC. Second, satellite-based QKD provides a quantum satellite application scenario communication infrastructure for remote regions, enabling Quantum Key Distribution via satellites and obviating concerns about the high construction costs of terrestrial QKD networks. Third, backhaul link encryption based on quantum cryptography offers users high-security transmission guarantees and mitigates the risk of information leakage. However, the framework involves a large number of devices, leading to considerable overall costs. Beyond 5GC, QGS, and IPSec VPN on the network side, it requires the deployment of multiple independent devices (including VSAT, QGS, IPSec VPN, and gNB) on the user side. Future work could explore device integration efforts to reduce the system construction costs.

In this experiment, a 5G-enabled NTN was established using GEO satellites for communication. Due to the significantly large orbital altitude radius of GEO satellites, the system's signal propagation characteristics were degraded by environmental factors, result-

ing in elevated measured latency compared to theoretical predictions. Furthermore, the experimental configuration involved geographically separating the satellite gateways and the 5G core network by a distance of gateway and 5GC between two cities 2000 km across two distinct metropolitan areas. This intentional geographical dispersion introduced a substantial additional communication delay. Currently, low-latency satellite communication technology based on LEO is maturing; future research could be conducted on LEO communication satellite constellations to reduce RTT metrics and improve end-user experience.

In addition, only one quantum satellite was used in this experiment. The QGS in Beijing and Shanghai both needed to interface with "Jinan-1". Since these two cities are geographically close in longitude, "Jinan-1" could only interface with one of the QGS during a single satellite pass, while the other had to wait for the next satellite pass to establish the connection. Future efforts could focus on developing quantum satellite constellations to enhance satellite-ground QKD interfacing capability, thereby meeting the demands arising from the growth in user numbers.

6. Conclusions

This paper explores the integration architectures of 5G-enabled NTNs (in different modes) with satellite-based QKD and proposes a quantum-enhanced security framework for next-generation space–terrestrial networks. To this end, we developed a testbed and conducted experiments using real-world devices. These validations confirm the feasibility of the security framework, enhance the security of 5G-enabled NTN communications, and expand the application scenarios of quantum satellites.

To reduce latency in future commercial deployments, transitioning to LEO satellites represents a feasible strategy. Co-locating satellite gateways with 5G core network elements will further reduce the latency contribution caused by terrestrial network transmission. Establishing a dedicated quantum satellite constellation provides a viable approach to significantly enhancing the key delivery capabilities of satellite-based QKD. Subsequently, we intend to extend this architecture to quantum satellite constellations. Key issues that we need to focus on addressing in the next step include key management, such as inter-satellite key routing and transmission, task scheduling for simultaneous QKD sessions between multiple ground stations and the satellite constellation, as well as cooperation among multiple satellites.

Author Contributions: Conceptualization, C.H., and J.T.; Data curation, C.H. and Q.W.; Formal analysis, C.H. and J.L.; Funding acquisition, J.T. and J.W.; Investigation, C.H. and Y.X.; Methodology, C.H. and Y.Z.; Project administration, C.H. and J.W.; Resources, C.H. and F.Z.; Supervision, J.T. and S.L.; Validation, C.H. and Y.J.; Writing—original draft, C.H.; Writing—review and editing, C.H. and W.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Sci-Tech Innovation 2030 Agenda (2021ZD0301300).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used and/or analyzed during the current study are available from the author upon reasonable request. Due to privacy and ethical considerations, some data may be restricted.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

NTN	Non-Terrestrial Network
QKD	Quantum Key Distribution
5G	5th Generation mobile communication
QoE	Quality of Experience
RTT	Round-Trip Time
VPN	Virtual Private Network
HTS	High Throughput Satellite
ITU	International Telecommunication Union
3GPP	3rd Generation Partnership Project
CAGR	Compound Annual Growth Rate
CII	Critical Information Infrastructure
QEYSSat	Quantum EncrYption and Science Satellite
DV	Discrete Variable
QRNG	Quantum Random Number Generators
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
PM	Prepare-and-Measure
QGS	Quantum Ground Stations
gNB	Next-generation NodeB
CN	Core Network
6G	6th Generation Mobile Communication Technology
UE	User Equipment
VSAT	Very Small Aperture Terminal
GS	Gateway Station
DN	Data Network
RF	Radio Frequency
QoS	Quality of Service
SRI	Satellite Radio Interface
KMS	Key Management System
QKD-U	QKD in User side
QKD-N	QKD in Network side
QS	Quantum Satellite
EG-U	Encryption Gateway in User side
EG-N	Encryption Gateway in Network side
OT	Optical Terminal
TT	Tracking Turntable
TC	Tracking Controller
BLH	Beacon Light Host
LCH	Laser Communication Host
QEE	QKD Electronic Equipment
TSH	Task Scheduling Host
QKA	Quantum Key Adapter
IC	Integrated Controller
QKR	Quantum Key Router
QSS	Quantum SubSystem
SSS	Service SubSystem
NSS	Network SubSystem
QSOCC	Quantum Satellite Operation and Control Centers
FSO	Free-Space Optical
GEO	Geostationary Earth Orbit
SSO	Sun-synchronous orbit
VoNR	Voice over New Radio
MOS	Mean Opinion Score

References

1. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef] [PubMed]
2. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef] [PubMed]
3. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y.; et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* **2018**, *120*, 030501. [CrossRef] [PubMed]
4. 3GPP TR 38.811. Study on New Radio (NR) to Support Non-Terrestrial Networks. 2019. Available online: https://www.3gpp.org/ftp//Specs/archive/38_series/38.811 (accessed on 6 November 2025).
5. 3GPP TR 38.821. Solutions for NR to Support Non-Terrestrial Networks (NTN). 2020. Available online: https://www.3gpp.org/ftp/Specs/archive/38_series/38.821 (accessed on 6 November 2025).
6. ITU-R WP4B Contribution 39. Considerations on the Integration of Satellite-Based Solutions into 5G Networks. 2016. Available online: https://www.itu.int/md/R15-WP4B-C-0039 (accessed on 6 November 2025).
7. Grand View Research. Satellite Communication Market (2025–2030). 2025. Available online: https://www.grandviewresearch.com/industry-analysis/satellite-communication-market (accessed on 6 November 2025).
8. The New York Times. Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service. 2024. Available online: https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html (accessed on 6 November 2025).
9. Yin, J.; Cao, Y.; Li, Y.H.; Liao, S.K.; Zhang, L.; Ren, J.G.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Satellite-based entanglement distribution over 1200 km. *Science* **2017**, *356*, 1140–1144. [CrossRef] [PubMed]
10. Ren, J.G.; Xu, P.; Yong, H.L.; Zhang, L.; Liao, S.K.; Yin, J.; Liu, W.Y.; Cai, W.Q.; Yang, M.; Li, L.; et al. Ground-to-satellite quantum teleportation. *Nature* **2017**, *549*, 70–73. [CrossRef] [PubMed]
11. Li, Y.; Liao, S.K.; Cao, Y.; Ren, J.G.; Liu, W.Y.; Yin, J.; Shen, Q.; Qiang, J.; Zhang, L.; Yong, H.L.; et al. Space–ground QKD network based on a compact payload and medium-inclination orbit. *Optica* **2022**, *9*, 933. [CrossRef]
12. Li, Y.; Cai, W.Q.; Ren, J.G.; Wang, C.Z.; Yang, M.; Zhang, L.; Wu, H.Y.; Chang, L.; Wu, J.C.; Jin, B.; et al. Microsatellite-based real-time quantum key distribution. *Nature* **2025**, *640*, 47–54. [CrossRef] [PubMed]
13. Canadian Space Agency. Quantum Encryption and Science Satellite (QEYSSat). 2025. Available online: https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp (accessed on 23 November 2025).
14. Jennewein, T.; Simon, C.; Fougeres, A.; Babin, F.; Asadi, F.K.; Kuntz, K.B.; Maisonneuve, M.; Moffat, B.; Mohammadi, K.; Panneton, D. QEYSSat 2.0—White paper on satellite-based quantum communication missions in Canada. *Can. J. Physics.* **2023**, *103*, 328–376. [CrossRef]
15. Institute of Communications Navigation. QUBE—Satellite-Based Quantum Key Distribution. *DLR*. 2024. Available online: https://www.dlr.de/en/kn/research-transfer/projects/qkd-quantum-technology-for-secure-communication/qube-satellite-based-quantum-key-distribution (accessed on 6 November 2025).
16. Technical University of Munich. Quantum Satellite Launched into Space, TUM. 2025. Available online: https://www.tum.de/en/news-and-events/all-news/press-releases/details/quantum-satellite-launched-into-space (accessed on 6 November 2025).
17. Hutterer, M.; Auer, M.; Baliuka, A.; Bayraktar, O.; Freiwang, P.; Gall, M.; Günther, K.; Haber, R.; Janusch, J.; Knips, L.; et al. QUBE-II—Quantum Key Distribution with a CubeSat. In Proceedings of the 73rd International Astronautical Congress (IAC), Paris, France, 18–22 September 2022.
18. The European Space Agency. ESA and European Commission to Build Quantum-Secure Space Communications Network. 2025. Available online: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_and_European_Commission_to_build_quantum-secure_space_communications_network (accessed on 23 November 2025).
19. EUSpace. IRIS^2: Infrastructure for Resilience, Interconnectivity and Security by Satellite. EUSPA. 2023. Available online: https://www.euspa.europa.eu/sites/default/files/2024-03/IRIS2.pdf (accessed on 6 November 2025).
20. Lindman, N. SAGA 1G-preparing for EuroQCI. Divqsec. 2023. Available online: https://divqsec.de/wp-content/uploads/2023/09/woq2023_03_lindman_saga.pdf (accessed on 6 November 2025).
21. Lu, C.Y.; Cao, Y.; Peng, C.Z.; Pan, J.W. Micius quantum experiments in space. *Rev. Mod. Phys.* **2022**, *94*, 035001. [CrossRef]
22. Ghassemlooy, Z.; Khalighi, M.A.; Zvanovec, S.; Stevens, N.; Alves, L.N.; Shrestha, A.; Tavakkolnia, P.D.; Tegos, S.A.; Papanikolaou, V.K.; Aparicio-Esteve, E.; et al. Final White Paper, NEWFOCUS CA19111 COST Action: European Network on Future Generation Optical Wireless Communication Technologies. COST (European Cooperation in Science and Technology) Action CA19111, NEWFOCUS. 2024. Available online: https://hal.science/hal-04671609 (accessed on 6 November 2025).
23. Meyer, J.; Reches, Y.; Gary Rozenman, G.; Oz, Y.; Suchowski, H.; Arie, A. Analogy of free-space quantum key distribution using spatial modes of light: Scaling up the distance and the dimensionality. *Opt. Lett.* **2025**, *50*, 3297–3300. [CrossRef]
24. Oliveira, R.D.; Zhang, P.; Davidson, Z.C.; Salas, E.H.; Kosmatos, E.A.; Stavdas, A.; Lord, A.; Rarity, J.; Nejabati, R.; Simeonidou, D. On the integration and control of quantum key distribution over free-space optics and 5G networks. In Proceedings of the 2024

International Conference on Optical Network Design and Modeling (ONDM), Madrid, Spain, 6–9 May 2024; IEEE: Piscataway, NJ, USA, 2024.
25. Zhang, P.; Sagar, J.; Hastings, E.; Stefko, M.; Joshi, S.; Rarity, J. End-to-end demonstration for CubeSatellite quantum key distribution. *IET Quantum Commun.* **2024**, *5*, 291–302. [CrossRef]
26. Baselga, O.; Calveras, A.; Ruiz-de-Azua, J.A. Exploring the Performance of Transparent 5G NTN Architectures Based on Operational Mega-Constellations. *Network* **2025**, *5*, 25. [CrossRef]
27. 3GPP TR 38.300. NR and NG-RAN Overall Description. 3GPP. 2025. Available online: https://www.3gpp.org/ftp/Specs/archive/38_series/38.300 (accessed on 6 November 2025).
28. Wang, C.; Ma, X.; Xing, R.; Li, S.; Zhou, A.; Wang, S. Delay- and Resource-Aware Satellite UPF Service Optimization. *IEEE Trans. Mob. Comput.* **2025**, *24*, 2564–2579. [CrossRef]
29. Cheng, S.; Ling, X. Latency Analysis of LEO Satellite Relay Communication: An Application of Conditional Contact Angle Distribution. Geometric Topology (math.GT). *arXiv* **2023**, arXiv:2309.05572.
30. Luan, X.; Wu, J.; Xu, X.; Ren, S.; Xiang, H. Research on the propagation delay characteristic of multi-beam GEO satellite communications system. In Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011), Gangwon, Republic of Korea, 13–16 February 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 620–623.