Prospects of time-bin quantum key distribution in turbulent free-space channels

Prospects of time-bin quantum key distribution in turbulent free-space channels

Tello Castillo, Alfonso, Novo, Catarina, Donaldson, Ross

Alfonso Tello Castillo, Catarina Novo, Ross Donaldson, "Prospects of time-bin quantum key distribution in turbulent free-space channels," 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, 1154006 (20 September 2020); doi: 10.1117/12.2573479

Event: SPIE Security + Defence, 2020, Online Only

Prospects of time-bin quantum key distribution in turbulent free-space channels.

Alfonso Tello Castillo[1], Catarina Novo[1], Ross Donaldson[1]

Scottish Universities Physics Alliance, Institute of Photonics & Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, David Brewster Building, Edinburgh EH14 4AS, Scotland, UK

ABSTRACT

Quantum key distribution is a quantum communication protocol which seeks to address potential vulnerabilities in data transmission and storage. One of the main challenges in the field is achieving high rates of secret key in lossy and turbulent free-space channels. In this scenario, most experimental demonstrations have used the polarization of photons as their qubit carriers, due to the relative robustness of polarization in free-space propagation. Time-bin or phase-based protocols are considered less practical due to the wave-front distortion caused by atmospheric turbulence. However, demonstrations of novel free-space interferometer designs are enabling interferometers to measure multimodal signals with high visibility. That means it is now viable to consider the prospects of implementing time-bin or phase-based protocols, which have demonstrated high key rates and long transmission distances in optical fiber. In this work, we present the possibilities of implementing time-bin protocols in turbulent free-space channels, using the coherent one-way protocol as the example. We present an analysis of the secret key rate and quantum bit error rate of the system, providing the errors due to noise counts, and the extinction ratio of the pulses. Finally, we developed a model to quantify the expected losses for a turbulence free-space channel, specifically for a free-space satellite-to-ground station channel.

Keywords: quantum communication, free-space quantum key distribution, time-bin QKD, quantum technology, single-photon detection, atmospheric turbulence.

1. INTRODUCTION

Quantum key distribution (QKD) is a key sharing protocol that relies on quantum phenomena, such as quantum superposition and quantum entanglement, to address potential vulnerabilities in data transmission and data storage[1,2]. QKD is part of a broader research area, termed quantum communications (QC), which seeks to address other communication vulnerabilities using quantum phenomena[3–5]. Quantum digital signatures is an example of another QC protocol, which seeks to provide digital signatures which cannot be forged or repudiated[6–10], arguably as important as key sharing.

Demonstrations of QKD protocols using optical fiber have been performed in the laboratory and over established dark fiber networks at transmission distances of up to several hundred kilometers[11–14]. Expanding the transmission distance to reach inter-continental distances is challenging, as efficient quantum amplifiers or repeater stations are technologically challenging and have fundamental limitations[15–17]. Use of trusted nodes is seen as a way to expand quantum networks[18], but reliance on trusted nodes in terrestrial networks is not recognised as secure long-term solution. While there have been developments in next-generation low loss optical fiber[19] and protocols which are more robust to loss[20], free-space links is perceived as the most efficient and near-term solution to achieve a global quantum network[21,22].

Free-space QKD is a growing field, with interest in applications areas of short-range hand-held[23], last-mile coverage[24], medium to long terrestrial links[25], underwater links[26,27], and satellite links[22,28,29]. In contrast to optical fiber based QKD, where demonstrations are performed using phase or time-bin based protocols, free-space demonstrations are dominated by polarization-based protocol demonstrations[30]. There are two main benefits for using polarization protocols over phase or time-bin based for free-space; polarization encoding is relatively robust to atmospheric transmission[31]; the receiver measurement is based on passive splitting and robust to turbulence[25]. The reliance on multiple laser sources and detectors does, however, make the implementation expensive[29]. Phase and time-bin protocols, which rely on an interferometry measurement by the receiver, are less explored in free-space applications due to the challenges of multimode interferometry. Time and phase-based protocols have relatively simpler transmitter architectures and rely on fewer

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
1154006 · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2573479

detectors for the measurement[32,33], and could prove more cost effective. Recent developments have demonstrated free-space interferometer designs with passive optical elements that enable measurements of multimode quantum signals from turbulent free-space channels. The various designs have included relay optical lenses[34], interferometer paths with different refractive indexes[34,35], and other optical elements[36].

Here we present the prospects of implementing time-bin protocols in turbulent free-space channels, such as long distance a satellite-to-ground link. The operation of a three-state time-bin protocol, the coherent one-way (COW)[37], is the focus of the study. The performance model for the COW, secret key rate (SKR) and quantum bit error rate (QBER), is first outlined with various model parameters. A model for atmospheric turbulence is then outlined, specifically for the satellite-to-ground downlink scenario. Both models are used to look at system optimization and set bounds for optical channel losses.

2. COW PROTOCOL PERFORMANCE MODEL

In time-bin QKD protocols, the key information is encoded using time-bins[1]. Experimental demonstrations of time-bin protocols have been performed with faint coherent pulses[13], entangled photon-pair sources[34], and quantum dot single-photon sources[38]. The use of faint coherent pulses enables relatively simple architectures for the transmitter and receiver, as is highlighted in Figure 1, which shows a schematic diagram for the COW protocol[37,39]. The relative simplicity of the transmitter makes it attractive for free-space QKD, where it may be integrated into a platform with low size, weight, and power requirements, such as a satellite[40] or high-altitude platform[41]. With the recent developments in asymmetric multimode free-space interferometry, time-bin protocols could be a viable option for free-space QKD.

2.2 Overview of the COW protocol

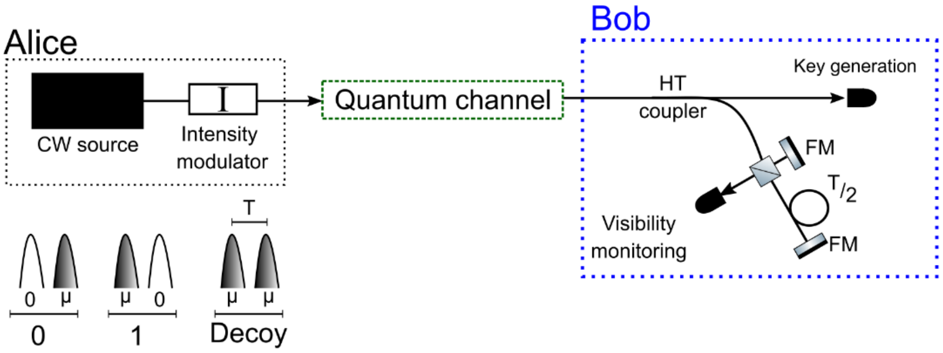


Figure 1. Schematic diagram for the coherent one-way protocol. A simple transmitter, constructed of a long-coherent length continuous-wave (CW) source and intensity modulator (I), is used to create the encoded signals 0, 1, and decoy. After passing through the quantum channel, the receiver (Bob) uses a passive beamsplitter, typically with a high transmission (HT coupler) to route the signal sent by Alice to a key generation or visibility monitoring stage. The key generation stage is simple a single-photon detector, which measures the time-of-arrival of the signal sent by Alice and it is used to record raw key information. The visibility monitoring stage is constructed of a time-delayed interferometer, with a time delay of half a period (T) each pass, giving a total time-delay of one period, T. Faraday mirrors (FM) are used to compensate for any polarization drift within the interferometer arms. Only one single-photon detector is required to monitor the visibility of the successive pulses.

In the COW QKD protocol time-bin information is encoded using an intensity modulator (IM) to pulse carve phase-coherent optical pulses from a long-coherence length continuous-wave (CW) laser[32]. Alice uses the pulse carving to prepare optical pulses with an intensity of μ, the mean photon number, or an empty (vacuum) pulse. Three time-bin signals can be prepared, providing a key bit 0 or 1, and a decoy state, shown in Figure 1. Alice then transmits the encoded time-bin signal to the receiver, Bob, through a quantum channel. Bob has two measurements: a key generation stage and a monitoring line. The key generation stage measures direct time-of-arrival of the incoming photons to generate raw key information. The monitoring line is a time-delayed, typically Michelson, interferometer that overlaps successive optical pulses and measures interferometric visibility of consecutive optical pulses. The interferometric visibility infers how much potential information could have been leaked to an eavesdropper or other malicious parties. Error correction and privacy amplification codes are used to reduce the amount of information leaked, and correct potential errors in the shared key, to produce a final shared secure key[37].

2.3 Secret key rate

To understand how the COW could perform in a real scenario, the model below is proposed. This model gives the SKR based on the probability of having a detection, an estimation of the QBER, and the amount of information a potential eavesdropper might have gained during the communication. For this last point, the model assumes that Eve could only perform the so-called beam-splitter attack (BSA) and the intercept-resend attack[39]. While the equations can be generalized to any type of channel, what is specific of a free-space implementation is the estimation of the parameters. The final equation that gives the SKR reads,

$$SKR = 0.5{\cdot}\mathrm{F}{\cdot}R_{sifted} \cdot [1 - h(QBER) - I_{EVE}] \tag{1}$$

where $h(\cdot)$ is the binary entropy function, F is the operational frequency (the factor of 0.5 is there because every bit is coded in two pulses), R_{sifted} is the probability of having a detection at the receiver after some basis reconciliation has been done, and I_{EVE} is the information gained by an eavesdropper. The probability of a sifted detection can be estimated as:

$$R_{sifted} = (R_{raw} + (1 - R_{raw}) \cdot p_{noise}) \cdot (1 - f) \tag{2}$$

being R_{raw} the probability of having a detection from any of the sequences sent by Alice, p_{noise} the probability of having a detection due to dark counts or background photons, and f the probability of a decoy sequence. In other words, equation (2) is the probability of having a detection by one of Alice's photon, plus the probability of having a noise count when no pulses are coming, multiplied by the probability that a detection is not a decoy sequence. Finally,

$$R_{raw} = \mu \cdot t \cdot t_B \cdot \eta \tag{3}$$

where μ is the mean photon number, t is the transmittivity of the channel, t_B is the transmittivity of the first beam splitter (HT coupler in Figure 1) of the receiver, and η is the quantum efficiency of the detector.

An eavesdropper (Eve) could gain information from the communication through two strategies, both presented in the original COW paper[39]. The BSA will introduce no errors, so the best thing it can be done is to assume all the losses of the channel have been introduced by Eve. On the contrary, the intercept-resend attack does introduce errors, so an estimation of the information gained by Eve can be calculated using the visibility measured at the monitoring line. Hence, Eve's information can be expressed as:

$$I_{EVE} = \mu \cdot (1 - t) + (1 - V) \cdot \frac{1 + e^{-\mu t}}{2e^{-\mu t}} \tag{4}$$

where V accounts for the visibility measured at the receiver.

The QBER estimation is usually restricted in other works to the contributions from dark counts. Although it is the most important source of errors, is not the only one existing in a real scenario. Hence, in this work we have expand this QBER estimation to include the contribution from background noise (something characteristic of free-space channels) and the errors due to the imperfection in Alice's device, which in practice cannot prepare empty pulses as true vacuum states.

$$QBER = QBER_{noise} + QBER_{coding} \tag{5}$$

First, the $QBER_{noise}$ is given by the ratio of detection which will not occur because of a photon sent by Alice,

$$QBER_{noise} = \frac{0.5 \cdot (1 - R_{raw}) \cdot p_{noise} \cdot (1 - f)}{R_{sifted}} \tag{6}$$

with $p_{noise} = p_{darkCounts} + p_{background}$. Both probabilities are estimated from the dark count rate of the detector and the background count rate. While the former is a parameter provided by the manufacturers, the latter has been figured following the analysis on reference[42], and an estimate light pollution for the site of interest. In this paper, the site is located close to Edinburgh, Scotland.

In order to translate from counts rate to probability of counts, the operational frequency and the gate width applied in the post-processing stage has been considered,

$$p_{count} = R_{count} \cdot G_{width} \cdot \min\left(F \cdot G_{width}, 1\right) \quad (7)$$

where R_{count} is the count rate (for dark counts or background counts), and G_{width} is the width in time of the gate. The fraction $F \cdot G_{width}$ should be always lower than 1 (otherwise it would imply that a gate-width longer than the time between two pulses is being applied), but the minimum $(\cdot,\cdot)$ function is included for the sake of clarity.

Finally, the QBER due to coding is given by the extinction ratio between the empty and non-empty pulses. Taking the data experimentally, an extinction ratio of 17 dB was measured, corresponding to a QBER of 0.02. This could be improved adding a second IM in cascade at the transmitter

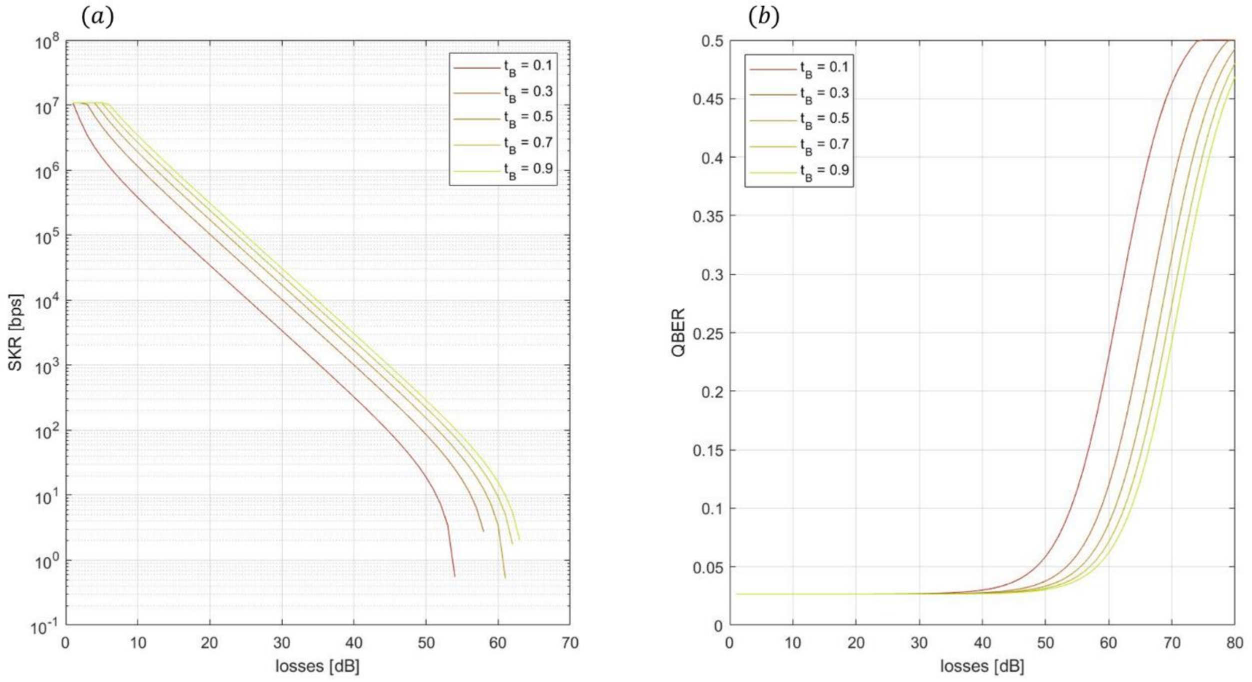


Figure 2. Secret key rate and quantum bit error rate of the coherent one-way protocol in a free-space scenario, for different beam-splitter ratios. For this simulation, the operational frequency was set to 1 GHz, with a gate width of 200 ps, a dark count rate at the detector of 100 counts/s, a probability of a noise count in the order of 10^{-8}, and an interferometric visibility of 0.98. At low losses, the saturation effect of the detectors due to the dead time can be seen. The data was generated under moonless sky conditions.

Simulations were conducted to give a performance estimation of the COW protocol in a free-space scenario using equation (1) at 1 GHz, with a gate width of 200 ps, a dark count rate at the detector of 100 counts/s, a probability of a noise count in the order of 10^{-8}, and an interferometric visibility of 0.98. Specifically, we are interested in understanding which is the optimal beam splitter ratio (t_B) to design the receiver. The results for SKR and QBER can be seen in Figure 2 (a) and (b) respectively. We observed a linear increase in the SKR when increasing the beam-splitter ratio, i.e. increasing the transmission to the key generation stage. We considered that in order to boost the SKR generation, but at the same time not to lose precision on the security analysis due to the number of counts, an optimal ratio should be around 70:30 or 80:20. Due to its availability, a 70:30 beam splitter was said to be a good solution for a free-space implementation.

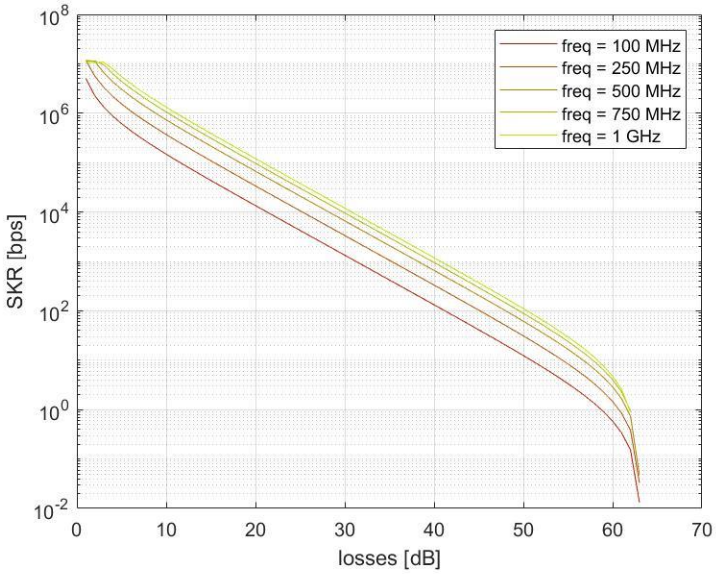


Figure 3. Secret key rate (SKR)of the coherent one-way protocol in a free-space scenario for different operational frequencies. As can be seen, as the operation frequency increases, so does the SKR. At large channel losses, >60 dB, the SKR falls off due to the signal-to-noise ratio at the detectors.

A simulation was also conducted to understand the expected SKR for different operation frequencies. Results can be seen in Figure 3. As the operation frequency was increased, it can be seen that the SKR rate also increases, which is expected. At very low channel losses a detector saturation effect can be observed when reaching the gigahertz operation. At high losses, >60 dB, it can be seen that the SKR falls off, even for high operational frequencies, which is due to an increase in the probability of a noise count. Even though the signal probability is higher, because there is an increase in gated time, this leads to an increase in noise also. Fundamentally, to improve the SKR rate, a decrease in dark count rate and noise would be required. Noise reduction could be achieved by improving detector technology, narrowing optical filters, and reducing the field-of-view of the optical system.

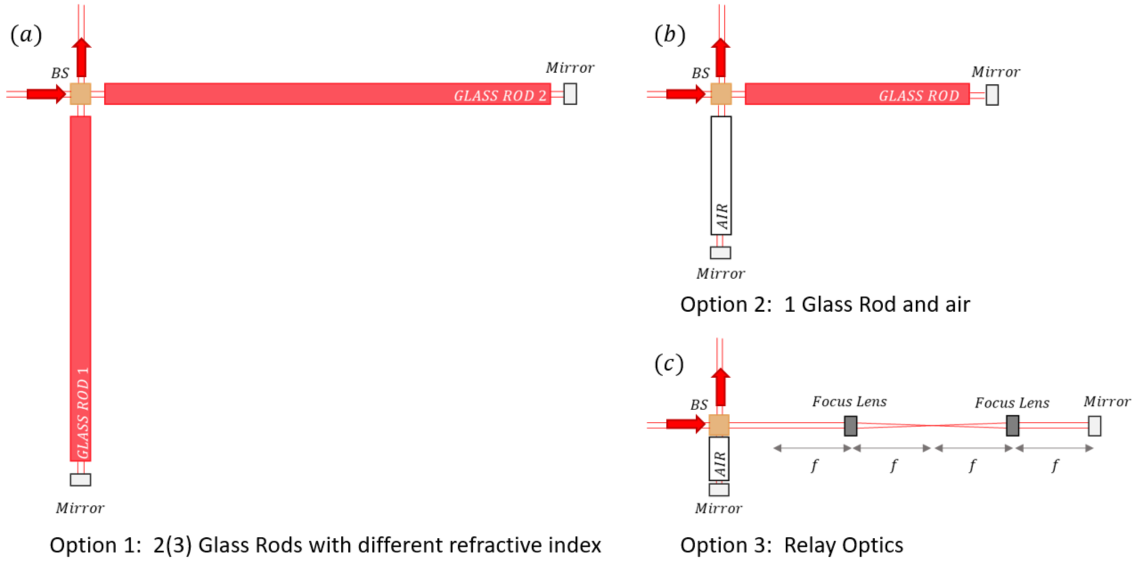
The results show that the COW protocol could operate in large loss channels, like those expected in free-space QKD, which are typically in the range of 20-40 dB[29], not counting channel turbulence. The next section will discuss the additional losses due to atmospheric turbulence, which put a bound on the performance. As a note of performance, at 1 GHz operational frequency, the estimated SKR is 10 kbps at a channel loss of 30 dB, Figure 3.

3. ATMOSPHERIC TURBULENCE EFFECTS

Free-space propagation loss is dynamic and complex, with many sources of loss[43]. However, in this analysis we present a study on one of these sources, the atmospheric turbulences. We do this because it is the least studied for QKD channels and is most relevant to time-bin protocols, where the interferometers must be able to monitor multimodal channels.

3.1 Passives optics to overcome turbulence effects

Atmospheric turbulence has several effects on the transmitted beam. Two of them are the reason why time-bin QKD is considered challenging: beam wandering and beam scintillation, which induce variable angle of incident in the interferometer. To overcome both issues, passive optics solutions have already been proposed and demonstrated. Here, we give a brief overview of the main advantages and disadvantages of each of the three possible designs (Figure 4): two (or three) glass rods (plus an air gap) (a)[35], one glass rod and air (b)[34], and relay optics (c)[34]. In order to understand which design performs better under certain conditions, three figures of merit are considered: the size of the interferometer, its cost, and its thermal stability. The rest of the receiver will remain the same independently of the chosen design, so is considered as constant, and therefore not included in the analysis.



Option 1: 2(3) Glass Rods with different refractive index

Option 2: 1 Glass Rod and air

Option 3: Relay Optics

Figure 4. Three different designs for a multimode free-space unbalanced interferometer. Option (a) gives the best thermal stability, option (b) has the smallest size of the three designs and option (c) is the cheapest of the three of them. Each could be the best solution in a real scenario, depending on the project's constraints.

First, size must be considered for a real application scenario, since small and compact systems are more desirable. Here, the option with two (three) glasses (Figure 4 (a)) is the largest, as the system is forced to be the most thermally stable possible. The fact that two (three) different material are used, forces both arms to be about the same size, making the system the largest. The glass plus air solution, Figure 4 (b), is the smallest possible because of the big difference in the refractive indexes between arms. However, it comes at the cost of a thermally stable system. Finally, the relay optical system, Figure 4 (c), is a reasonable solution, specially for slow frequencies operations, where lenses may also be commercially available. The difference between the interferometer arm lengths for a range of operational frequencies can be seen in Figure 5 (a), highlighting the lengths of glass required.

Second, the cost of the optics is considered. The price of the focus lenses and the glass rods depends on the materials and the size of them, as well as the fabrication processes required to make them. For slower operational frequencies (MHz), the relay optical elements are more cost effective, due to the ease in fabrication and alignment. For faster operations frequencies (GHz), the glass rods are a more cost effective option, as the fabrication and alignment is easier.

Finally, the last figure of merit is the thermal stability. As can be seen in Figure 5 (b), the option with glass and air is very unstable. Relay optics seems to behave more reasonable, while the two (three) design is the most stable solution by far, being even theoretically stable if three materials are used for its construction. Also, the smallest the system is (or the higher the operational frequency) the most stable all the designs will be. At the GHz regime, the option with one glass and air could start being interesting due to its size advantage.

There is no clear-cut winner between the three interferometer designs, and it is the operational aspect of the protocol that will determine the best design solution. All of the designs can be used as robust solutions for multimode interferometry.

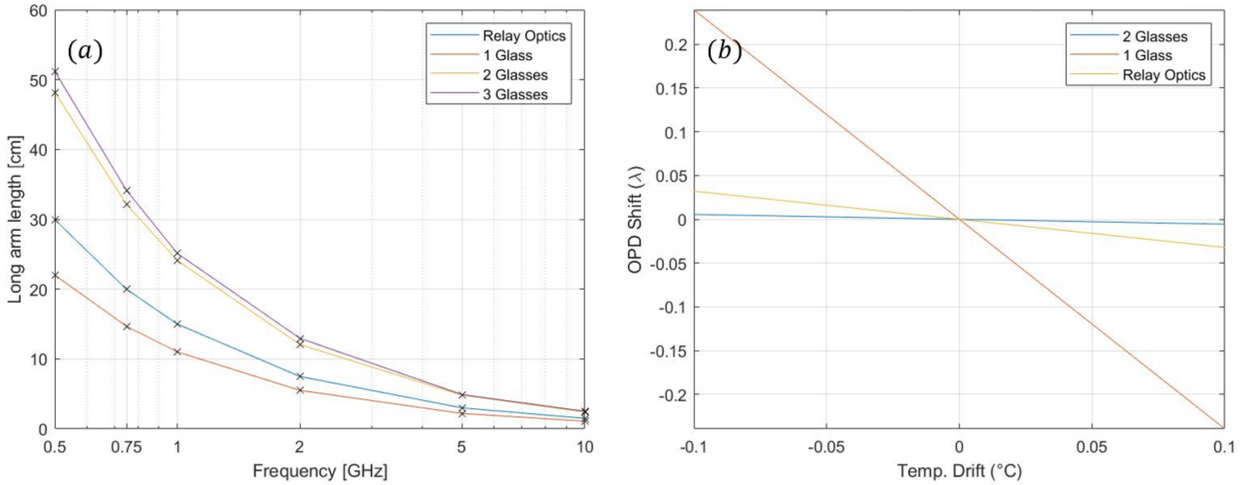


Figure 5. Size and thermal stability of the different designs. (a) shows the decrease in size for different operational frequencies. All the designs decrease with a rate of 1/frequency. While for high frequencies all the sizes are comparable, there is a big difference at low frequencies. (b) gives an estimation on the optical path different (OPD) shift with respect to the wavelength for 1 GHz. Considering this, the design with only one glass rod is unstable due to the different behaviour between glass and air. Nevertheless, this stability can be always increased in any design making the system smaller (increasing the frequency). We see that the design with two glasses is the most stable, followed by the design with the relay lens optics.

3.2 Losses for a satellite to ground link

Another important effect of the atmospheric turbulence is a statistical fading on the power of the beam. On the contrary to the other effects presented, this is a loss that cannot be corrected with any other method. In this section, a study is proposed to understand which losses should be expected under some conditions.

Here we make use of the model proposed in reference[44]. Other models have been presented in order to understand losses due to turbulence in QKD scenarios[45,46]. However, they do not consider the statistical effects of it, or they rely on complex computational simulations. The approach we took here is to give a relatively simple mathematical equation that can offer a numerical loss taking into account the statistics of it, making use of the gamma-gamma model,

$$p(I) = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{x} \cdot I^{\frac{\alpha+\beta}{2}-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta I}\right) \tag{8}$$

where $p(I)$ is the probability of an irradiance I, α and β are values associated to the scintillation index[44], and $K_x(\cdot)$ is the modified Bessel function of second kind.

To estimate the wind speed across the atmosphere for the Hufnagel-Valley model we make use of the equation,

$$v_{RMS} = \sqrt{v_g^2 + 30.69 v_g + 348.61} \tag{9}$$

where v_g is the speed of the wind at ground level in m/s. With this model, we are able to plot the fading statistics of the irradiance for different atmospheric conditions and angle of elevations, this is, the probability that the loss in power is greater than a threshold. Figure 6 (a) and (b) show the probability against loss for an elevation angle of 20° and 80° (with respect to the vertical) for low, medium, and high levels of turbulence (see Figure 6 for details). Finally, in order to translate this model into a numerical loss (Table 1) the maximum losses of a channel with a confidence of 90% has been calculated, in other words, the losses will only be greater than that maximum 10% of the time. The numerical value allows us to set an estimated loss value for the link budget, to account for turbulence losses. It can be seen from Table 1 that up to 10 dB channel loss could be added to the link budget from variation in turbulence levels. As an example, following the previous section, that additional loss at 1 GHz operational frequency will increase the channel loss from 30 dB to 40 dB, reducing the key rate from 10 kbps to 1 kbps.

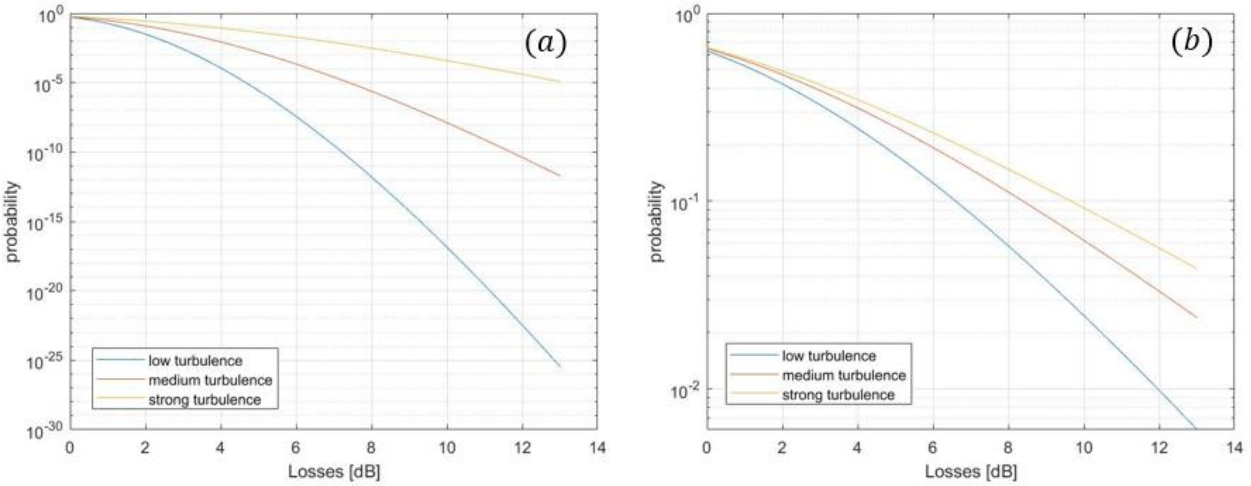


Figure 6. Probability of having a loss higher than a certain value for different turbulence conditions: low turbulence (v_g = 1 m/s, and the nominal ground-level value of $C_n^2$of the Hufnagel-Valley model A = $1.7 \cdot 10^{-14}$), medium turbulence (v_g = 15 m/s, A = $1.7 \cdot 10^{-13}$) and strong turbulence (v_g = 35 m/s, A = $1.7 \cdot 10^{-12}$). Figure (a) shows the result for an elevation angle of 20° (with respect to the vertical) while figure (b) does it for an elevation angle of 80°. Other parameters used for the simulation were an orbit height of 500 km, ground station elevation of 200 m, and light wavelength of 850 nm.

Table 1. Estimated losses due to atmospheric turbulences under different conditions. The loss is given as the maximum during 90% of the time, in accordance to simulation results.

Condition	**Elevation angle 20º**	**Elevation angle 80º**
Low turbulence	1.3 dB	6.7 dB
Medium turbulence	2.1 dB	8.2 dB
Strong turbulence	3.7 dB	9.6 dB

4. CONCLUSIONS

In this paper, a model for the performance of the COW protocol in a free-space implementation was presented together with an analysis of the effects of atmospheric turbulence during the communication. The COW analysis can be expanded to include more general attacks with the work presented in reference[13].

The COW protocol model highlighted that SKRs in the order of kilo-bits per second could be achieved at an operational frequency of 1 GHz within a loss budget range of 20-40 dB, the expected range for satellite-based QKD. Many of the models previously used to estimate free-space channel loss do not specifically account for atmospheric turbulence at different levels, and generally assign a set value incorporated into atmospheric loss. Our model highlights that turbulence could add additional losses of up to 10 dB for large elevation angles. With the various multimode interferometer design options and capability to generate secure keys in lossy and turbulent channels, time-bin protocols look to be a viable option for free-space QKD.

REFERENCES

[1] Tittel, W., Zbinden, H. and Gisin, N., "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).

[2] Bennett, C. H. and Brassard, G., "Quantum Cryprography: Public Key distribution and coin tossing," Int. Conf. Comput. Syst. Signal Process. (1984).

[3] 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).

[4] 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).

[5] Bogdanski, J., Rafiei, N. and Bourennane, M., "Experimental quantum secret sharing using telecommunication fiber," Phys. Rev. A - At. Mol. Opt. Phys. **78**(6), 3–8 (2008).

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] 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).

[11] Sasaki, M., "Quantum networks: where should we be heading?," Quantum Sci. Technol. **2**(2), 020501 (2017).

[12] Simon, C., "Towards a global quantum network," Nat. Photonics **11**(11), 678–680 (2017).

[13] Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., Sanguinetti, B., Thew, R. and Zbinden, H., "Provably secure and practical quantum key distribution over 307 km of optical fiber," Nat. Photonics **9**(3), 163–168 (2015).

[14] Yin, H.-L., Chen, T.-Y., Yu, Z.-W., Liu, H., You, L.-X., Zhou, Y.-H., Chen, S.-J., Mao, Y., Huang, M.-Q., Zhang, W.-J., Chen, H., Li, M. J., Nolan, D., Zhou, F., Jiang, X., Wang, Z., Zhang, Q., Wang, X.-B. and Pan, J.-W., "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber," Phys. Rev. Lett. **117**(19), 190501 (2016).

[15] 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).

[16] 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).

[17] Bäuml, S., Christandl, M., Horodecki, K. and Winter, A., "Limitations on Quantum Key Repeaters," 41 (2014).

[18] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., et al., "Field test of quantum key distribution in the Tokyo QKD Network.," Opt. Express **19**(11), 10387–10409 (2011).

[19] Poletti, F., "Nested antiresonant nodeless hollow core fiber," Opt. Express **22**(20), 23807 (2014).

[20] Lucamarini, M., Yuan, Z. L., Dynes, J. F. and Shields, A. J., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**(7705), 400–403 (2018).

[21] 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).

[22] Bedington, R., Mantilla, J. M. A. and Ling, A., "Progress in satellite quantum key distribution" (2017).

[23] Chun, H., Choi, I., Faulkner, G., Clarke, L., Barber, B., George, G., Capon, C., Niskanen, A., Wabnig, J., O'Brien, D. and Bitauld, D., "Handheld free space quantum key distribution with dynamic motion compensation," Opt. Express **25**(6), 6784 (2017).

[24] Kollmitzer, C. and Pivk, M., [Applied quantum cryptography] (2010).

[25] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H. and Zeilinger, A., "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**(7), 481–486 (2007).

[26] Fahim Raouf, A. H., Safari, M. and Uysal, M., "Performance analysis of quantum key distribution in underwater turbulence channels," J. Opt. Soc. Am. B **37**(2), 564 (2020).

[27] Shi, P., Zhao, S.-C., Li, W.-D. and Gu, Y.-J., "Feasibility of underwater free space quantum key distribution," 481–486 (2014).

[28] 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).

[29] 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).

[30] 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. **98**(1), 1–4 (2007).

[31] Zhang, J., Ding, S., Zhai, H. and Dang, A., "Theoretical and experimental studies of polarization fluctuations over atmospheric turbulent channels for wireless optical communication systems," Opt. Express **22**(26), 32482 (2014).

[32] Stucki, D., Fasel, S., Gisin, N., Thoma, Y. and Zbinden, H., "Coherent one-way quantum key distribution," Proc. SPIE **6583**, 65830L-65830L – 4 (2007).

[33] 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).

[34] Jin, J., Agne, S., Bourgoin, J. P., Zhang, Y., Lütkenhaus, N. and Jennewein, T., "Demonstration of analyzers for multimode photonic time-bin qubits," Phys. Rev. A **97**(4), 1–10 (2018).

[35] Cahall, C., Islam, N. T., Gauthier, D. J. and Kim, J., "Multimode Time-Delay Interferometer for Free-Space Quantum Communication," Phys. Rev. Appl. **13**(2), 024047 (2020).

[36] Jin, J., Bourgoin, J.-P., Tannous, R., Agne, S., Pugh, C. J., Kuntz, K. B., Higgins, B. L. and Jennewein, T., "Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel," Opt. Express **27**(26), 37214 (2019).

[37] 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).

[38] Takemoto, K., Nambu, Y., Miyazawa, T., Sakuma, Y., Yamamoto, T., Yorozu, S. and Arakawa, Y., "Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors," Sci. Rep. **5**(1), 14383 (2015).

[39] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V., "Towards practical and fast Quantum Cryptography" (2004).

[40] 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).

[41] Tozer, T. C. and Grace, D., "High-altitude platforms for wireless communications," Electron. Commun. Eng. J. **13**(3), 127–137 (2001).

[42] 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).

[43] 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).

[44] Andrews, L. C., Young, C. Y., Al-Habash, A., Phillips, R. L. and Tjin-Tham-Sjin, D. E., "Fade statistics associated with a spaceground laser communication link at large zenith angles," Propag. Imaging through Atmos. III **3763**, M. C. Roggemann and L. R. Bissonnette, Eds., 268–277, SPIE (1999).

[45] Sharma, V. and Banerjee, S., "Analysis of atmospheric effects on satellite-based quantum communication: a comparative study," Quantum Inf. Process. **18**(3), 67 (2019).

[46] Villaseñor, E., Malaney, R., Mudge, K. A. and Grant, K. J., "Atmospheric effects on satellite-to-ground quantum key distribution using coherent states" (2020).

[47] 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).