Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9927255, 15 pages
https://doi.org/10.1155/2022/9927255

Review Article

An Overview on Deployment Strategies for Global Quantum Key Distribution Networks

Jing Wang and Bernardo A. Huberman

Next-Generation Systems, CableLabs, 858 Coal Creek Circle, Louisville, CO 80027, USA

Correspondence should be addressed to Jing Wang; j.wang@cablelabs.com

Received 4 March 2021; Revised 28 December 2021; Accepted 2 April 2022; Published 25 April 2022

Academic Editor: Weizhi Meng

We present a comprehensive literature review and comparative study on the deployment strategies of quantum key distribution (QKD) networks for global coverage. The state-of-the-art deployment strategies, including terrestrial QKD via optical fibers, free-space QKD via ground-based fixed links and ground-to-air dynamic links, and satellite QKD, are reviewed and compared in terms of channel loss, interference, distance limit, connection topology, and deployment cost. Selection criteria and deployment strategies are developed to enable a global coverage of QKD networks from intercontinental, long-haul, metro, to access networks.

1. Introduction

Modern telecommunication relies on cryptography to protect the security of data traffic, where the confidentiality and integrity of keys become the bottlenecks of the whole system. Today's cryptographic systems can be divided into two categories, symmetric and asymmetric. The security of asymmetric cryptographic algorithms, i.e., public key algorithms, relies on the computational complexities of intractable mathematical problems, e.g., the integer factorization problem (RSA), the discrete logarithm problem (Diffie-Hellman), and the elliptic-curve discrete logarithm problem (ECC) [1]. Solving these problems requires tremendous amounts of computational resources. While not feasible for classical computers, these problems can be solved in polynomial time by a quantum computer running Shor's algorithm [1, 2]. To make things worse, increasing the key length does not help, since the required qubit number only scales linearly with the key length [1]. In 2019, Google claimed to have achieved quantum supremacy [3], whereas IBM argued that quantum computers will never reign supreme over, but rather work in concert with classical computers [4]. On the other hand, symmetric cryptographic algorithms, e.g., AES and SNOW 3G, are considered to be resistant against quantum computers. Although Grover's algorithm does speed up the attacks against symmetric ciphers, increasing the key length can effectively block these attacks [1, 5]. In modern communication, symmetric cryptography is only used for encryption and decryption. All other functions, such as signature, authentication, and key exchange, are carried out by asymmetric cryptography. Once sufficiently powerful quantum computers exist, classical cryptography will no longer be safe.

To address the challenges of quantum computing, two technological strategies were developed, postquantum cryptography (PQC) and quantum key distribution (QKD). PQC, also known as quantum-safe or quantum-proof cryptography, focuses on increasing the computational complexity by inventing new intractable problems [5]. Thanks to its software implementation and full compatibility with existing systems, PQC is considered a good candidate for postquantum eras. Three rounds of submissions have been organized by the National Institute of Standards and Technology (NIST) [6–8]. It is worth noting that, like the classical counterparts, PQC algorithms also rely on the assumptions of the computational power of attackers. They are only safe against quantum computers with a certain number of qubits but may lead to long-term issues due to the ever-growing computational power.

QKD, also known as quantum cryptography, relies on quantum mechanics, instead of mathematical assumptions, to guarantee the security of keys [9–12]. Instead of computational security, it offers information-theoretic security, i.e., the keys are deemed secure even if the adversary has unlimited computing power. From the first idea [13] to the first demonstration [14], various QKD protocols [10] and network topologies [11, 12] have been reported. It was found later, however, that the absolute security of QKD is only guaranteed for ideal devices, e.g., single-photon sources and single-photon detectors (SPDs) [15]. The lack of perfect single-photon sources and low detection efficiency of SPDs create security loopholes, which could be exploited by side-channel attacks.

In real systems, expensive single-photon sources are replaced by attenuated lasers to produce weak coherent pulses (WCP), whose photon number per pulse follows the Poisson distribution, so there are always pulses containing multiple photons. Multiphoton pulses could be the target of a photon-number-split (PNS) attack, where an eavesdropper blocks all single-photon pulses and divides multiphoton pulses, keeping half for herself and sending the rest to Bob. To eliminate this loophole, decoy-state protocols were invented to vary the photon number per pulse [16–18] so the blocking strategy of the eavesdropper will be revealed.

On the detector side, measurement-device-independent (MDI) protocols can close all detection loopholes and are immune to side-channel attacks on imperfect detectors [19, 20]. In conventional prepare-and-measure protocols, Alice prepares qubits and sends them to Bob; Bob makes measurements on the received qubits. In MDI protocols, both Alice and Bob prepare random qubits independently and send them to a third party, Charlie, for Bell state measurement (BSM). Charlie can only tell the results of BSM but cannot tell the two photons from Alice and Bob since they are indistinguishable; therefore, he does not know the qubits sent by Alice/Bob. Charlie announces the results of successful BSM events, based on which Alice and Bob infer each other's keys. Since Charlie serves as an untrusted relay, he can be controlled by an eavesdropper without information leakage. The postselection of successful BSM events entangles the qubits from Alice and Bob; that is why MDI-QKD is equivalent to a time-reversed entangled-photon-pair (EPR) protocol. In summary, MDI-QKD with decoy-state protocols eliminates the loopholes on both photon sources and detectors.

So far, QKD technologies have grown out of the laboratory and become ready to reach the market [21, 22]. Various demonstrations and field trials have been reported, including terrestrial QKD via optical fibers, free-space QKD on the ground and in the atmosphere, and satellite QKD between a satellite and a ground station. Meanwhile, quite a few different QKD protocols have also been studied. For terrestrial QKD networks in optical fibers, both discrete-variable protocols, e.g., polarization/phase-encoding BB84, E92, and coherent one way, and continuous-variable protocols have been investigated, and there is no decisive conclusion about the best choice. For free-space and satellite QKD, on the other hand, polarization-encoding BB84 protocol has been used extensively. Terrestrial QKD networks via optical fibers include the DARPA quantum network in Boston [23, 24], SwissQuantum network in Geneva [25, 26], SECOQC network in Vienna [27–30], metropolitan QKD networks in Tokyo [31] and Cambridge [32], and Beijing-Shanghai QKD backbone network in China [33]. QKD links in optical fibers are limited by short transmission distances, less than 600 km in the lab and ~100 km in the field. This is because the key rate scales linearly with channel transmittance, which decays exponentially with distance in optical fibers due to the photon absorption.

There are several strategies to extend QKD distance, including quantum repeater and trusted and untrusted relays. Despite recent advances, a quantum repeater remains infeasible because it requires high-quality quantum memory and complicated local entanglement distillation. Trusted relays can unlimitedly extend QKD distance with the penalty of key exposure since the key information ceases to be quantum at each intermediate node. Untrusted relays seem to be a promising candidate to extend QKD distance. Extensive research effort has been spent on MDI-QKD [34–40] and twin-filed QKD (TF-QKD) [41–48], where Alice and Bob independently prepare random qubits, and both send them to the relay node for measurement. Several field trials of time-bin phase-coding MDI-QKD have been reported in China [34–37], featuring a metropolitan scale of less than 200 km and a key rate of several bits per second [35]. A field trial demonstrated 15-30 km distances from users to the relay node with key rates of 16-38.8 bit/s [37]. More sophisticated three-intensity [38] and asymmetric four-intensity [39, 40] decoy-state protocols were proposed to further extend the distance and increase the key rate. The asymmetric four-intensity decoy-state protocol exploits three intensities (vacuum, weak, and signal states) in the X basis, and one intensity in the Z basis, and archives a distance record of 404 km using ultralow loss optical fibers (0.16 dB/km) with a key rate of only 1.16 bits per hour [40].

The key rates of prepare-and-measure and MDI-QKD protocols scale linearly with the channel transmittance η. Since the channel transmittance decays exponentially with distance in optical fibers, this linear bound severely limits the achievable distances and key rates [41]. Phase-matching QKD [41, 42] and twin-field QKD [43–48] can overcome this linear constraint by matching the phases of two coherent states and encoding key information on the common phase. It makes the key rates scale with the square root of the channel transmittance while keeping the same untrusted relay merit as MDI-QKD. Using a practical sending-or-not-sending (SNS) protocol [41], several milestone experiments have been demonstrated to set new distance records for terrestrial QKD, e.g., 509 km in the lab with ultralow loss fibers [45], 511 km [46] and 428 km [47] in field trials, and 605 km using dual-band stabilization technique for Rayleigh scattering noise reduction [48].

There is another category of QKD protocols, continuous-variable QKD, based on Gaussian modulation and coherent detection [49]. It features higher key rate for a short distance and improved compatibility with commercial coherent optical communication systems [50]. So far,

the distance records of CV-QKD are 200 km in the lab [51] and 50 km in the field [52], making it suitable for metropolitan networks.

The point-to-point (P2P) nature of quantum channels and its requirement of dedicated fibers hamper the wide deployment of terrestrial QKD networks. To enable the coexistence of quantum and classical channels in existing fiber infrastructures, wavelength division multiplexing (WDM) techniques have been investigated [53, 54]. Many works focus on the mitigation of interference caused by spontaneous Raman scattering (SRS) from classical channels [55–58]. So far, the coexistence of quantum and classical channels has been demonstrated in backbone [59, 60], metro [61–64], and access [65–71] networks.

Due to the low channel loss in space and negligible interference from classical channels, satellite QKD drew significant research interest and has been considered as a promising candidate to enable global coverage of QKD networks [72, 73]. The feasibility studies of satellite QKD started back in 2002 [74–76]. The first free-space QKD link on the ground was realized in 1996 [77] with a distance of 150 m (indoor) or 75 m (outdoor). After that, several ground-based fixed free-space QKD links were reported with distances up to 144 km [78–82]. The road toward satellite QKD was paved by the demonstration of dynamic free-space QKD links with airborne quantum transmitters [83, 84] or receivers [85–87]. Ground-based free-space QKD links were investigated as a preliminary step toward satellite QKD, but from the perspective of deployment, they are not quite practical due to the limit of line-of-sight (LoS) connections, geographical constraints (e.g., landscape and buildings), and adverse environmental influences (e.g., vibration, weather, and atmospheric turbulence). In real applications, ground-based free-space QKD links are only suitable for the last segment of access networks.

On the other hand, satellite QKD can achieve distances up to more than 1000 km thanks to the low channel loss in space [88–98]. Most reported works focused on low-earth-orbit (LEO) satellites, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite with high angular speed [88, 89]. The Micius satellite of China at ~500 km altitude realized downlink QKD from the satellite to ground over 1200 km [90]. As a trusted relay, it also enables intercontinental quantum-secured communication over 7600 km between China and Austria [91, 92]. Although the downlink QKD scheme from a satellite to the ground has the potential for higher detection efficiency and higher key rates, it requires more payload on the satellite and is not as flexible as the uplink scheme. An uplink scheme has higher channel loss and low detection efficiency but features a simple payload of quantum receivers on a spacecraft. Micius uses downlink channels for QKD and entanglement distribution and is also compatible with uplink schemes for quantum teleportation [89]. Canada's satellite plan (QEYSSat) employs an uplink scheme [93] and the feasibility of high channel loss [94–96], optical terminal design [97], and noise of SPDs in space [98] have been investigated. To further simplify the payload on satellite, a corner cube retroreflector with a modulator for polarization encoding is proposed [99]. Besides LEO satellites, QKD via medium earth orbit (MEO) [100] and geostationary orbit (GEO) [101, 102] satellites are also under investigation. Miniaturization and standardization of satellites have now become the trends of satellite QKD [103–107].

All aforementioned satellite QKD utilizes the satellite as a trusted relay. To eliminate the key leakage at the satellite, satellite-to-ground entanglement distribution has been demonstrated [108–111] with a distance record of 1200 km [110]. Before that, free-space entanglement distribution on the ground was studied [112–115] with distances of more than 100 km in the atmosphere [113, 115]. Moreover, free-space MDI-QKD was also demonstrated as an alternative to entanglement distribution [116].

Deployment strategies of QKD networks include terrestrial QKD via optical fibers, free-space QKD on the ground or from the ground to an airborne platform, and satellite QKD. Each method has its strengths and limitations and none of them can achieve global coverage alone. So far as we know, there is no comparative study of different deployment strategies. In this paper, we present a literature overview of existing deployment strategies of QKD networks and compare their pros and cons in terms of channel loss, interference, distance, connection topology, deployment cost, and use scenarios. Selection criteria and requirements for different network segments are developed to enable a global coverage of QKD networks, from intercontinental, long-haul, metro, to access networks.

Figure 1 shows a global telecommunication network, which can be divided into four segments, intercontinental (>5000 km), long-haul (1000-5000 km), metro (100-1000 km), and access (<100 km). Each segment features different connectivity topologies. Intercontinental and long-haul networks feature point-to-point (P2P) connectivities; metro networks utilize ring and mesh topologies; access networks have tree or star topologies.

2. Terrestrial QKD via Optical Fibers

Figure 2(a) shows the architecture of a terrestrial QKD link via optical fibers. Ideally, a quantum channel is deployed in a dedicated dark fiber to avoid the interference caused by SRS noise from classical channels. In case of fiber deficiency, it can also share the same fiber with classical channels using time/wavelength-division multiplexing (TDM/WDM) techniques. There are several techniques to reduce the interference from classical channels, such as spectral filtering before the quantum receiver, temporal filtering (i.e., gated SPDs), and power control of classical channels.

Figure 2(b) shows the setup of a prepare-and-measure QKD protocol. So far, several terrestrial QKD networks via optical fibers have been demonstrated, including the DARPA quantum network in Boston [23, 24], SwissQuantum network in Geneva [25, 26], SECOQC network in Vienna [27–30], metropolitan QKD networks in Tokyo [31] and Cambridge [32], and Beijing-Shanghai QKD backbone network in China [33]. Most of them are based on prepare-and-measure protocols with distance limits of hundred kilometers. In real deployments, the usable distance

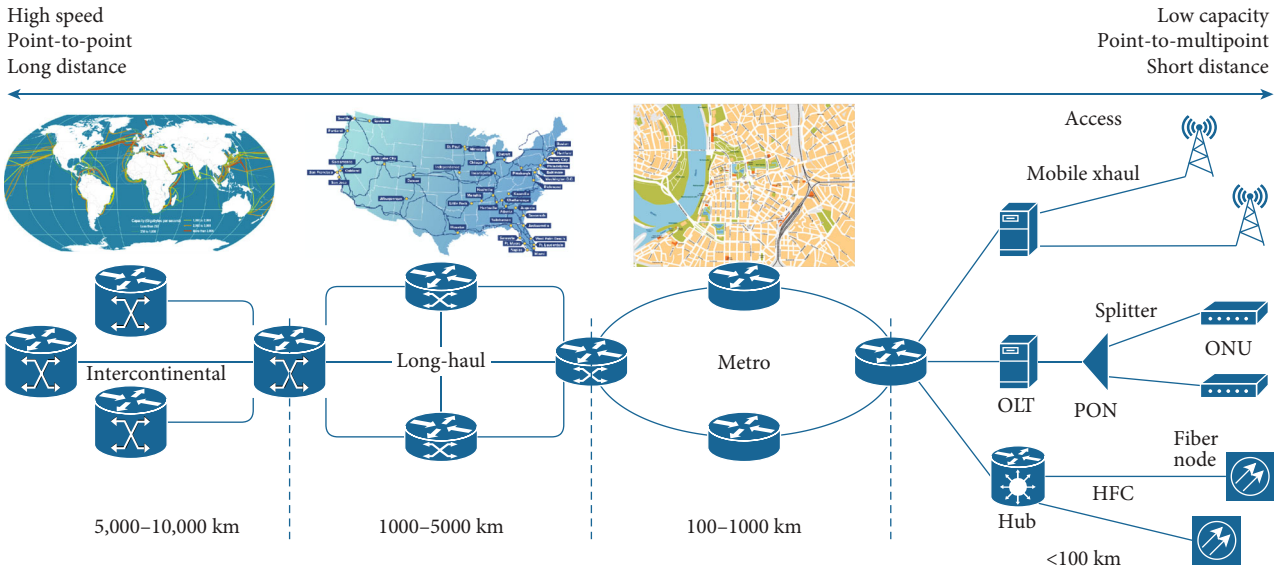

Figure 1: Global coverage of telecommunication networks, from the intercontinental, long-haul, metro, to access networks.

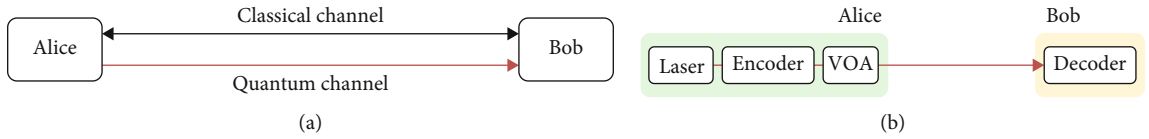

Figure 2: Terrestrial QKD via optical fibers. (a) To avoid interference from classical channels, the quantum channel is deployed in a dedicated fiber. (b) The setup of a prepare-and-measure protocol.

will be further reduced to ~100 km. This is because the achievable key rate scales linearly with channel transmittance, which decays exponentially with distance in optical fibers due to absorption. Therefore, terrestrial QKD via optical fibers is impractical for long-haul applications. For example, with a loss of 0.2 dB/km, a 1000 km fiber introduces a channel loss of 200 dB, which is so high that only 0.3 photons arrive at the receiver per century even if a 10 GHz single-photon source was used at the transmitter.

Relay technologies are essential to increase the distance and enhance the coverage area of terrestrial QKD networks. There are two categories of relaying technologies, trusted and untrusted, depending on whether the relay node has access to the keys. The operation principles of a trusted relay node are shown in Figure 3(a). It connects two neighboring nodes that are too far away from each other to establish a direct QKD link. The trusted relay node, Charlie, performs QKD with Alice and Bob, respectively, and obtains keys of K_A and K_B. He then makes a parity announcement of $K_C = K_A \oplus K_B$, which is a bitwise parity check of K_A and K_B. Since the original keys are independent bit strings, their bitwise parity is a uniformly random bit string, which does not reveal any information about the keys. With the help of K_C, both Alice and Bob can then infer the key of each other using the fact that $K_A \oplus (K_A \oplus K_B) = K_B$ and $K_B \oplus (K_A \oplus K_B) = K_A$. Trusted relay can extend the distance of secure communication unlimitedly, but with the penalty of key exposure at each relay node.

An interesting synergy is that classical fiber cables have repeaters every 100 km for the reamplification, reshaping, and retiming of classical pulses. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. For example, the Beijing-Shanghai backbone link in China uses 32 trusted relay nodes to divide the overall distance of more than 2000 km into many small segments, each less than 100 km. Moreover, a trusted relay node offers compatibility to the point-to-multipoint (P2MP) network topology, as shown in Figure 3(b).

On the other hand, an untrusted relay eliminates the key leakage at the relay node. It can be implemented by the distribution of entangled photon pairs or measurement-device-independent (MDI) QKD. In either case, the relay node has no information on the keys and could even be an eavesdropper itself. Figure 4(a) shows an entanglement distribution setup, where an entangled photon source at the relay node generates entangled photon pairs (EPR) using a nonlinear crystal or nonlinear fibers. The entangled photons are distributed to two users, who make independent measurements and get correlated results. The relay node is considered secure since the entangled photon source has no access to the exact states of two photons, but the measurement results of two users are always correlated. Figure 4(b) shows an MDI-QKD setup. Two users prepare random qubits

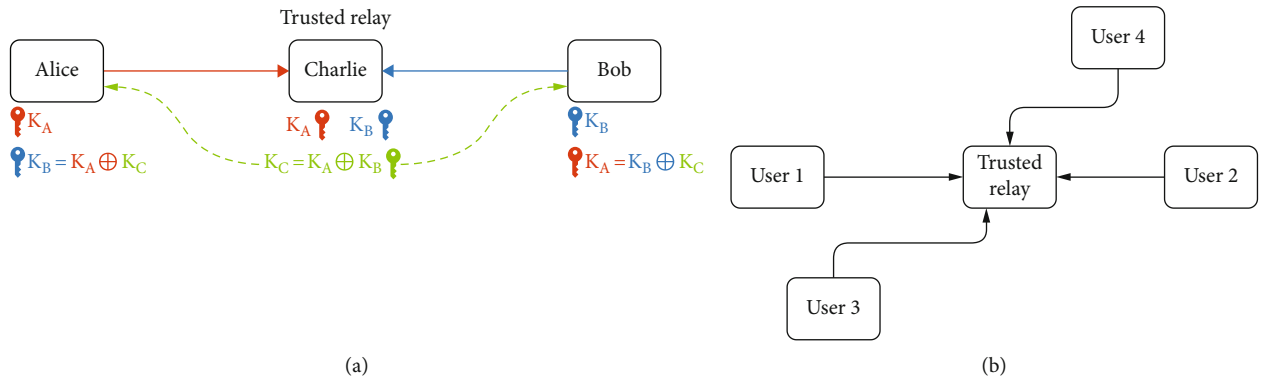

Figure 3: Trusted relay for terrestrial QKD networks. (a) The operation principles of a trusted relay. (b) A trusted relay node offers compatibility with point-to-multipoint networks.

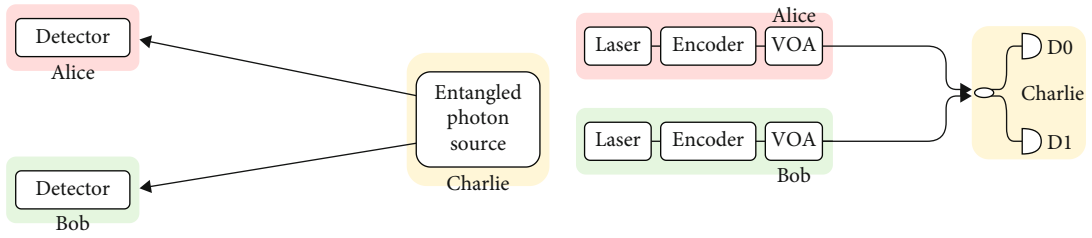

Figure 4: Untrusted relay for terrestrial QKD networks. (a) Distribution of entangled photon pairs. (b) Measurement-device-independent (MDI) QKD.

independently and send them to the relay node for Bell state measurements (BSM). Although the BSM cannot tell the exact states of two incoming photons, it can tell whether or not the two photons have entangled states. By postselecting entangled photons from the two users, MDI-QKD is equivalent to a time-reversed EPR protocol. So far, the distance record for MDI-QKD is 404 km using asymmetric four-intensity decoy-state protocol in ultralow loss optical fibers [40]. The key rate, however, is only 1.16 bit/s per hour, which is orders of magnitude lower than practical requirements.

The key rate of conventional QKD, including prepare-and-measure protocols, entanglement distribution, and MDI-QKD, has linear dependency on the channel transmittance η. Since the channel transmittance decays exponentially with distance in optical fibers, this linear bound severely limits the achievable key rate and distance of terrestrial QKD networks. Recently, a new QKD protocol, twin-field (TF) QKD, was proposed to overcome the linear key-rate constraint. Its setup is almost identical to a phase-encoding MDI-QKD and maintains the same merit of an untrusted relay, where pairs of phase-randomized optical fields are generated at two distant locations and combined at a central measuring station. Fields imparted with the same random phase are "twins" and can be used to distill a key. By matching the phases of two coherent states and encoding key information into the common phase, TF-QKD exhibits the same dependence on distance as quantum repeaters, i.e., its key rate scales with the square root of the channel transmittance. Several milestone experiments have been demonstrated to set new distance records of fiber-based terrestrial QKD links [45–48]. It should be noted that in MDI-QKD, the two photons from two users interfere at the relay station, where Charlie's receiver has two-photon interference and records coincidence detections. In TF-QKD, however, two optical fields are sent from two users to Charlie's receiver, where a single-photon interference is carried out followed by a single-photon detection event. TF-QKD retains the characteristics of MDI-QKD, whereas gaining extra distance thanks to the square-root dependence of key rate on the channel transmittance.

3. Free-Space QKD

Figure 5 shows the architectures of free-space QKD. Figure 5(a) shows ground-based free-space QKD links. Different from optical fibers, free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. The associated classical channels could exploit wireless links, e.g., cellular, microwave, or rely on free-space optics as well. Since no fiber trenching is required, free-space QKD features low deployment cost and easy and fast installation and is an important reinforcement for fiber-based QKD networks owing to its configurational flexibility. The distance record for ground-based free-space QKD is 144 km [82]. Dynamic free-space QKD links to/from an aircraft were investigated as a preliminary step toward satellite QKD, and the feasibility of both downlink and

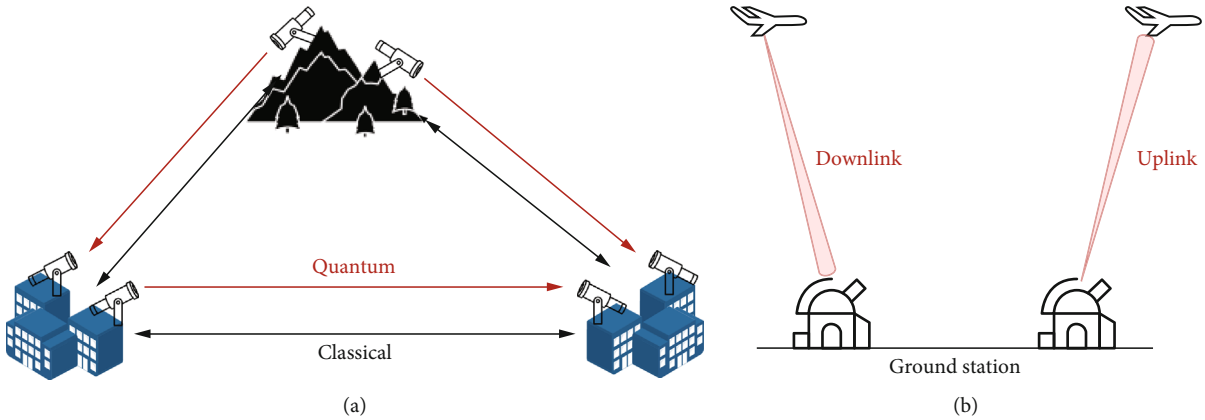

Figure 5: Free-space QKD. (a) Ground-based free-space QKD links. (b) Free-space QKD links to/from an aircraft.

uplink configurations has been verified, shown in Figure 5(b). A downlink scheme includes a flying transmitter on an airborne platform and a receiver on the ground [83, 84]; an uplink configuration uses a ground-based transmitter and places a quantum receiver on aircraft [86, 87]. The downlink scheme has higher detection efficiency, whereas the uplink scheme has a smaller payload on aircraft.

Since the quantum channel is not confined in the waveguide of optical fibers, free-space QKD is subject to environmental influence, such as vibration, adverse weather (fog, rain, and cloud), and atmospheric turbulence. Although the atmosphere has lower absorption than optical fibers, only 0.07 dB/km at 2400 m, the channel loss of free-space QKD is not dominated by absorption. Instead, it is determined by diffraction, weather, turbulence, and misalignment. Moreover, free-space quantum channels are subject to decoherence more than those in optical fibers, which further limits the link distance. On the other hand, there is no interference from classical channels in free space and the coexistence of quantum and classical channels is no longer an issue. Free-space QKD can easily support P2MP topologies, making it a promising candidate for interbuilding secure communication in the last few miles of access networks.

4. Satellite as a Trusted Relay

Thanks to the low channel loss in space, negligible interference from classical channels, and reduced environmental influences, satellite QKD can achieve distances more than 1000 km and is not limited by terrestrial conditions and can provide coverage for rural areas. Most reported work focused on LEO satellites with altitudes of less than 900 km, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite. The feasibility of MEO and GEO satellites is also under investigation. Miniaturization and standardization of satellites are also trends of satellite QKD. Figure 6 shows the operation principles of satellite QKD where the satellite is used as a trusted relay. An LEO satellite performs downlink QKD with two ground stations, Alice and Bob, respectively. It then makes a parity announcement so that Alice and Bob can infer each other's keys. The satellite needs LoS connections with Alice and Bob, but not necessarily at the same time. It can exchange keys with several ground stations one after another as it flies over them. As a trusted relay, any access to the satellite leaks the complete information about keys. The associated classical channels for satellite QKD can rely on terrestrial fibers, microwave, or free-space laser communication in space. For example, most Starlink satellites are currently operating in Ku and Ka bands and can be upgraded to laser communication in the future.

Since the effective thickness of the atmosphere is only ~10 km, the propagation of a quantum channel takes place mostly in vacuum space with negligible absorption and turbulence. Instead of absorption, the channel loss of satellite QKD is determined by beam diffraction and scales quadratically with distance. In comparison, the channel loss of terrestrial QKD is dominated by fiber absorption and scales exponentially with distance. Channels in space also have smaller decoherence than those in the atmosphere or optical fibers. For example, a 600 km optical fiber has a channel loss of 120 dB, whereas a link of the same length in space from satellite to the ground has a loss of only 50 dB given a reasonable aperture size is used at the receiver telescope. This is why satellite QKD can reach much longer distances. Intersatellite channels have even lower losses due to the absence of atmosphere.

Channel loss in space comes from two sources, beam diffraction and beam spreading beyond the effects of diffraction. Diffraction loss depends on the divergence of the transmitter telescope and the aperture size of the receiver telescope. Further beam spreading arises from wavefront aberrations caused by refractive index inhomogeneities due to atmospheric turbulence. There are two categories of turbulence. Small turbulence induces beam spreading, whereas large turbulent eddies with sizes larger than the beam spot cause beam wandering. A long-term beam spot is a superposition of moving short-term beam spots. The short-term beam size is determined by spreading and the instantaneous beam displacement from the unperturbed position caused by beam wandering. In real applications, the channel loss from a satellite to a ground station is dominated by diffraction, followed by beam spreading. Beam wandering and absorption have negligible contributions to the channel loss.

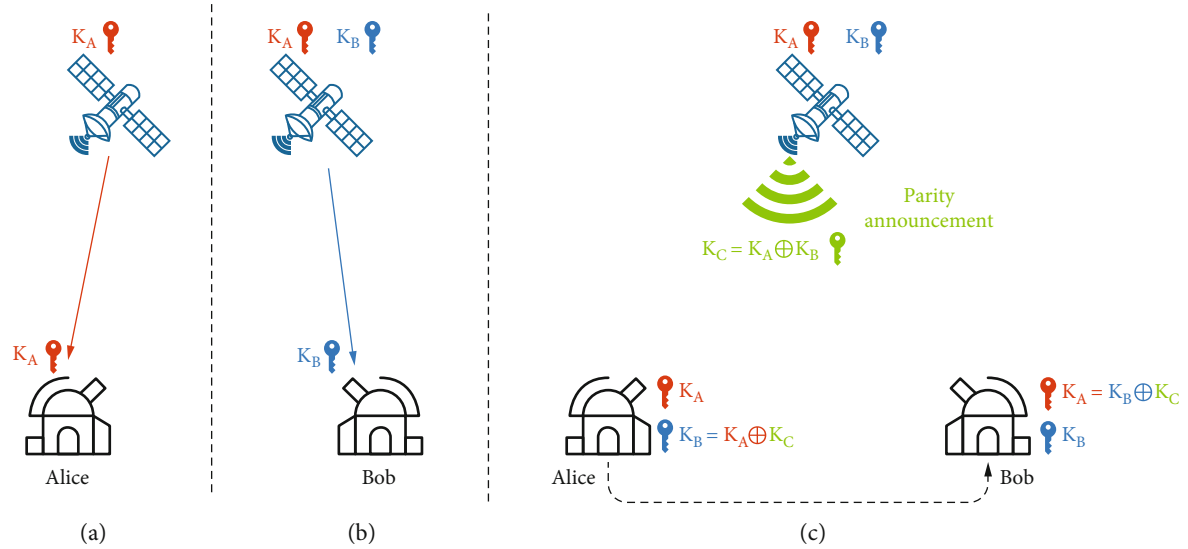

Figure 6: Satellite QKD using the satellite as trusted relays. The relay satellite first exchanges keys with ground stations, (a) Alice and (b) Bob, respectively. (c) The satellite makes a parity announcement so that Alice and Bob can infer each other's keys.

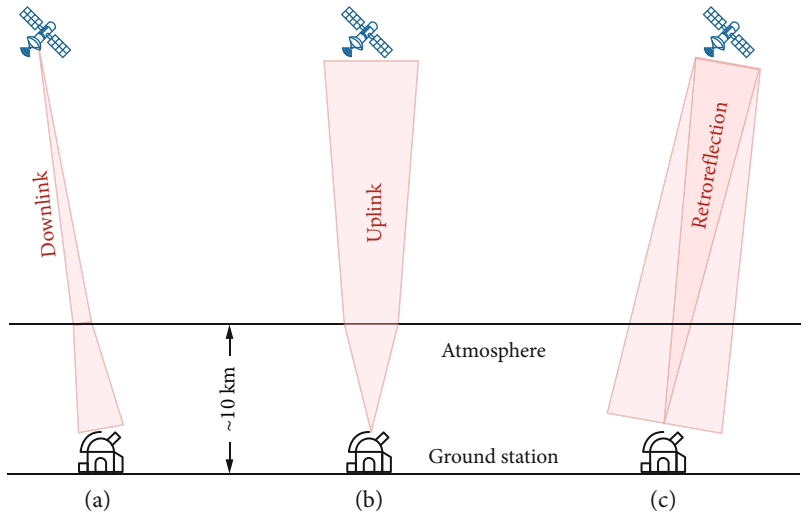

Figure 7: (a) Downlink and (b) uplink configurations of satellite QKD.

Satellite QKD has three different schemes, downlink, uplink, and retroreflection. In Figure 7(a), the downlink scheme has the quantum transmitter on a satellite and receiver on the ground. Since the effective thickness of the atmosphere is only ~10 km, the optical beam first propagates through vacuum space where the only channel loss is diffraction and then passes through the atmosphere in the final stage of the path. Due to the diffraction effect, when the beam arrives at the atmosphere, its size has been larger than most turbulent eddies. There is no beam wandering, and the beam size is spread slightly by wavefront aberrations caused by turbulence. For the downlink configuration, atmospheric turbulence has a limited impact on the channel loss and beam spreading. For example, the beam size after 1200 km downlink propagation expands to 12 m with diffraction loss of ~22 dB depending on the receiver telescope size [90]. Atmospheric turbulence introduces additional 3-8 dB attenuation, with an overall channel loss of less than 30 dB [90].

In Figure 7(b), an uplink channel first propagates through the atmosphere, where the wavefront aberration induced by turbulence causes significant beam spreading. At 500 km altitude, the beam size of an uplink channel can reach up to 50 m, much larger than any available spaceborne telescope aperture. Downlink channels can exploit large aperture receiver telescopes on the ground, but uplink channels have limited aperture size for receiver telescopes due to the weight and size limit on satellites. Thanks to the strong wavefront aberration, large beam spot, and small aperture size, uplink channels have higher losses than downlink ones. For example, a 500 km uplink channel has a loss up to 50 dB, whereas a downlink channel of the same length would have a loss less than 20 dB [94]. Most uplink channels cannot work without the help of the decoy-state technique [94].

Although the downlink scheme has higher detection efficiency and higher key rates, the transmitter setup requires more payload on the satellite and needs more adjustment during operation, which makes the downlink scheme not as flexible as an uplink configuration. The uplink scheme, on the other hand, only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. The downlink scheme leaves expensive and delicate SPDs on the ground for better protection, cooling, and maintenance, whereas the uplink scheme has to launch the sensitive SPDs into space, which have to go through launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space. Due to the sunlight, the satellite temperature varies by up to tens of degrees in one orbit, and there is limited electrical power on the satellite for cooling. The only way to dissipate heat is by radiation. To make things worse, most SPDs are avalanche photon detectors (APD), which are sensitive to dark counts caused by ionizing radiation in space. The feasibility of low-noise SPDs on a satellite is under investigation [98]. So far, downlink and uplink schemes are both considered important for future satellite QKD. For example, Micius uses downlink QKD and entanglement distribution, and it is also compatible with uplink for quantum teleportation [89]. Canada's satellite plan (QEYSSat) employs an uplink scheme [93], and many works have been done to verify the feasibility of high channel loss [94–96], optical terminal design [97], and noise of SPDs in space [98].

In a quantum channel, the qubits are carried by single photons and no amplification is allowed. The only way to increase the signal-to-noise ratio (SNR) is to reduce channel loss and background noise. Thanks to the low loss, downlink channels have larger SNR than uplink ones. In the daytime, the background noise from sunlight makes it difficult to establish a QKD link. One way to improve SNR in the daytime is to use the wavelengths at Fraunhofer lines, i.e., Sun absorption lines. At night, background noise is dominated by moonlight and scattered light from human activities, which depends on the location of the ground stations. SNR at night is orders of magnitude higher than that in the daytime, which is why most satellite QKD works were demonstrated at clear night by downlink channels. There are several techniques to improve the SNR of a free-space quantum link, e.g., reducing the beam size, reducing the field of view of the receiver telescope, narrowband spectral filtering before the receiver, and temporal filtering (gating window) of SPDs.

To further simplify the payload on satellites, a third configuration, retroreflection, was proposed [99, 100], as shown in Figure 7(c). It uses an orbiting corner cube retroreflector on a satellite with a modulator to encode polarizations. The single-photon transmitter is realized by corner cube retroreflectors mounted on a satellite. Only the reflected beam from the satellite to the ground is a quantum channel; the laser beam from the ground station to the satellite has bright classical pulses. This configuration features a compact and low-cost payload on satellite and can be used on not only LEO but also MEO and GEO satellites. The feasibility of single-photon exchange from an MEO satellite using a retroreflection scheme has been verified [100].

5. Satellite as an Untrusted Relay

When a satellite is used as a trusted relay, it has access to all the keys of all ground stations. To avoid the key leakage at the satellite, untrusted relaying is preferred since the eavesdropper gets no information even if it takes full control of the satellite. Figure 8 shows the architecture of satellite QKD with the satellite as an untrusted relay. Figure 8(a) shows entanglement distribution, where an entangled photon source on a satellite sends entangled photons down to two ground stations, Alice and Bob, respectively. Alice and Bob make independent measurements on the incoming photons and get correlated results. Since the entangled photon source has no control over the exact qubits carried by each photon, the satellite has no information of the key. For entanglement distribution, the loss of two downlink channels has to be combined since only photon pairs that both arrive at ground stations can be used for keys.

As an alternative, Figure 8(b) shows satellite MDI-QKD, where two ground stations independently prepare random qubits and send them via uplink channels to a satellite for BSM. Satellite MDI-QKD is equivalent to a time-reversed entanglement distribution protocol. The BSM can only tell whether or not the two photons are entangled, but it cannot tell the exact states of two incoming photons. The loss of two uplink channels has to be combined since only photon pairs that both arrive at the satellite can be used for keys. Due to the high loss of uplink channels, there is no demonstration of satellite MDI-QKD so far. But the feasibility study of free-space MDI-QKD has been reported on the ground over 19.2 km [116], well beyond the effective thickness of the atmosphere (~10 km).

Unlike trusted relaying, untrusted relaying requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation distance between ground stations. For a given altitude of the satellite, wider separation between ground stations makes lower slant angles and longer propagation in the atmosphere, which leads to higher channel loss. The current distance record for entanglement distribution is ~1200 km, achieved by an LEO satellite Micius of China [110].

6. Deployment Strategies for Global Coverage of QKD Networks

Table 1 lists the pros and cons of different deployment strategies of QKD networks, including fiber-based terrestrial QKD, free-space QKD including ground-based and ground-to-air schemes, and satellite QKD with the satellite used as a trusted or untrusted relay. Terrestrial QKD via optical fibers suffers from high channel loss and short distance but offers compatibility with existing fiber infrastructure and P2MP topologies. Since the quantum channels are confined in fiber waveguides, terrestrial QKD networks can operate all day in adverse environments, such as background light, weather, and vibration. Without relays, a single span of fiber-based QKD can reach ~100 km in the field, only suitable for metro and access networks. Trusted relaying can unlimitedly extend the distance of fiber-based QKD with

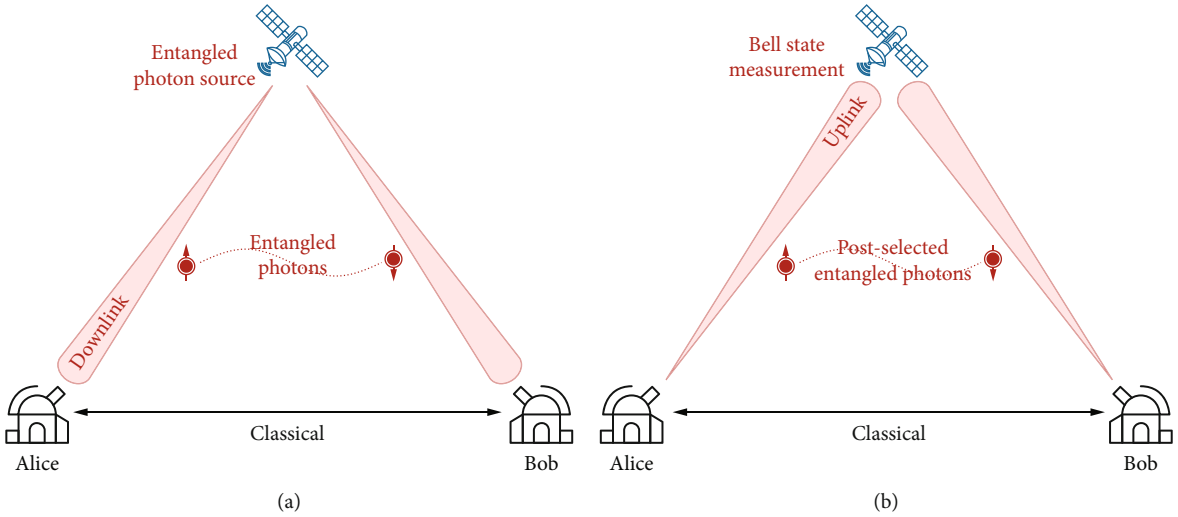

FIGURE 8: Satellite QKD with the satellite as an untrusted relay. (a) Entanglement distribution from a satellite. (b) Free-space MDI-QKD to a satellite.

the penalty of key leakage at each relay node. An interesting synergy is that classical fiber cables also have repeaters every 100 km. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. In contrast, satellite QKD using a satellite as a trusted relay is more secure because the satellite and quantum links are moving fast, making side-channel attacks difficult.

Ground-based free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. It supports P2MP topology and can handle the coexistence of quantum and classical channels without interference. These features make it suitable for the last few miles of access networks among buildings. Although the atmosphere has lower absorption, the channel loss of free-space QKD is dominated by diffraction, adverse weather, and atmospheric turbulence. The distance record of ground-based free-space QKD is 144 km [78], but in real deployments, the usable distance will be less than 10 km for practical key rates. Since no fiber trenching is required, ground-based free-space QKD features low deployment cost and fast and easy installation and serves as an important reinforcement for fiber-based QKD networks. The ground-to-air free-space QKD shares the same pros and cons of ground-based counterparts plus the additional channel loss caused by misalignment and vibration due to the movement of the aircraft. We do not include the applications of airborne free-space QKD here, since it was mainly investigated as a preliminary step towards satellite QKD.

Compared with terrestrial and free-space QKD, satellite QKD features low channel loss and long distances. The downlink scheme from satellite to the ground has higher detection efficiency and higher key rates thanks to the lower loss and less turbulence-induced wavefront abbreviation. But it requires more payload on the satellite and needs more adjustment during operation. The uplink channels are more flexible, since it only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. On the other hand, the downlink scheme leaves expensive and delicate SPDs on the ground for the easiest maintenance, whereas the uplink scheme launches the sensitive SPDs into space, which have to go through the launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space.

Satellite QKD requires LoS connections between the satellite and ground stations and only works at night due to the background noise from sunlight during the daytime. To reduce the channel loss, LEO satellites are preferred, but low altitude leads to the fast movement of the satellite, a small coverage area, and a short flyover time window for each ground station. MEO satellites at higher orbit provide wider coverage and longer flyover time, but with the penalty of higher channel loss and lower key rate [100]. To choose an appropriate altitude, a trade-off must be made between the coverage area and time window versus channel loss and key rate. An extreme example is a geostationary orbit (GEO) satellite, which has an operational time window of the whole night but with a long path length of 35,786 km [101, 102]. There is a strong synergy between satellite QKD and classical satellite communication. For example, space communication also exploits LEO satellites at an altitude of 300-1000 km. Starlink plans to launch thousands of satellites at altitudes of 350-580 km. Although these satellites are using microwave communication in Ku and Ka bands, most of them are equipped with optical transceivers for future upgrades to laser communication. By adding quantum transmitters onboard, these satellites can be used as a trusted relay for QKD in space. Since quantum transmitters for most prepare-and-measure protocols only consist of commercial off-the-shelf devices, this upgrade will not significantly increase the satellite cost. The beam acquisition, tracking, and pointing systems designed for laser communication in space can also be reused by quantum channels. Satellite QKD covers long-haul networks, and by using the

Table 1: Pros and cons of terrestrial, free-space, and satellite QKD.

Deployment strategies	Terrestrial QKD via optical fibers	Free-space QKD on ground	Free-space QKD ground-to-air	Satellite QKD (trusted relay)	Satellite QKD (untrusted relay)
Attenuation	Fiber absorption	Diffraction Turbulence Weather Absorption	Same as ground-based QKD plus Misalignment Vibration	Diffraction Turbulence Weather	Diffraction Turbulence Weather
Interferences from classical channels	Spontaneous Raman scattering noise	No	No	No	No
Channel loss	High, scale exponentially with fiber length	High, scale exponentially with distance		Low Scale quadratically with distance	
Distance	~100 km in fields without relay Unlimited distance with trusted relay MDI-QKD: 404 km in the lab [40] 200 km in fields [35] TF-QKD: >500 km in lab [45, 46, 48] 428 km in fields [47]	144 km in experiments [82] <10 km in real fields	96 km in experiments [84]	Satellite to the ground distance over 1200 km [90] Unlimited distance between ground stations	1200 km between ground stations for a 500-km altitude LEO satellite Longer for MEO/GEO
Compatibility to P2MP topology	P2MP	P2MP	P2P at a time	P2P at a time	Satellite to two ground stations
Line of sight	No	Yes	Yes	Yes	Simultaneous LoS with both ground stations
Time window	Whole day	Only night Need special care for daytime operation		Short window in the clear night	
Deployment	Low cost Dedicated fiber or reuse existing ones	Low cost Simple and fast installation No fiber trenching		Expensive and slow Synergy with satellite laser communication in space	
Application scenarios	Metro, access	Last few miles of access networks		Long haul	

satellites as a trusted relay, its secure distance can be extended unlimitedly.

The scheme with a satellite as an untrusted relay shares the same pros and cons with trusted relays but eliminates the key leakage at satellites. It requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation between two ground stations. The distance record of entanglement distribution from a satellite is 1200 km, which can be employed for long-haul networks, but not long enough for intercontinental connections. Figure 9 shows the deployment strategies for global coverage of QKD networks, from the intercontinental, long-haul, metro, to access networks.

It should be noted that not all user devices are equipped with optical terminals for fiber or free-space optics connections. Radio access has been and will continue to be used extensively in the last few miles of access networks. In these cases, keys have to be distributed wirelessly in a classical way to user devices. Figure 10 shows a hierarchical key delivery architecture. Several secure sites, e.g., bank buildings, business campuses, and government offices, are connected by satellite, fiber-based, or free-space QKD links, so the keys are delivered in an absolute secure way among these secure sites. Within each secure site, however, the keys are distributed wirelessly to mobile users using PQC algorithms. This is a trade-off between security and mobility because it is not feasible to connect all devices with optical fibers or free-space optics. We have to leverage the ubiquity and flexibility of radio access technologies in the last few miles. In this hierarchical architecture, two different levels of security-as-a-service (SaaS) are provided, i.e., absolute security over long-distance among secure sites and computational classical security over a short distance within each site. Once the mobile users

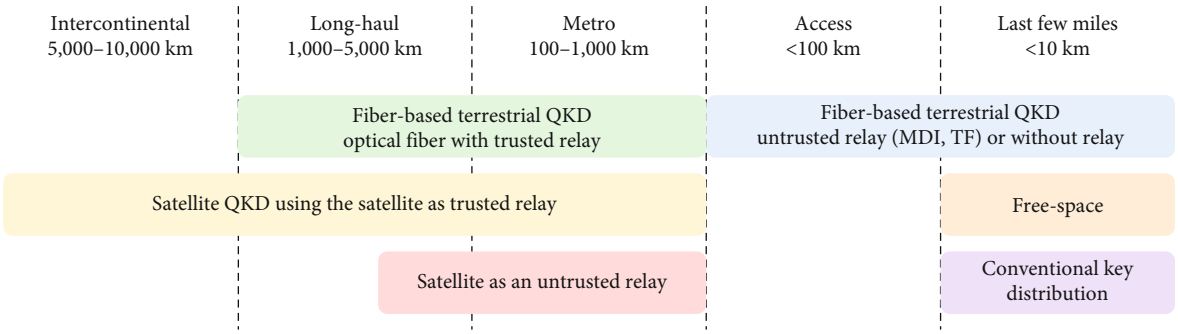

Figure 9: Deployment strategies for global coverage of QKD networks.

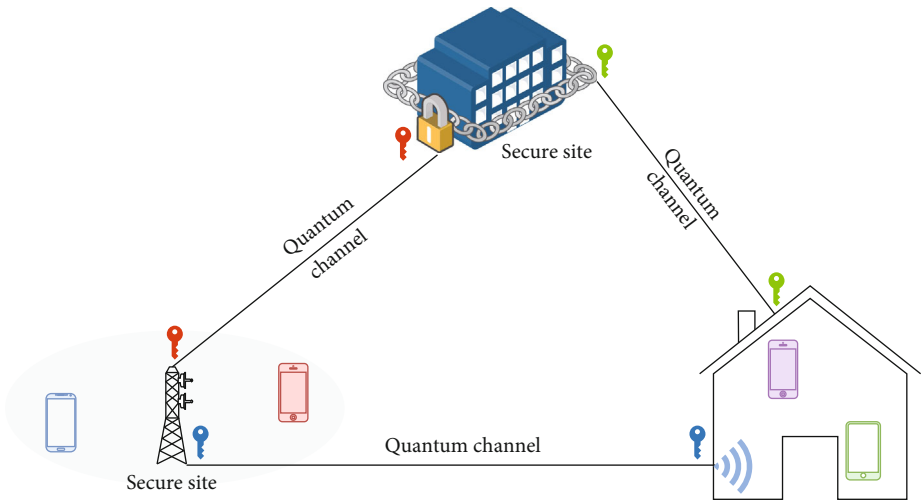

Figure 10: Hierarchical key delivery in the last few hundred meters.

get the keys, they can use these keys to encrypt their wireless communication. They can even roam away from the secure site and continue the secure communication as soon as they still possess the keys. Once they consume all the keys, they have to return to a secure site to fetch new keys. It should be noted that PQC and QKD do not necessarily compete with each other. Instead, they should work in an orchestrated way to complement each other. For example, PQC could exploit the keys delivered by QKD to enhance its security, while QKD can employ PQC for authentication, which cannot be handled by QKD itself.

7. Conclusions

To date, many deployment strategies of QKD networks have been demonstrated, but none of them provides global coverage of QKD networks. A comparative study on the pros and cons of various deployment strategies is still missing. In this paper, the state-of-the-art deployment technologies of QKD networks, including fiber-based terrestrial QKD, free-space QKD, and satellite QKD, are compared in terms of channel loss, interference, distance limit, connection topology, deployment cost, and application scenarios. Instead of competing with each other, these different deployment strategies will work in an orchestrated way to complement each other and enable a global coverage of QKD networks, from intercontinental, long-haul, metro, to access networks.

Given its compatibility with P2MP topology and ~100 km distance limit without relay, fiber-based terrestrial QKD is suitable for metro and access networks. With the help of a trusted relay, the QKD distance can be extended unlimitedly to cover long-haul networks, where the relay nodes are collocated with classical fiber repeaters. Ground-based free-space QKD is limited to 10 km due to diffraction, weather, and atmosphere turbulence and is suitable for the last few miles among buildings in access networks. Satellite QKD features low channel loss, high key rates, and long distances more than 1000 km. By utilizing satellites as trusted relays, the QKD distance can be extended infinitely and can be used for intercontinental, long-haul, and metro networks. Furthermore, satellite QKD is not restricted by terrain conditions and can reach rural underserved areas without difficulty. On the other hand, using a satellite as an untrusted relay requires simultaneous LoS connections from the satellite to both ground stations, where the separation between the ground stations is limited by the altitude of the satellite.

Data Availability

Data are not available.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] E. Grumbling and M. Horowitz, *Quantum Computing: Progress and Prospects*, The National Academies Press, Washington, 2019.

[3] F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[4] IBM Research Blog, *On Quantum Supremacy*, vol. 22, 2019, Oct 2019.

[5] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., Springer, Berlin, Heidelberg, 2009.

[6] L. Chen, S. Jordan, Y.-K. Liu et al., *Report on Post-Quantum Cryptography*, NISTIR 8105, 2016.

[7] G. Alagic, J. Alperin-Sheriff, D. Apon et al., *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8240, 2019.

[8] G. Alagic, J. Alperin-Sheriff, D. Apon et al., *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8309, 2020.

[9] C. H. Bennett, "Quantum cryptography: uncertainty in the service of privacy," *Science*, vol. 257, no. 5071, pp. 752-753, 1992.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[12] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, Bangalore, India, December 1984.

[14] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[15] D. Gottesman, L. Hoi-Kwong, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information & Computation*, vol. 4, no. 5, pp. 325–360, 2004.

[16] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, article 057901, 2003.

[17] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, article 230503, 2005.

[18] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, article 230504, 2005.

[19] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, article 130503, 2012.

[20] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 112, no. 19, article 190503, 2014.

[21] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441-442, 2014.

[22] M. Peev, "Why do I believe that quantum key distribution (QKD) is finally about to reach telecom markets and grow out of its present exotic standing?," in *Optical Fiber Communications Conference (OFC) 2019, paper W4D.3*, San Diego, CA, 2019.

[23] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Building the quantum network," *New Journal of Physics*, vol. 4, p. 46, 2002.

[24] C. Elliott, A. Colvin, D. Pearson et al., "Current status of the DARPA quantum network," *Quantum Information and Computation III*, vol. 5815, 2005.

[25] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, article 063027, 2010.

[26] D. Stucki, M. Legré, F. Buntschu et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, article 123001, 2011.

[27] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *International Journal of Quantum Information*, vol. 6, no. 2, pp. 209–218, 2008.

[28] M. Peev, T. Länger, T. Lorünser et al., "The SECOQC quantum-key-distribution network in Vienna," in *Optical Fiber Communication Conference (OFC) 2009*, 2009, paper OThL2.

[29] M. Peev, A. Poppe, O. Maurhart, T. Lorünser, T. Langer, and C. Pacher, "The SECOQC Quantum Key Distribution Network in Vienna," in *35th European Conference on Optical Communication*, Vienna, Austria, 2009, paper 1.4.1.

[30] M. Peev, C. Pacher, R. Alléaume et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, article 075001, 2009.

[31] M. Sasaki, M. Fujiwara, H. Ishizuka et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[32] J. F. Dynes, A. Wonfor, W. S. Tam et al., "Cambridge quantum network," *Nature Partner Journals (NPJ) Quantum Information*, vol. 5, article 101, 2019.

[33] Q. Zhang, F. Xu, Y.-A. Chen, C. Z. Peng, and J. W. Pan, "Large scale quantum key distribution: challenges and solutions [invited]," *Optics Express*, vol. 26, no. 18, pp. 24260–24273, 2018.

[34] Y. Liu, T. Y. Chen, L. J. Wang et al., "Experimental measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 111, article 130502, 2013.

[35] Y. L. Tang, H. L. Yin, S. J. Chen et al., "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, article 190501, 2014.

[36] Y. L. Tang, H. L. Yin, S. J. Chen et al., "Field test of measurement-device-independent quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, article 6600407, pp. 116–122, 2015.

[37] Y. L. Tang, H. L. Yin, Q. Zhao et al., "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Physical Review X*, vol. 6, article 011024, 2016.

[38] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," *Physical Review A*, vol. 87, no. 1, article 012320, 2013.

[39] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Physical Review A*, vol. 93, article 042324, 2016.

[40] H.-L. Yin, T.-Y. Chen, Z.-W. Yu et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, article 190501, 2016.

[41] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, 2018.

[42] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, article 031043, 2018.

[43] X. T. Fang, P. Zeng, H. Liu et al., "Implementation of quantum key distribution surpassing the linear rate- transmittance bound," *Nature Photonics*, vol. 14, no. 7, pp. 422–425, 2020.

[44] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Physical Review A*, vol. 98, no. 6, article 062323, 2018.

[45] J.-P. Chen, C. Zhang, Y. Liu et al., "Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km," *Physical Review Letters*, vol. 124, no. 7, article 070501, 2020.

[46] J. P. Chen, C. Zhang, Y. Liu et al., "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, pp. 570–575, 2021.

[47] H. Liu, C. Jiang, H. T. Zhu et al., "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km," *Physical Review Letters*, vol. 126, article 250502, 2021.

[48] M. Pittaluga, M. Minder, M. Lucamarini et al., "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photonics*, vol. 15, pp. 530–535, 2021.

[49] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, article 057902, 2002.

[50] H. Guo, Z. Li, S. Yu, and Y. Zhang, "Toward practical quantum key distribution using telecom components," *Fundamental Research*, vol. 1, no. 1, pp. 96–98, 2021.

[51] Y. Zhang, Z. Chen, S. Pirandola et al., "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Physical Review Letters*, vol. 125, no. 1, article 010502, 2020.

[52] Y. Zhang, Z. Li, Z. Chen et al., "Continuous-variable QKD over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, article 035006, 2019.

[53] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[54] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, article 103042, 2010.

[55] M. S. Goodman, P. Toliver, R. J. Runser et al., "Quantum cryptography for optical networks: a systems perspective," *The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society*, vol. 2, pp. 1040-1041, 2003, paper ThEE1.

[56] N. A. Peters, P. Toliver, T. E. Chapuran et al., "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New Journal of Physics*, vol. 11, article 045012, 2009.

[57] T. E. Chapuran, P. Toliver, N. A. Peters et al., "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics*, vol. 11, no. 10, article 105001, 2009.

[58] N. A. Peters, P. Toliver, T. E. Chapuran et al., "Quantum communications in reconfigurable optical networks: DWDM QKD through a ROADM," in *Conference on Optical Fiber Communication (OFC) 2010, paper OTuK1*, San Diego, CA, 2010.

[59] L.-J. Wang, K.-H. Zou, W. Sun et al., "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," *Physics Review A*, vol. 95, no. 1, article 012301, 2017.

[60] Y. Mao, B.-X. Wang, C. Zhao et al., "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics Express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[61] W. Chen, Z. F. Han, T. Zhang et al., "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[62] S. Wang, W. Chen, Z. Yin et al., "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[63] S. Wang, W. Chen, Z. Yin et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, 2014.

[64] T.-Y. Chen, J. Wang, H. Liang et al., "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[65] K. A. Patel, J. F. Dynes, I. Choi et al., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, no. 4, article 041010, 2012.

[66] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–72, 2013.

[67] K. A. Patel, J. F. Dynes, M. Lucamarini et al., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, article 051123, 2014.

[68] I. Choi, Y. Zhou, J. F. Dynes et al., "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Optics Express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[69] B. Fröhlich, J. F. Dynes, M. Lucamarini et al., "Quantum secured gigabit optical access networks," *Scientific Reports*, vol. 5, article 18121, 2015.

[70] J. F. Dynes, W. W.-S. Tam, A. Plews et al., "Ultra-high bandwidth quantum secured data transmission," *Scientific Reports*, vol. 6, article 35149, 2016.

[71] L. J. Wang, L. K. Chen, L. Ju et al., "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, article 081108, 2015.

[72] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *Nature Partner Journals (NPJ) Quantum Information*, vol. 3, article 30, 2017.

[73] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-Based QKD," *Optics and Photonics News*, vol. 29, no. 2, pp. 26–33, 2018.

[74] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, pp. 82.1–82.21, 2002.

[75] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, article 045017, 2009.

[76] A. Tomaello, A. Dall'Arche, G. Naletto, and P. Villoresi, "Intersatellite quantum communication feasibility study," in *Quantum Communications and Quantum Imaging IX, 816309*, vol. 8163 of *Proceedings of the SPIE*, San Diego, CA, USA, 2011.

[77] B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," *Optics Letters*, vol. 21, no. 22, pp. 1854–1856, 1996.

[78] W. T. Buttler, R. J. Hughes, P. G. Kwiat et al., "Free-space quantum key distribution," *Physical Review A*, vol. 57, no. 4, pp. 2379–2382, 1998.

[79] W. T. Buttler, R. J. Hughes, P. G. Kwiat et al., "Practical free-space quantum key distribution over 1 km," *Physical Review Letters*, vol. 81, no. 15, pp. 3283–3286, 1998.

[80] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[81] C. Kurtsiefer, P. Zarda, M. Halder et al., "A step towards global key distribution," *Nature*, vol. 419, p. 450, 2002.

[82] T. Schmitt-Manderbach, H. Weier, M. Fürst et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, article 010504, 2007.

[83] S. Nauerth, F. Moll, M. Rau et al., "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, pp. 382–386, 2013.

[84] J. Y. Wang, B. Yang, S. K. Liao et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, pp. 387–393, 2013.

[85] J.-P. Bourgoin, B. L. Higgins, N. Gigov et al., "Free-space quantum key distribution to a moving receiver," *Optics Express*, vol. 23, no. 26, pp. 33437–33447, 2015.

[86] C. J. Pugh, S. Kaiser, J. P. Bourgoin et al., "Airborne demonstration of a quantum key distribution receiver payload," in *2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), paper EB_4_1*, Munich, 2017.

[87] C. J. Pugh, S. Kaiser, J. P. Bourgoin et al., "Airborne demonstration of a quantum key distribution receiver payload," *Quantum Science and Technology*, vol. 2, no. 2, article 024009, 2017.

[88] J. Yin, Y. Cao, S.-B. Liu et al., "Experimental quasi-single-photon transmission from satellite to earth," *Optics Express*, vol. 21, no. 17, pp. 20032–20040, 2013.

[89] J. Pan, "Quantum science satellite," *Chinese Journal of Space Science*, vol. 34, no. 5, pp. 547–549, 2014.

[90] S. K. Liao, W. Q. Cai, W. Y. Liu et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[91] S. Liao, W. Cai, J. Handsteiner et al., "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, no. 3, article 030501, 2018.

[92] T. Scheidl, J. Handsteiner, D. Rauch, and R. Ursin, "Space-to-ground quantum key distribution," in *International Conference on Space Optics (ICSO) 2018*, vol. 11180, Chania, Greece, 2018.

[93] T. Jennewein, J. P. Bourgoin, B. Higgins et al., "QEYSSAT: a mission proposal for a quantum receiver in space," in *Advances in Photonics of Quantum Computing, Memory, and Communication VII*, vol. 8997 of *Proceedings of the SPIE*, San Francisco, CA, USA, February 2014.

[94] E. Meyer-Scott, Z. Yan, A. MacDonald, J. P. Bourgoin, H. Hübel, and T. Jennewein, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," *Physical Review A*, vol. 84, no. 6, article 062326, 2011.

[95] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins et al., "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, vol. 15, article 023006, 2013.

[96] J. P. Bourgoin, N. Gigov, B. L. Higgins et al., "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Physical Review A*, vol. 92, article 052339, 2015.

[97] H. Podmore, I. D'Souza, D. Hudson et al., "Optical terminal for Canada's quantum encryption and science satellite (QEYSSat)," *IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2019.

[98] M. Yang, F. Xu, J.-G. Ren et al., "Spaceborne, low-noise, single-photon detection for satellite-based quantum communications," *Optics Express*, vol. 27, no. 25, pp. 36114–36128, 2019.

[99] G. Vallone, D. Bacco, D. Dequal et al., "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, article 040502, 2015.

[100] D. Dequal, G. Vallone, D. Bacco et al., "Experimental single-photon exchange along a space link of 7000 km," *Physical Review A*, vol. 93, article 010301, 2016.

[101] K. Günthner, I. Khan, D. Elser et al., "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[102] Y. A. Chen, Q. Zhang, T. Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, pp. 214–219, 2021.

[103] T. Jennewein, C. Grant, E. Choi et al., "The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite," in *Emerging Technologies in Security and Defence II; and Quantum-Physics-based Information Security III, 925402*, vol. 9254 of *Proceedings of the SPIE*, Amsterdam, Netherlands, October 2014.

[104] D. K. L. Oi, A. Ling, J. A. Grieve, T. Jennewein, A. N. Dinkelaker, and M. Krutzik, "Nanosatellites for quantum science and technology," *Contemporary Physics*, vol. 58, pp. 25–52, 2016.

[105] R. Bedington, X. Bai, E. Truong-Cao et al., "Nanosatellite experiments to enable future space-based QKD missions," *EPJ Quantum Technology*, vol. 3, article 12, 2016.

[106] D. K. Oi, A. Ling, G. Vallone et al., "CubeSat quantum communications mission," *EPJ Quantum Technology*, vol. 4, article 6, 2017.

[107] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photonics*, vol. 11, no. 8, pp. 502–508, 2017.

[108] K. Boone, J. P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, "Entanglement over global distances via quantum repeaters with satellite links," *Physical Review A*, vol. 91, article 052325, 2015.

[109] Z. Tang, R. Chandrasekara, Y. C. Tan et al., "Generation and analysis of correlated pairs of photons aboard a nanosatellite," *Physical Review Applied*, vol. 5, no. 5, article 054022, 2016.

[110] J. Yin, Y. Cao, Y.-H. Li et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[111] A. Villar, A. Lohrmann, X. Bai et al., "Entanglement demonstration on board a nano-satellite," *Optica*, vol. 7, no. 7, pp. 734–737, 2020.

[112] C.-Z. Peng, T. Yang, X.-H. Bao et al., "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Physical Review Letters*, vol. 94, no. 15, article 150501, 2005.

[113] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach et al., "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[114] X.-M. Jin, J.-G. Ren, B. Yang et al., "Experimental free-space quantum teleportation," *Nature Photonics*, vol. 4, no. 6, pp. 376–381, 2010.

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

[116] Y. Cao, Y. H. Li, K. X. Yang et al., "Long-distance free-space measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 125, article 260503, 2020.