Link loss analysis for a satellite quantum communication down-link

Link loss analysis for a satellite quantum communication down-link

Zhang, Chunmei, Tello, Alfonso, Zanforlin, Ugo, Buller, Gerald, Donaldson, Ross

Chunmei Zhang, Alfonso Tello, Ugo Zanforlin, Gerald S. Buller, Ross J. Donaldson, "Link loss analysis for a satellite quantum communication down-link," Proc. SPIE 11540, Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III, 1154007 (20 September 2020); doi: 10.1117/12.2573489

SPIE.

Event: SPIE Security + Defence, 2020, Online Only

Link loss analysis for a satellite quantum communication down-link

Chunmei Zhang*, Alfonso Tello, Ugo Zanforlin, Gerald S. Buller, Ross J. Donaldson
Scottish Universities Physics Alliance, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, EH14 4AS

ABSTRACT

The analysis of link loss is one of the first and most important steps for the design of an optical communication system. This is particularly vital in quantum communications systems where the information is encoded at the single photon level, and the quantum optical signal cannot be amplified deterministically. In most cases, the desired quantum bit error rate and secure key rate can only be achieved by minimizing the link attenuation and the background noise level in the quantum communication system.

In optical fiber implementations, the transmission distance is inherently limited by the loss per unit distance of the optical fiber, meaning fully global coverage is not readily achievable with the current optical fiber backbone networks. To overcome the terrestrial link limitations for quantum communications, long-distance free-space links, using low-Earth orbit satellites are being proposed and implemented. Due to the optical link length, the main contributors to link losses are geometric loss, atmospheric attenuation, and losses associated with pointing and tracking errors. The total link loss is dominated by the geometric loss, therefore, it is important to analyze its importance in relation to the quantum communications link.

In this paper, the loss of a low-Earth orbit satellite-to-ground (downlink) quantum communication link is analyzed. The analysis includes losses associate with the channel (geometric and atmospheric) and the receiver system. This paper also compares the data of a known satellite quantum communications mission, highlighting trade-offs in investment for satellite platform and optical ground station. Based on the link loss analysis, decoy state BB84 and E91 protocols were chosen to demonstrate the link performance under an example scenario. The work contributes to the design of the optical ground station for a CubeSat mission.

Keywords: quantum communication, satellite quantum key distribution, link analysis, quantum technology, single-photon detection, optical ground station

1. INTRODUCTION

Secure communication protocols are essential for protecting everyday electronic communications, from sending instant messages to financial transactions. As our reliance on electronic communications grows, so do the threats from malicious parties. In particular, there is growing potential threat of a universal quantum computer [1], which could make many of today's commonly used public key communication protocols insecure. In a world where a universal quantum computer, of sufficient size, exists, post-quantum communications and quantum communications seek to provide viable solutions to counter attacks [2,3].

Quantum communications seek to address potential attacks by malicious parties by encoding information onto quantum

*Chunmei.Zhang@hw.ac.uk

Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro-and Nanosystems in Security and Defence III, edited by G. S. Buller et al, Proc. of SPIE Vol. 11540
1154007 · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2573489

bits (qubits) using one (or more) degree of freedom of the information carrier (typically a photon) in two conjugate basis sets [3]. Quantum phenomena, such as quantum superposition and quantum entanglement, are used to construct quantum-equivalent communication protocols for key distribution [4–9], digital signatures [10–14], finger-printing [15,16], oblivious transfer [17], random number generation [18] , and bit-commitment [19]. Quantum key distribution (QKD) is the most mature protocol, having been explored extensively in the laboratory and dark-fiber infrastructure [20–22].

Although quantum phenomena have allowed the construction of secure communication protocols, the underlying quantum properties make it challenging to amplify or repeat a quantum signal in transit without adding noise [18,23–26]. Those challenges have led to satellite-based quantum communications being identified as the most efficient route to a global coverage [27].

Satellite-based quantum communications saw a surge in interest in 2016, when the first quantum capable satellite was launched into orbit [28]. The research area is flourishing, with research teams working on feasibility studies [29–31], verification tests with existing satellites [32–35], technology demonstrations with CubeSats [36,37], and demonstrating satellite-to-ground QKD links using weak-coherent pulses and entangled states [38,39]. As teams move towards satellite demonstrations of capability, accurate modelling of the long free-space link is critical for mission success [40].

Here we present link loss analysis of a low-Earth orbit (LEO) satellite-to-ground (downlink) quantum communication link. The analysis concentrates on the geometric loss and its dependence on different variables, for instance, link distance, divergence angle, operating wavelength, aperture of receiving/transmitting telescopes. We also present analysis for other losses in the link from the atmosphere and system design (telescope obscuration, detector efficiency, and acquisition, pointing and tracking (APT). We compare the link loss model against a known satellite quantum communications mission [39], highlighting trade-offs in investment for satellite platform and optical ground station (OGS). The results from link loss analysis were then used to analyze the link performance for both decoy BB84 and E91 protocols. The work in this paper is being used to justify resources and requirements for the optical ground station of a CubeSat mission.

2. LINK LOSS ANALYSIS

The estimation of optical loss, in the context of secure communication, is considered more important for QKD than for classical communications since quantum signals are much weaker and cannot be easily amplified [37,41,42]. The ideal efficiency of a quantum link can only be achieved by decreasing the channel attenuation and background noise, so that successful QKD links can be established. There are several factors that contribute to channel losses [41-43], including geometric loss, atmospheric loss, loss induced by the structure of the telescopes, detector loss, and APT system. This section discusses each of these contributions to the link budget, outlines a scenario using a CubeSat and estimates the link budget for that scenario. The link budget value will then be used in the next section to estimate the performance of different QKD protocols.

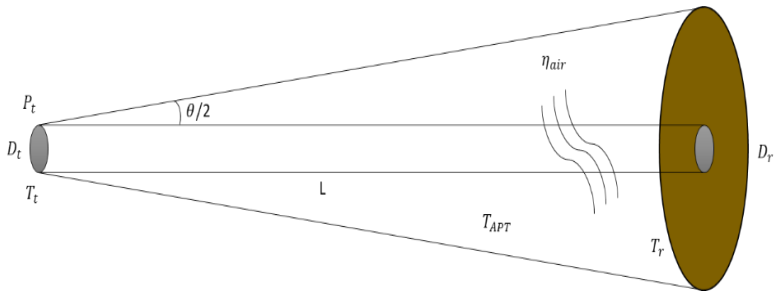

Figure 1. Schematic illustration of the beam spread effect when the light propagates from transmitter main mirror (left) to the receiver main mirror (right). L - link distance; θ – divergence angle of the light beam; η_{air} - the overall transmittance of the Earth's atmosphere; P_t - the power of the light beam at the transmitter main mirror; T_t - the efficiency of transmitting system; D_t - the aperture diameter of transmitter; T_r -the efficiency of the receiving optical system; D_r – the aperture diameter of receiver; T_{APT} - the loss introduced by the APT system.

2.1 Geometric loss

Geometric loss, or diffraction loss, refers to the loss due to the beam spread effect [44] when it propagates from the satellite to the optical ground station. Figure 1 shows an illustration of the beam spread effect when a light beam propagates from

the transmitting telescope main mirror (left) to the receiving telescope main mirror (right). Here, we assume that the laser power before the transmitting telescope main mirror is P_t, the efficiency of the transmitter optics is T_t, the efficiency of the receiver is T_r and T_{APT} represents the loss introduced by the APT system. η_{air} is the atmosphere's transmittance used to describe the overall effect induced by the Earth's atmosphere. The ratio of the power measured at the receiver point to the total power sent from the transmitter can be expressed by

$$\frac{P_r}{P_t} = \frac{{D_r}^2 T_t T_r (1-T_{APT}) \eta_{air}}{(D_t + L\theta)^2} \tag{1}$$

Since the focus is on the geometric loss in this section, other contributions are negated. The transmitting system was designed to work near the diffraction limit. A coefficient m is introduced to describe how close the actual far-field divergence angle of the laser beam is to the theoretically perfect case ($2.44\lambda/D_t$). The geometric loss (in dB) can then be rewritten as:

$$\frac{P_r}{P_t} = 20log \frac{D_r D_t}{{D_t}^2 + 2.44 m L \lambda} \tag{2}$$

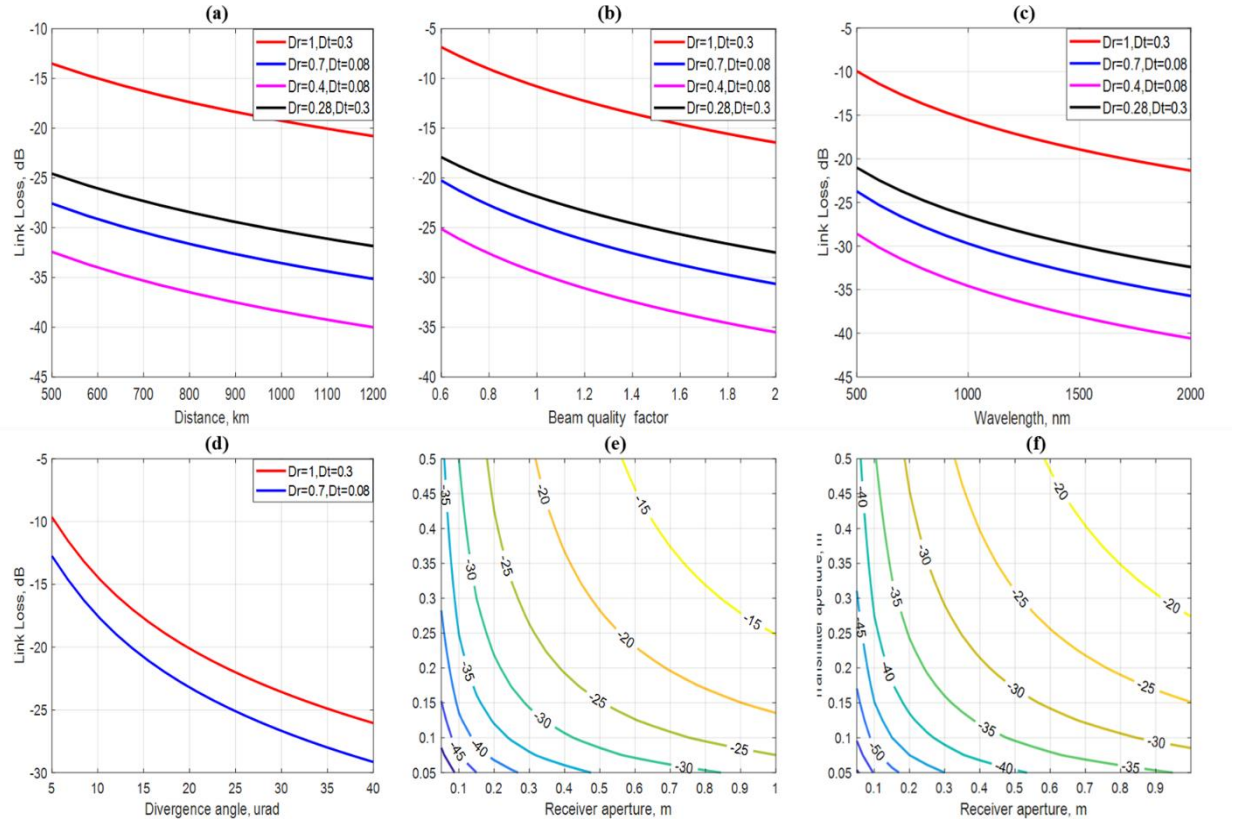

Figure 2. The effect of various parameters on the geometric loss. Here *Dr* represents the aperture diameter of receiver in meters and *Dt* is the aperture diameter of transmitter in meters. a) geometric loss vs link distance; b) geometric loss vs beam quality factor *m*; c) geometric loss vs operating wavelength when link distance equals to 500 km; d) geometric loss vs beam divergence angle; Geometric loss and its dependence on both receiver aperture and transmitter aperture at link distance of e) 500 km and f) 1000 km. In each case the operational wavelength $\lambda = 780\ nm$ except (c). The link distance, *L*, was 500 km except in (a) and (f).

Figure 2 (a)-(c) shows that the geometric losses increase when the link distance, beam quality factor *m*, or operating wavelength increase. Another common effect shown in these three figures is that, the red line case (D_r = 1 m and D_t = 0.3 m) performs best, the pink case (D_r = 0.4 m and D_t = 0.08 m) performs worst, with black and blue line cases lying within these extremes. Figure 2 (a) presents the geometric loss and its dependence on the link distance, ranging from 500 km to 1200 km, for four chosen cases. Within this figure the red line case has the lowest geometric losses of less than

-15 dB at 500 km link distance, and slightly over -20 dB at 1200 km, while the values are about -32 dB at 500 km, and -40 dB at 1200 km for the pink line case. The beam quality factor in Figure 2 (b) was introduced in this work to determine the performance of the transmitting optics if the system was not operated near the diffraction limit. Figure 2 (b) also demonstrates that when the beam quality factor *m* rises, the transmitting optics performs worse and the loss increases for all four cases. Figure 2 (c) highlights that a shorter wavelength can enable a lower loss link, when other parameters of the system are fixed, however there are other known issues that arise when transitioning to shorter wavelengths [29].

The far-field divergence angle of the laser beam from the transmitter plays an important role in a QKD link. To effectively reduce the link loss, the divergence angle of a quantum signal must be as close to the diffraction limit as possible. To achieve this condition, the size of the transmitting telescope needs to be chosen carefully and designed to eliminate aberrations. Figure 2 (d) indicates that the red line case (D_t = 0.3 m) has better performance than that of the blue line case (D_r = 0.08 m), which agrees well with previous theoretical models. The trend is that the geometric loss increases when the far-field divergence angle does too. In Figure 2 (d), only the divergence angle is varied, however both transmitter and receiver telescope diameters were fixed. As a general rule, larger telescope apertures mean smaller far-field divergence angles, however, the volume and weight of the telescope necessarily increases, especially for the transmitter on the satellite, which will induce challenges to the APT requirements. Figure 2 (e) and (f) illustrate the effects of aperture sizes of both transmitter and receiver on the diffraction loss, for link ranges of 500 km and 1000 km, respectively. The values embedded in these two sub-plots are loss numbers expressed in dB units so that it is straightforward to look up loss numbers for specific settings of telescope sizes. The results show that increasing the diameter of both transmitter and receiver provides the most benefit.

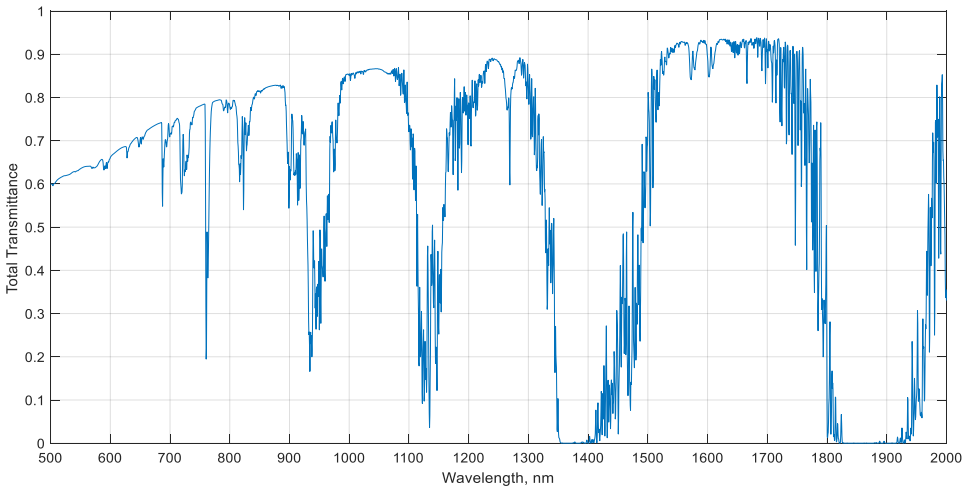

Figure 3. Atmospheric transmittance over 500-2000 nm spectral range for a 500 km vertical path on a cloudless, rainless summer day in rural area (visibility range 23 km).

2.2 Atmospheric loss

When light propagates through the Earth's atmosphere, absorption, scattering and turbulence are three main effects that need to be considered [45]. Low loss atmospheric windows occur for wavelengths, such as 650 nm, 850 nm or 1550 nm, which are typically used for free-space optical communications. If a low loss window is chosen for operation, then absorption can be greatly reduced (see Figure 3). The total attenuation coefficient of the atmosphere is made up of absorption and scattering coefficients of the molecules and particles, respectively. In the visible and short-wave infrared range, the atmospheric loss is predominantly caused by the absorption from water vapor and scattering from various particles, such as dust, haze, aerosols.

MODTRAN [46], a computer program designed to model the propagation of electromagnetic waves through the Earth's atmosphere, was used to estimate the atmospheric total transmittance coefficient in this work. During the modelling and analysis, we assumed that the observer is located on a satellite orbiting at an altitude of 500 km, and the target is located on the ground. The spectral range used in the analysis is between 500 nm to 2000 nm. Our analysis shows that the atmospheric transmission is strongly influenced by both the aerosol and the visibility range (Figure 4), weather conditions

especially rain (Figure 5) and path lengths (Figure 6) for fixed orbiting altitudes. The term visibility [47], or surface meteorological range, refers to the distance at which the contrast of a given object with respect to its background equals the contrast threshold. Visibility is usually measured with 550 nm wavelength collimated light beam, measuring the distance when it is attenuated to a specific fraction (5% or 2%) of its original power.

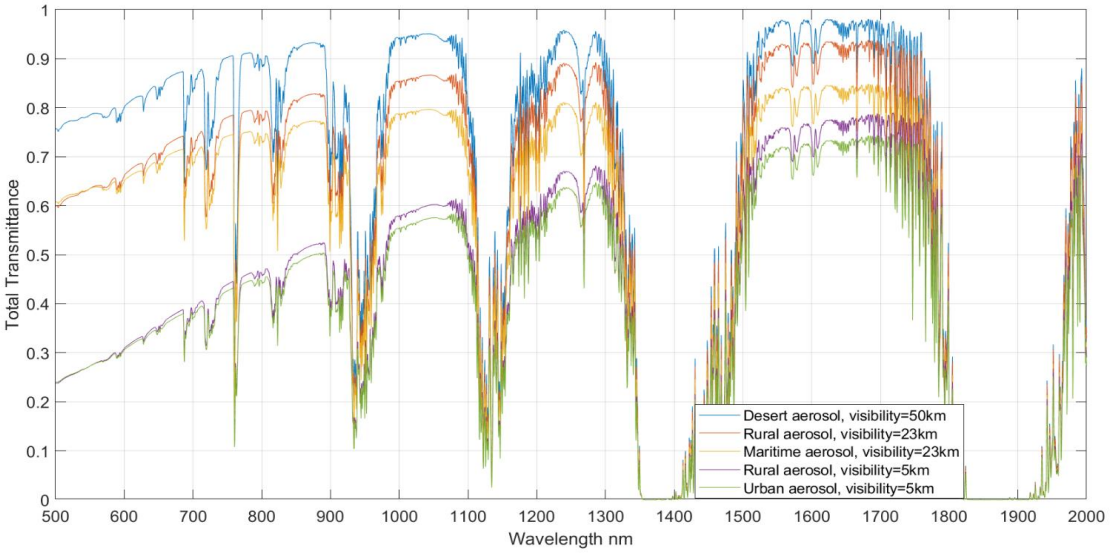

Figure 4. Atmospheric transmission for a 500 km vertical path for various aerosol and visibility conditions. The desert aerosol with 50 km visibility has highest transmittance, followed by two aerosols both with 23 km visibility, and two aerosols both with 5 km visibility. Rural locations have higher transmittance than urban and maritime aerosols when the visibility is the same, such as 23 km and 5 km.

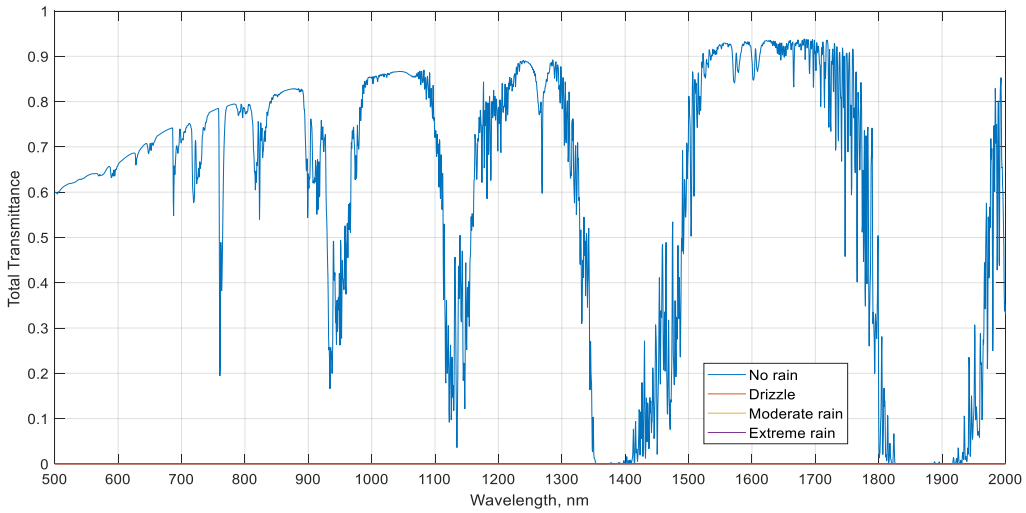

Figure 5. Various rain conditions and their effects on the atmospheric transmittance. The rural aerosol with 23 km visibility range is chosen here as default for all four cases. Transmittance for drizzle (red), moderate (yellow) or extreme rain (purple) drops close to zero, different from the no-rain condition (blue). From this figure, we see that operating optical communications between 500 nm and 2000 nm is only feasible when there is no rain, an important note for commercial service.

2.3 Other losses

In addition to geometric and atmospheric loss, other losses in a QKD communication system originate from the telescope structure, single-photon detector (SPD) detection efficiencies, and the APT components.

The Cassegrain telescope is widely used in radar and communication systems [48]. Although its aperture size can be made relatively large, and optimized to eliminate chromatic, spherical, and other aberrations, it frequently has a central obstruction that partially blocks the incoming laser light, introducing additional losses. Here, we consider a Cassegrain reflector that is described by the obstruction ratio, which is defined as the ratio of the diameter of secondary mirror to that of the primary mirror. The fundamental Gaussian mode is used for the calculation. Cassegrain telescopes typically have an obscuration ratio of 0.4, corresponding to a loss of approximately -1.6 dB.

SPDs are a critical technology for QKD [49] systems. When it comes to the link loss, one of the most important parameters of the single-photon detectors is their detection efficiency. For the purposes of this paper, we model free-space coupled silicon single-photon avalanche diodes (SPAD), which typically have a detection efficiency of approximately 60% at a wavelength of 780 nm, the chosen operational wavelength used in this modelling, which is equivalent to an induced loss of -2.21 dB.

The divergence angle needs to be small in a long-distance QKD free-space link so that the loss can be minimized as highlighted in Figure 2 (d). However, a narrow divergence angle requires the implementation of a high-precision APT system, typically with μrad resolution. Although APT technology has been verified in free-space laser communications [50,51], it could still be improved to reduce the loss contribution for QKD applications. When the APT components of QKD are designed, one must consider and compensate for the pointing ahead requirement due to the fast movement of the satellite and the installation offset of the ground beacon laser [52]. The loss in the APT system for satellite-to-ground QKD link originates from two sources. The first one is the random altitude jitter due to micro-vibrations and thermal effects within the micro-satellite, which induces discrepancies between the pointing position and the actual position of the target. The second contribution is caused by the random pointing jitter of the tracking optical axes [51-53]. The pointing probability density is believed to follow the Rician function [54], and the APT loss can be calculated for a Gaussian profile laser beam.

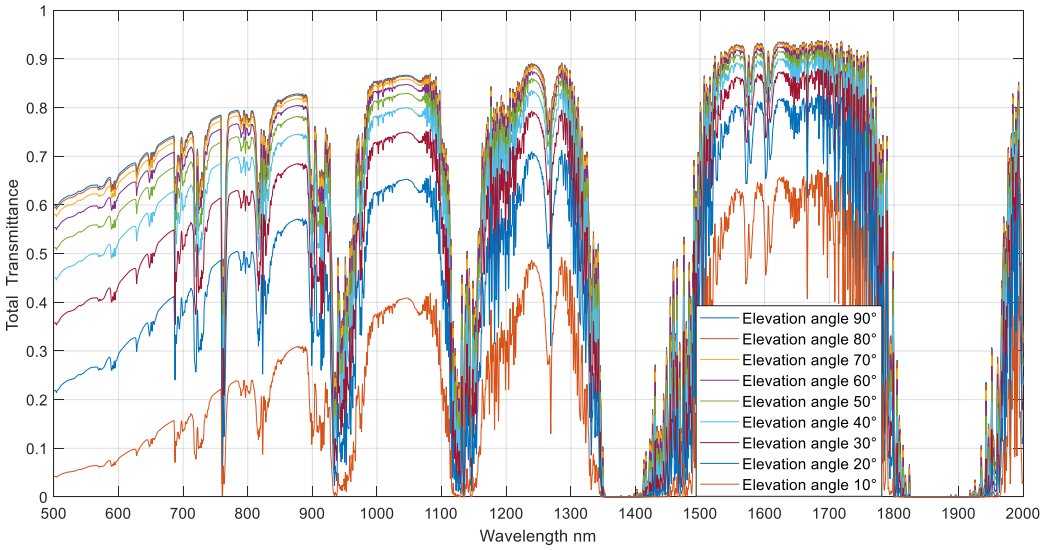

Figure 6. Slant path atmospheric transmittance for elevation angle range from 10 to 90 degree. The elevation angle is with respect to the horizontal plane. Other parameters used here are rural aerosol with 23 km visibility, no clouds, sub-arctic summer climate and 500 km altitude. Results indicate that a longer transmission path through the atmosphere will lead to higher losses.

To give an example of performance for the CubeSat mission, we define the following losses from this section: geometric loss of about -27dB for a 500 km vertical QKD link if the aperture diameters of transmitter and receiver are 8 cm (CubeSat) and 70 cm, respectively (Figure 2). With cloudless and rainless weather conditions, the atmospheric loss is approximately -1 dB in rural areas (visibility range of 23 km) for 500 km vertical QKD link. The Cassegrain structure loss is

approximately -1.6 dB for 40 % central obstruction ratio. The loss introduced by the single-photon detector is about -2.21 dB for a detecting efficiency of 60% at the wavelength of 780 nm. If the APT system has an efficiency of 50%, it induces a -3 dB loss. Therefore, the total loss for this scenario, disregarding the receiver system loss and turbulence, is approximately -35 dB. This loss value will be used in the next section to estimate the highest secure key rate that could be achieved using a QKD payload when the CubeSat flies directly over the OGS.

3. LINK PERFORMANCE

Given the losses of the channel, two protocols have been studied under different conditions, decoy BB84 [55] and E91 [56] in order to estimate their performance in a free-space scenario. Both are polarization-based implementations.

Decoy BB84 is a version of the original BB84 protocol where different intensity levels are applied to the pulses, so a better estimation of the quantum bit error rate (QBER) and a more efficient privacy amplification procedure can be performed. Historically, this protocol allowed an extension of the maximum achievable transmission distance of QKD to hundreds of kilometers [57]. Today, it is the most widely used protocol and many others have incorporated the idea of using decoy states [58,59].

To estimate the secret key rate (SKR) and the QBER of the protocol, the model is based on the equations derived from the notorious GLLP work [60,61]

$$R \geq R_{sifted} \cdot \{-Q_\mu \cdot f \cdot h(QBER_{BB84}) + Q_1[1 - h(e_1)]\} \tag{3}$$

where R_{sifted} is the number of detections at the receiver after applying the basis reconciliation, Q_μ is the quantum signal gain, $QBER_{BB84}$ is the total error of the communication, $h(\cdot)$ is the binary entropy function, Q_1 is the gain from the 1-photon pulses and e_1 is their associated error.

Making use of the decoy states, an estimation of Q_1 and e_1 can be done using the following linear system for each of the decoy states,

$$Q_s = \sum_{n=0}^{\infty} P_\mu(n) Y_n \tag{4}$$

$$E_s Q_s = \sum_{n=0}^{\infty} P_\mu(n) e_n Y_n \tag{5}$$

where $P_\mu(n) = \mu^n e^{-\mu}/n!$ is the probability of having *n* photons in a pulse and follows the Poisson distribution, Y_n is the conditional probability that a signal will be detected by Bob, Q_s and E_s are the gain and error observed in each signal, e_n is the error of the pulses with *n* photons and μ is the mean photon number.

Finally,

$$Q_1 = Y_1 \mu e^{-\mu} \tag{6}$$

Different from BB84, the E91 protocol exploits the unique property of entanglement as unit of information where specific photon detection correlations provide knowledge of the measured quantum state via Bell state measurements [62–64]. The original protocol envisioned the use of quantum particles where entanglement was achieved via discrete spin correlations[56], however, since then entanglement was also shown to be a property of specific photonic systems exploiting spontaneous parametric down conversion (SPDC) generation and manipulation of photon pairs [65–67]. Over the past few decades, several works have demonstrated the versatility of entangled photon generation and its use in the context of secure quantum communications, however, most of these works still rely on a fiber-based optical infrastructure [68–70]. Recently, attention has been directed to satellite-based optical system to take advantage of limited loss for selected operational wavelengths, longer transmission distances and scalability of free-space setups [36,71].

In the context of satellite quantum communications, the architecture envisioned for the E91 protocol assumes that a LEO satellite functions as a state generation station, with the source of the entangled photon pairs, as well as an onboard receiver unit where partial state measurement is already performed. The remaining partial state is then sent via a downlink channel to a ground station where entanglement swapping is performed and total state reconstruction/key generation is achieved. It is important to stress that the present model assumes that the entanglement generating source produces correlated photon pairs via SPDC deterministically with unity efficiency within an operational period *T*. This might be considered a strong assumption especially since realistic sources are intrinsically probabilistic [72–74], however, this can be easily accounted for in the theoretical estimations simply by rescaling the overall generation rate by a multiplicative factor. As for the BB84 protocol, the E91 is fully characterized by the SKR and QBER which define the rates of final key generation and

experimental error of sifted bits respectively. Based on the model of [75], it is possible to define the SKR, R, of E91 as follows:

$$R = \frac{1}{2} P_{succ} h(QBER_{E91}) \frac{1}{T} \tag{7}$$

where P_{succ} is the probability of successfully creating a link between the satellite and ground station, $h(\cdot)$ is the binary entropy function, $QBER_{E91}$ is the QBER of the protocol, T is the operational period of the entanglement source and the ½ factor reflects the measurement basis selection similarly to the BB84 protocol. The $QBER_{BB84}$ and $QBER_{E91}$, can be expressed as the sum of several independent contributions:

$$QBER_{BB84} = QBER_{dark} + QBER_{background} + QBER_{coding} \tag{8}$$

$$QBER_{E91} = QBER_{dark} + QBER_{background} \tag{9}$$

where $QBER_{dark}$ is the expected experimental bit error rate which is strictly dependent on the dark count rates of the detection stages of both the satellite and ground station, $QBER_{background}$ is the contribution of the background noise, and $QBER_{coding}$ is the expected error due to imperfections when generating polarized photons.

To run the simulation realistic parameters were considered for the decoy BB84 protocol: an operational frequency of 500 MHz; detection efficiency of 1 to be consistent with the losses model; a dark count rate of 400 counts per second (100 counts/s per detector); a background rate of 350 counts per second; a $QBER_{coding}$ of 0.01; mean photon numbers of 0.85, 0.1, and 0 for the quantum signal and two decoy states respectively; a gate width of 500 ps. Similarly, the E91 protocol was simulated using the same experimental parameters of the BB84 protocol, except for the operational frequency, which was reduced to 1 MHz. This choice was made to reflect realistic values of experimental SPDC sources currently available[72–74]. An estimation of the SKR and QBER for both protocols can be seen in Figure 7, where the dotted red line has been plotted at a -35 dB corresponding to the maximum link loss estimated from the previous section. The decoy BB84 is expected to operate at approximately 4 kbps rate while E91 at a 0.02 bps rate. Both protocols had QBERs less than 0.01.

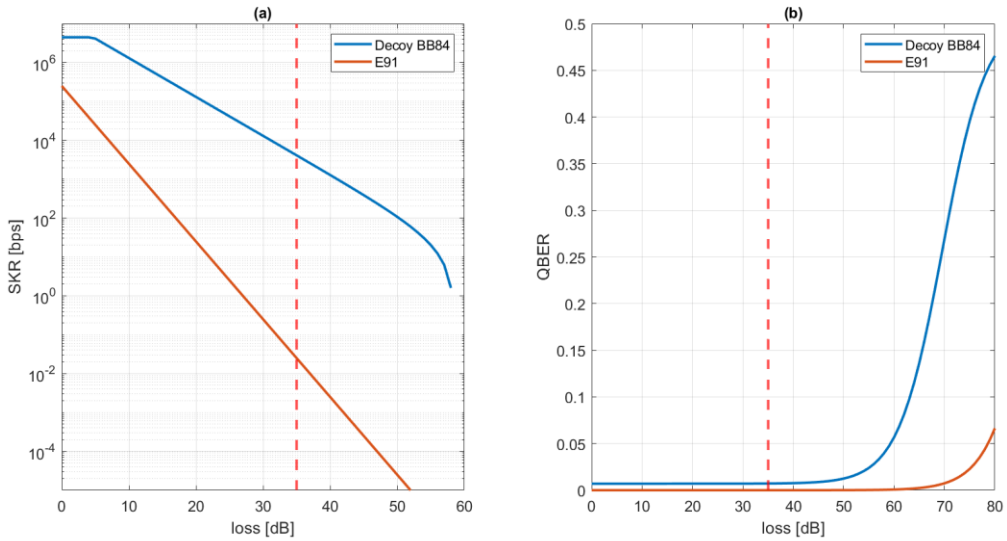

Figure 7. SKR performance and QBER estimation of the decoy BB84 and E91 protocols. The dotted red line indicates the -35 dB loss that it is expected for the example commented above. In a real scenario it is expected that decoy BB84 always has a greater SKR than an entanglement protocol due to the difference in operational frequency capabilities. Some important parameters used in the simulation were: operational frequency of 500 MHz for decoy BB84 and 1 MHz for E91, unitary detection efficiency, dark count rate of 400 counts per second, and background rate of 350 counts per second, and a gate width of 500 ps.

4. CONCLUSION

Significant contributions to the loss budget of a satellite-to-ground QKD link (downlink) were discussed. The most significant contribution was found to be the geometric loss, primarily due to the long link length. Variables that contribute to the geometric loss were discussed in this paper, such as wavelength, telescope aperture sizes, and divergence angle. We find that the geometric loss is mainly determined by the aperture size of the telescopes if the altitude of the satellite and the operating wavelength are fixed. Atmospheric loss and its dependence on the aerosol, visibility and rain conditions were discussed. We highlighted that visibility had the largest impact on atmospheric loss. Another key finding is that atmospheric loss is heavily influenced by location and weather conditions. From the sources of losses discussed, we estimated a loss budget of -35 dB for a QKD downlink with a CubeSat (altitude 500 km, telescope aperture 8 cm, operation wavelength 780 nm) and 70 cm receiver aperture OGS.

We outlined a basic model to estimate SKR rate and QBER for decoy BB84 and E91 QKD protocols. For the calculated loss budget of -35 dB we estimated SKRs 4 kbps for a decoy BB84 protocol operating at a frequency of 500 MHz and 0.02 bps for the E91 protocol with a correlated pair generation rate of 1 MHz.

The analysis of link loss budget and link performance will be used to justify the design and location of the OGS for a CubeSat mission.

5. ACKNOWLEDGMENTS

This research was funded by; the UK Engineering and Physical Sciences Research Council (EPSRC) through projects EP/K015338/1, EP/T001011/1, EP/S026428/1 and EP/N003446/1; and the Royal Academy of Engineering through an Early Career Research Fellowship No. RF\201718\1746.

REFERENCES

[1] Pirandola, S. and Braunstein, S. L., "Physics: Unite to build a quantum Internet," Nature **532**(7598), 169–171 (2016).
[2] Bernstein, D. J., [Introduction to post-quantum cryptography], Springer Berlin Heidelberg (1998).
[3] Tittel, W., Zbinden, H. and Gisin, N., "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
[4] Stucki, D., Fasel, S., Gisin, N., Thoma, Y. and Zbinden, H., "Coherent one-way quantum key distribution," Proc. SPIE **6583**, 65830L-65830L – 4 (2007).
[5] Sibson, P., Erven, C., Godfrey, M., Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M., Terai, H., Tanner, M. G., Natarajan, C. M., Hadfield, R. H., O'Brien, J. L. and Thompson, M. G., "Chip-based quantum key distribution," 1–5 (2015).
[6] Guan, J.-Y., Cao, Z., Liu, Y., Shen-Tu, G.-L., Pelc, J. S., Fejer, M. M., Peng, C.-Z., Ma, X., Zhang, Q. and Pan, J.-W., "Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution," Phys. Rev. Lett. **114**(18), 1–5 (2015).
[7] Ali, S. and Wahiddin, M. R. B., "Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols," Eur. Phys. J. D **60**(2), 405–410 (2010).
[8] Tamaki, K., Koashi, M. and Imoto, N., "Security of the Bennett 1992 quantum-key distribution against individual attack over a realistic channel," Phys. Rev. A, 16 (2002).
[9] Bennett, C. H. and Brassard, G., "Quantum Cryprography: Public Key distribution and coin tossing," Int. Conf. Comput. Syst. Signal Process. (1984).
[10] Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J. and Buller, G. S., "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.," Nat. Commun. **3**, 1174 (2012).
[11] Collins, R. J., Donaldson, R. J., Dunjko, V., Wallden, P., Clarke, P. J., Andersson, E., Jeffers, J. and Buller, G. S., "Realization of quantum digital signatures without the requirement of quantum memory," Phys. Rev. Lett. (2014).
[12] Donaldson, R. J., Collins, R. J., Kleczkowska, K., Amiri, R., Wallden, P., Dunjko, V., Jeffers, J., Andersson, E. and Buller, G. S., "Experimental demonstration of kilometer-range quantum digital signatures," Phys. Rev. A **93**(1), 012329 (2016).
[13] Collins, R. J., Amiri, R., Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., Takeoka, M., Andersson, E., Buller, G. S. and Sasaki, M., "Experimental transmission of quantum digital signatures over 90-km of installed optical

fiber using a differential phase shift quantum key distribution system," Opt. Lett. **41**(21), 4883–4886 (2016).
[14] Collins, R. J., Amiri, R., Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., Takeoka, M., Sasaki, M., Andersson, E. and Buller, G. S., "Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution," Sci. Rep. **7**(1), 3235 (2017).
[15] Xu, F., Arrazola, J. M., Wei, K., Wang, W., Palacios-Avila, P., Feng, C., Sajeed, S., Lutkenhaus, N. and Lo, H.-K., "Experimental quantum fingerprinting with weak coherent pulses," Nat Commun **6** (2015).
[16] Arrazola, J. M. and Lütkenhaus, N., "Quantum fingerprinting with coherent states and a constant mean number of photons," Phys. Rev. A **89**(6), 062305 (2014).
[17] Amiri, R., Stárek, R., Mičuda, M., Mišta, L., Dušek, M., Wallden, P. and Andersson, E., "Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation," 1–20 (2020).
[18] Donaldson, R. J., Mazzarella, L., Zanforlin, U., Collins, R. J., Jeffers, J. and Buller, G. S., "Quantum state correction using a measurement-based feedforward mechanism," Phys. Rev. A **100**(2), 023840 (2019).
[19] Liu, Y., Cao, Y., Curty, M., Liao, S.-K., Wang, J., Cui, K., Li, Y.-H., Lin, Z.-H., Sun, Q.-C., Li, D.-D., Zhang, H.-F., Zhao, Y., Chen, T.-Y., Peng, C.-Z., Zhang, Q., Cabello, A. and Pan, J.-W., "Experimental Unconditionally Secure Bit Commitment," Phys. Rev. Lett. **112**(1), 010504 (2014).
[20] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P., "Advances in Quantum Cryptography," 1–118 (2019).
[21] Sasaki, M., "Quantum networks: where should we be heading?," Quantum Sci. Technol. **2**(2), 020501 (2017).
[22] Dynes, J. F., Wonfor, A., Tam, W. W.-S., Sharpe, A. W., Takahashi, R., Lucamarini, M., Plews, A., Yuan, Z. L., Dixon, A. R., Cho, J., Tanizawa, Y., Elbers, J.-P., Greißer, H., White, I. H., Penty, R. V. and Shields, A. J., "Cambridge quantum network," npj Quantum Inf. **5**(1), 101 (2019).
[23] Bäuml, S., Christandl, M., Horodecki, K. and Winter, A., "Limitations on Quantum Key Repeaters," 41 (2014).
[24] Specht, H. P., Nölleke, C., Reiserer, A., Uphoff, M., Figueroa, E., Ritter, S. and Rempe, G., "A single-atom quantum memory.," Nature **473**(7346), 190–193 (2011).
[25] Donaldson, R. J., Mazzarella, L., Collins, R. J., Jeffers, J. and Buller, G. S., "A high-gain and high-fidelity coherent state comparison amplifier," Commun. Phys. **1**(1), 54 (2018).
[26] Canning, D. W., Donaldson, R. J., Mukherjee, S., Collins, R. J., Mazzarella, L., Zanforlin, U., Jeffers, J., Thomson, R. R. and Buller, G. S., "On-chip implementation of the probabilistic quantum optical state comparison amplifier," Opt. Express **27**(22), 31713 (2019).
[27] Bourgoin, J.-P., Meyer-Scott, E., Higgins, B. L., Helou, B., Erven, C., Hübel, H., Kumar, B., Hudson, D., D'Souza, I., Girard, R., Laflamme, R. and Jennewein, T., "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," New J. Phys. **15**(2), 023006 (2013).
[28] BBC., "China launches quantum-enabled satellite Micius" (2016).
[29] Miao, E. L., Han, Z. F., Gong, S. S., Zhang, T., Diao, D. S. and Guo, G. C., "Background noise of satellite-to-ground quantum key distribution," New J. Phys. **7** (2005).
[30] Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G. and Villoresi, P., "Feasibility of satellite quantum key distribution," New J. Phys. **11**(4), 045017 (2009).
[31] Anisimova, E., Higgins, B. L., Bourgoin, J.-P., Cranmer, M., Choi, E., Hudson, D., Piche, L. P., Scott, A., Makarov, V. and Jennewein, T., "Mitigating radiation damage of single photon detectors for space applications," EPJ Quantum Technol. **4**(1), 10 (2017).
[32] Takenaka, H., Carrasco-Casado, A., Fujiwara, M., Kitamura, M., Sasaki, M. and Toyoshima, M., "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," Nat. Photonics **11**(8), 502–508 (2017).
[33] Vallone, G., Dequal, D., Tomasin, M., Vedovato, F., Schiavon, M., Luceri, V., Bianco, G. and Villoresi, P., "Interference at the Single Photon Level Along Satellite-Ground Channels," Phys. Rev. Lett. **116**(25), 1–6 (2016).
[34] Calderaro, L., Agnesi, C., Dequal, D., Vedovato, F., Schiavon, M., Santamato, A., Luceri, V., Bianco, G., Vallone, G. and Villoresi, P., "Towards Quantum Communication from Global Navigation Satellite System" (2018).
[35] Vallone, G., Marangon, D. G., Canale, M., Savorgnan, I., Bacco, D., Barbieri, M., Calimani, S., Barbieri, C., Laurenti, N. and Villoresi, P., "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," Phys. Rev. A **91**(4), 042320 (2015).
[36] Villar, A., Lohrmann, A., Bai, X., Vergoossen, T., Bedington, R., Perumangatt, C., Lim, H. Y., Islam, T., Reezwana, A., Tang, Z., Chandrasekara, R., Sachidananda, S., Durak, K., Wildfeuer, C. F., Griffin, D., Oi, D. K. L. and Ling, A., "Entanglement demonstration on board a nano-satellite," Optica **7**(7), 734 (2020).

[37] Kerstel, E., Gardelein, A., Barthelemy, M., Fink, M., Joshi, S. K. and Ursin, R., "Nanobob: A CubeSat mission concept for quantum communication experiments in an uplink configuration," EPJ Quantum Technol. **5**(1), 1–34 (2018).
[38] 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., Li, G.-B., Lu, Q.-M., Gong, Y.-H., Xu, Y., Li, S.-L., Li, F.-Z., Yin, Y.-Y., Jiang, Z.-Q., Li, M., et al., "Satellite-based entanglement distribution over 1200 kilometers," Science (80-.). **356**(6343), 1140–1144 (2017).
[39] 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., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., et al., "Satellite-to-ground quantum key distribution," Nature **549**(7670), 43–47 (2017).
[40] Bedington, R., Mantilla, J. M. A. and Ling, A., "Progress in satellite quantum key distribution" (2017).
[41] Tomaello, A., Bonato, C., Da Deppo, V., Naletto, G. and Villoresi, P., "Link budget and background noise for satellite quantum key distribution," Adv. Sp. Res. (2011).
[42] Pfennigbauer, M., Aspelmeyer, M., Leeb, W. R., Baister, G., Dreischer, T., Jennewein, T., Neckamm, G., Perdigues, J. M., Weinfurter, H. and Zeilinger, A., "Satellite-based quantum communication terminal employing state-of-the-art technology," J. Opt. Netw. (2005).
[43] Stotts, L. B., Kolodzy, P., Pike, A., Graves, B., Dougherty, D. and Douglass, J., "Free-space optical communications link budget estimation," Appl. Opt. (2010).
[44] Steen, W. ., "Principles of Optics M. Born and E. Wolf, 7th (expanded) edition, Cambridge University Press, Cambridge, 1999, 952pp. 37.50/US $59.95, ISBN 0-521-64222-1," Opt. Laser Technol. (2000).
[45] Andrews, L. C. and Phillips, R. L., [Laser beam propagation through random media: Second edition] (2005).
[46] Berk, A., Conforti, P., Kennett, R., Perkins, T., Hawes, F. and van den Bosch, J., "MODTRAN6: a major upgrade of the MODTRAN radiative transfer code," Algorithms Technol. Multispectral, Hyperspectral, Ultraspectral Imag. XX (2014).
[47] Singh, A., Bloss, W. J. and Pope, F. D., "60 years of UK visibility measurements: Impact of meteorology and atmospheric pollutants on visibility," Atmos. Chem. Phys. (2017).
[48] Malik, A. and Singh, P., "Free Space Optics: Current Applications and Future Challenges," Int. J. Opt. (2015).
[49] Buller, G. S. and Collins, R. J., "Single-photon generation and detection," Meas. Sci. Technol. (2010).
[50] Tolker-Nielsen, T. and Oppenhauser, G., "In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX," Free. Laser Commun. Technol. XIV (2002).
[51] Takayama, Y., Jono, T., Toyoshima, M., Kunimori, H., Giggenbach, D., Perlot, N., Knapek, M., Shiratama, K., Abe, J. and Arai, K., "Tracking and pointing characteristics of OICETS optical terminal in communication demonstrations with ground stations," Free. Laser Commun. Technol. XIX Atmos. Propag. Electromagn. Waves (2007).
[52] Zhang, L., Dai, J., Li, C., Wu, J., Jia, J. and Wang, J., "Design and in-orbit test of a high accuracy pointing method in satellite-to-ground quantum communication," Opt. Express (2020).
[53] Han, X., Yong, H.-L., Xu, P., Wang, W.-Y., Yang, K.-X., Xue, H.-J., Cai, W.-Q., Ren, J.-G., Peng, C.-Z. and Pan, J.-W., "Point-ahead demonstration of a transmitting antenna for satellite quantum communication," Opt. Express (2018).
[54] Toyoshima, M. and Araki, K., "Far-field pattern measurement of an onboard laser transmitter by use of a space-to-ground optical link," Appl. Opt. (1998).
[55] Hwang, W. Y., "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**(5), 057901 (2003).
[56] Ekert, A. K., "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**(6), 661–663 (1991).
[57] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A. and Weinfurter, H., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. (2007).
[58] Stucki, D., Brunner, N., Gisin, N., Scarani, V. and Zbinden, H., "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87**(19), 1–3 (2005).
[59] Lo, H. K., Curty, M. and Qi, B., "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**(13), 130503 (2012).
[60] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. and Pan, J.-W., "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**(2), 025002 (2020).
[61] Gottesman, D., Hoi-Kwonglo, L. O., Lütkenhaus, N. and Preskill, J., "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. (2004).

[62] Kim, Y. H., Kulik, S. P. and Shih, Y., "Quantum teleportation of a polarization state with a complete bell state measurement," Phys. Rev. Lett. **86**(7), 1370–1373 (2001).
[63] Liang, W. Y., Li, M., Yin, Z. Q., Chen, W., Wang, S., An, X. B., Guo, G. C. and Han, Z. F., "Simple implementation of quantum key distribution based on single-photon Bell-state measurement," Phys. Rev. A - At. Mol. Opt. Phys. **92**(1), 012319 (2015).
[64] Lu, H., Lin, J. and Chen, L., "Entangled squeezed states: Bell state measurement and teleportation," Chinese Opt. Lett. Vol. 2, Issue 10, pp. 618-620 **2**(10), 618–620 (2004).
[65] Hong, C. K., Ou, Z. Y. and Mandel, L., "Measurement of subpicosecond time intervals between two photons by interference," Phys. Rev. Lett. **59**(18), 2044–2046 (1987).
[66] Kaltenbaek, R., Blauensteiner, B., Zukowski, M., Aspelmeyer, M. and Zeilinger, A., "Experimental interference of independent photons," Phys. Rev. Lett. **96**(24), 240502 (2006).
[67] Keller, T. E. and Rubin, M. H., "Theory of two-photon entanglement for spontaneous parametric down-conversion driven by a narrow pump pulse," Phys. Rev. A - At. Mol. Opt. Phys. **56**(2), 1534–1541 (1997).
[68] Honjo, T., Nam, S. W., Takesue, H., Zhang, Q., Kamada, H., Nishida, Y., Tadanaga, O., Asobe, M., Baek, B., Hadfield, R., Miki, S., Fujiwara, M., Sasaki, M., Wang, Z., Inoue, K. and Yamamoto, Y., "Long-distance entanglement-based quantum key distribution over optical fiber," Opt. Express **16**(23), 19118 (2008).
[69] Fasel, S., Gisin, N., Ribordy, G. and Zbinden, H., "Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: A comparison of two chromatic dispersion reduction methods," Eur. Phys. J. D **30**(1), 143–148 (2004).
[70] Wengerowsky, S., Joshi, S. K., Steinlechner, F., Zichi, J. R., Dobrovolskiy, S. M., van der Molen, R., Los, J. W. N., Zwiller, V., Versteegh, M. A. M., Mura, A., Calonico, D., Inguscio, M., Hübel, H., Bo, L., Scheidl, T., Zeilinger, A., Xuereb, A. and Ursin, R., "Entanglement distribution over a 96-km-long submarine optical fiber," Proc. Natl. Acad. Sci. U. S. A. **116**(14), 6684–6688 (2019).
[71] Yin, J., Li, Y. H., Liao, S. K., Yang, M., Cao, Y., Zhang, L., Ren, J. G., Cai, W. Q., Liu, W. Y., Li, S. L., Shu, R., Huang, Y. M., Deng, L., Li, L., Zhang, Q., Liu, N. Le, Chen, Y. A., Lu, C. Y., Wang, X. Bin, et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature (2020).
[72] Magnitskiy, S., Frolovtsev, D., Firsov, V., Gostev, P., Protsenko, I. and Saygin, M., "A SPDC-Based Source of Entangled Photons and its Characterization," J. Russ. Laser Res. **36**(6), 618–629 (2015).
[73] Kaneda, F., Garay-Palmett, K., U'Ren, A. B. and Kwiat, P. G., "Heralded single-photon source utilizing highly nondegenerate, spectrally factorable spontaneous parametric downconversion," Opt. Express **24**(10), 10733 (2016).
[74] Kaneda, F., Christensen, B. G., Wong, J. J., Park, H. S., McCusker, K. T. and Kwiat, P. G., "Time-multiplexed heralded single-photon source," Optica **2**(12), 1010 (2015).
[75] Guha, S., Krovi, H., Fuchs, C. A., Dutton, Z., Slater, J. A., Simon, C. and Tittel, W., "Rate-loss analysis of an efficient quantum repeater architecture," Phys. Rev. A - At. Mol. Opt. Phys. **92**(2), 022357 (2015).