End-to-end simulation of satellite based quantum key distribution

Vladlen Galets'Ky
vladlen.galetsky@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

December 2021

Abstract

We simulate a satellite Quantum Key Distribution (QKD) downlink which was created during the concept development and preliminary design completion phases of the QuantSat-PT project mission life cycle. We shall consider in great detail all the losses for the mission accordingly to the defined requirements, with special attention to the turbulent and atmospheric losses for BB84 and E91 protocols which remained inconsistent with real data. We have obtained for the BB84 protocol a sifted key rate and Quantum Bit Error Rate of 32.1 kbit/s and 4% at zenith respectively for a 750 km orbit. For the E91 protocol the Clauser, Horne, Shimony and Holt (CHSH) test was performed obtaining a correlation factor of $S \in [-2.63 \pm 0.02, -1.91 \pm 0.03]$ for the mission. All results are consistent with the state of the art simulators and experiments in field of QKD.

For phase-dependent protocols a new convolutional neural network algorithm is proposed, to recover the disturbed intensity profiles of the signal at the ground station with the use of adaptive optics, improving up to an order of magnitude the mean square error between the disturbed images and the corrected ones.

Keywords: QKD simulation, Cubesat downlink, Turbulence modelling, Optical communications, CNN

1. Introduction

1.1. Quantum computer vulnerability

Recent advances in quantum computing performed by Google quantum AI claimed to reach for the first time quantum supremacy in 2019 [1]. More recently in 2021 by studying a new series of *Quantum Falcon* processors, IBM increased the quantum volume of circuits to 64 for their current architecture. Moreover in the same year, it has been claimed that the superconducting quantum processor, *Zuchongzhi*, also achieved quantum supremacy creating an opening for a new era of quantum computing. All these advances make us question the vulnerability of our data. One way to secure is applied in this thesis, by using Quantum key distribution (QKD). The following method applies the rules of the quantum computers against themselves, using the uncertainty principle and entanglement of states.

1.2. QKD in space

In order to globalize the protection to exchange information, a solution via a satellite link to ground is performed. Usually, a trade-off between key rate, QBER and distance is needed to define the optimal conditions for the mission. For downlinks the optical apparatus is located in the payload, leading to heavier requirements in the mass, energy consumption and higher risks. On the other hand for an uplink, the information transmission is more stable however the atmospheric and turbulent effects are more dominant thus decreasing the average key rate and Quantum Bit Error Rate (QBER).

For our mission we will use the former. The simulator presented in this work was developed during the phases A, B and C part of the QuantSat-PT project life cycle. The main objective of the project is to perform the first ever Portuguese QKD space mission on a 2U Cubesat. This work not only contributes as a viable simulator for the QuantSat-PT mission, but also, is as step in the right direction for a more realistic simulation of future satellite QKD missions.

In the next section we will provide an overview for the state of the art missions in the field of QKD as well as the simulators used. In section 3 the requirements for the mission are presented. Afterwards, in section 4 we shall define and simulate the orbit for QuantSat-PT. Moreover, in sections 5, 6, 7 and 8 we shall study the the geometrical, background, atmospheric and turbulent attenuation coefficients respectively and their influence on our signal. In section 9 we will propose a new method

for intensity profile correction for phase-dependent QKD protocols. The main results are presented in section 10 computing the QBER and sifted key rate for the BB84 and performing the CHSH test for the E91 protocol.

2. Overview

2.1. State of the art QKD missions

Micius [6]

Micius was successfully launched on August 2016 [6] from Jiuquan, China, and now orbits at an altitude of about 500 km in LEO. One of the satellite payloads had a BB84 decoy-state QKD transmitter at a wavelength of 850 nm cooperating with Xinglong ground observatory station. At optimal distance of 600 km, it achieved a QBER $\sim 2\%$ and a sifted key of 14 kbps. In 2017 the mission concept went onto a second phase [6], establishing a space-to-ground two-downlink channel creating a 1200 km distance QKD between two GS (Nanshan and Delingha), however, a secured node configuration was assumed, meaning that no Eve was present (QBER $\sim$ 8.1$\%$ with sifted key rate of 1.1 Hz). The measured overall two-downlink channel attenuation was at peak 82 dB which was more than predicted. With additional losses being justified from the turbulent behaviour of the atmosphere.

SOCRATES [12]

SOCRATES micro-satellite was first launched in 2014, with the main objective of technology demonstration for position and attitude control. SOTA, lasercom payload, had a secondary mission in 2016 of creating a B92-like QKD protocol at 800-nm band to perform the first-time quantum limited demonstration from space. From the results of the experiment [12], the total loss budgets from the simulation analysis and the real data losses received were off from a range of 29.5 dB to 13.8 dB. Thus, pointing to unmet simulation conditions for QKD analysis due to the complexity of the problem in study. In the article, these values are attributed to atmospheric scintillation, which typically could change losses by that order of magnitude, hence the thesis being incentivized for a more detailed study on the turbulence influence for the quantum laser communications.

2.2. QKD simulators

Bourgoin et al. [2]

Burgoin et al. simulated and calculated the expected performance for a year-long 600 km satellite conducting a QKD link at 670 nm for a sun-synchronous orbit implementing a decoy state BB84 protocol. A Rayleigh–Sommerfeld diffraction was considered with a custom beam profile with a convoluted pointing error. MODTRAN was used for the atmospheric attenuation calculation, artificial and natural background was considered. An in-depth comparison between up-link and downlink approaches were also performed.

Considering a 600 km orbit, and considering a beam waist of $w_0 = 0.05$ m and diameter of receiver of $D_R = 1.0$ m at the ground station (GS), the author's achieve a QBER below 11% between zenith angles of $\theta_{zen} \in [0, 70]$ deg.

Daniele Dequal et al. [3]

A different take on the approach looks into probability distribution of the transmission coefficient (PDTC), a statistical interpretation for the off-pointing, turbulence disturbance and atmospheric effects. It examines the effect of channel fluctuations in CV-QKD, using in the simulator a derivation of the equations for the secret key rate over generic fading channels. Overall, for a 800 km orbit a downlink transmissivity of 1.8% is achieved.

Carlo Liorni et al [7]

This method considers that imperfections from the truncation of the border in optical elements, conditions in the far field an additional broadening of the beam. Thus, it computes an imperfect quasi-Gaussian beam in a turbulent environment characterized by a PDF model. Considering the same parameters as in Daniele Dequal et al. for a 500 km orbit, the authors obtain a total loss 20 dB at zenith to 30 dB at the horizon. The author's work achieves for Cubesats a $QBER = 3\%$ at low zenith angles going up to $QBER = 14\%$ at zenith angles above $\theta_{zen} = 75\%$.

3. Requirements

To define the mission's parameters we must first select the most essential requirements for the mission, as seen in Table 1.

Technical Requirements are defined in TR [01-04], Table 1. They often coexist with the basic needs of the mission to perform QKD. Contractor requirements are present in CR [01-05], Table 1. They commonly differ from the first ones by being created for the specific needs of the mission. In our case they sub-categorize mainly into Operational and Environmental Requirements. Operational requirements add constrains on the QBER, defining that the mission uses a 2U Cubesat which restricts the mass and size of the optical apparatus. It gives us an expected minimum duration of the mission. Environmental constrains optimize the key rate by defining an active time and a location for the mission, by minimizing the artificial and natural background. The structure for the requirements follows ECSS-E-ST-40C and IEEE 15288.2 for ESA and NASA standardization procedures.

ID	Name	Text	Rationale
TR-01	Tracking	GS shall be able to track light from S/C with accuracy higher than 1.0×10^{-04} rad for FoV.	To diminish losses in key rate.
TR-02	Detection	GS shall be able to detect single photons from S/C.	To correctly distinguish the encoded information in QKD.
TR-03	Key sifting	GS shall be able to perform key sifting on the chosen QKD protocol.	To successfully perform QKD.
TR-04	Polarization Decoding	GS shall demultiplex polarization encoded photons.	To successfully perform polarization encoded QKD.
CR-01	Security	Mission shall be able to maintain secure communications. QBER$< 11\%$ for BB84 and $\|S\| \geq 2$ for E91	To successfully perform QKD.
CR-02	Mission Duration	Mission shall prevail for a life-time of at least 3 years.	To acquire enough data to successfully study QKD.
CR-03	Size of Satellite	Mission's S/C shall be a 2U Cubesat (20x10x10 cm).	To test QKD on a nanosatellite.
CR-04	Ground Location	GS shall be defined in Alqueva, Portugal.	To account for the lowest artificial background environment.
CR-05	Time measurements	S/C shall pass-by GS at least once after 23:00 (GMT+1).	To account for the lowest natural background environment.

Table 1: Requirements that directly define the properties of the simulator.

4. Orbit

In this section we shall define the satellite (S/C) orbit. In our case we use GMAT R2020a in order to propagate and obtain the distance of the satellite with respect to ground (GS). We shall perform this analysis for the 400, 500, 600 and 750 km altitude orbits. The parameters chosen are defined in Table 2.

The obtained results are shown in Fig 1. For the simulation the Runge-kutta 89 (RK89) integrator was used. The propagative error of the integator in position and velocity of the S/C was also performed leading to an absolute mean error of our results between different numerical integrators (shown in Table 3). We discovered that the order of magnitude for the propagative error is too low to have a dominant impact on the S/C altitude $[10^2, 10^3]$ km.

The end-of-life cycle of the orbits were also simulated using the ESA's OSCAR tool from DRAMA as seen in Fig 3. For 400, 500 and 600 km the orbits life-cycle was estimated to be 1, 4 and 20 years respectively. For the former, the orbit becomes not viable for the mission due to the requirement for the QuantSat-PT project to have a mission life-time of at least three years.

5. Geometrical losses

For this section, a geometrical analysis is performed to define the optimal geometrical parameters for the diameter of the receiver (D_R) and transmitter (D_T) as well as the orbit altitude. For that we shall consider the performance of the signal in terms of the chosen orbit, using Equation 1 we ob-

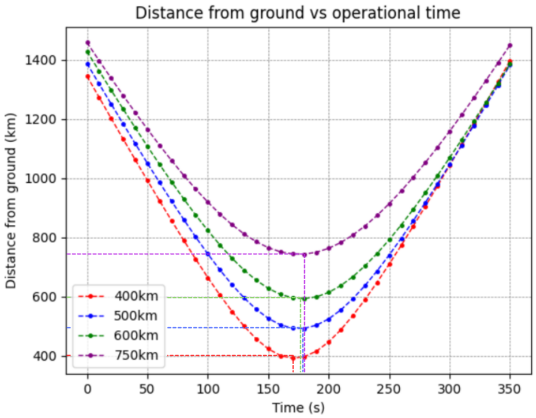

Figure 1: Optical path from S/C to GS for 400, 500, 600 and 750 km. The centroid and minimum distance is presented for each orbit.

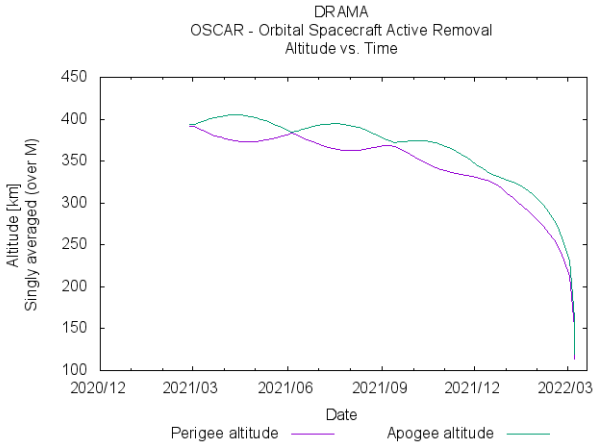

Figure 2: Altitude above ground of S/C in terms of time for 400 km.

Parameter	Description	Unit	Parameter	Description	Unit
Starting date	25 Feb 2021 22:00:00	-	Drag coefficient	2.20	-
Reflectivety coefficient	1.30	-	Coordinate system	Earth centered inertial (J2000)	-
State type	Keplerian	-	Integrator	RK89	-
Eccentricity	1.21×10^{-16}	-	Semi-major axis	6771.00	km
Inclination	98.00	deg	RAAN	295.00	deg
Argument of Perigee	0.00	deg	True Anomaly	1.48×10^{-6}	deg
Minimum GS elevation visibility	10.00	deg	D_T	0.03	m
Wavelength	850.0 ± 1.0	nm	D_R	2.0	m

Table 2: Orbital and optical parameters for 400 km altitude propagation of the spacecraft in GMAT

Parameter	RK4	RK-DP45	RK-DP78	RK-DP853	Unit
$\|E_1\|$	2.3×10^{-1}	6.11×10^{-4}	4.35×10^{-5}	2.22×10^{-3}	km
$\|E_2\|$	1.14×10^{-1}	2.98×10^{-4}	4.73×10^{-5}	1.08×10^{-3}	
$\|E_3\|$	2.53×10^{-1}	6.67×10^{-4}	6.28×10^{-5}	2.42×10^{-3}	
$\|E_{v1}\|$	2.69×10^{-4}	6.85×10^{-7}	5.00×10^{-8}	2.48×10^{-6}	km/s
$\|E_{v2}\|$	1.32×10^{-4}	3.39×10^{-7}	5.35×10^{-8}	1.23×10^{-6}	
$\|E_{v3}\|$	2.92×10^{-4}	7.55×10^{-7}	7.11×10^{-8}	2.74×10^{-6}	

Table 3: Absolute mean error between RK89 and the a chosen integrator used for orbit propagation.

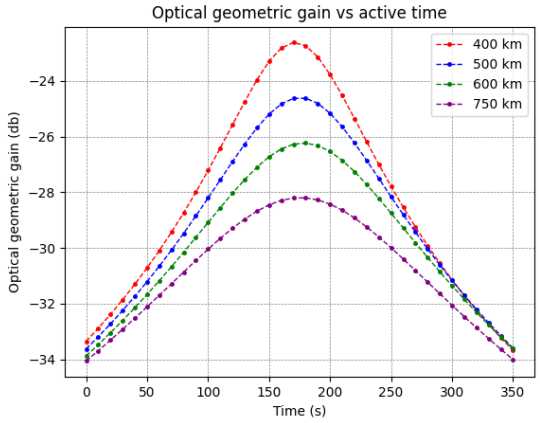

Figure 3: Optical loss for 400, 500, 600 and 750 km in altitude.

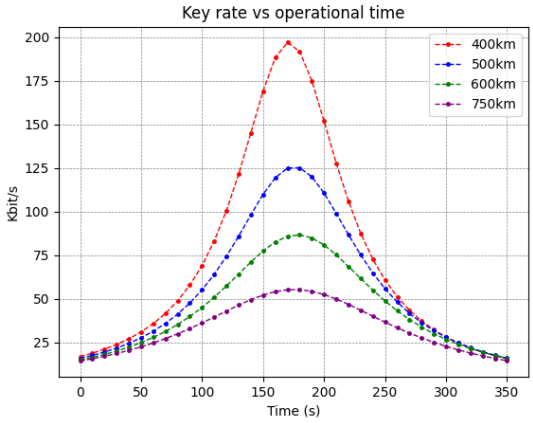

Figure 4: Sifted key rate for 400, 500, 600 and 750 km in altitude.

tain Fig 3.

$$\frac{P_R}{P_T} = 20log\left(\frac{D_R D_T}{D_T^2 + 2.44mL\lambda}\right) \quad (1)$$

Where P_R, P_T and L are the respective power at the receiver, transmitter and total optical path. In order to calculate the key rate that we would obtain at GS, we estimated the number of photons sent by the single photon source with a step of $\Delta t = 10$ s between each key exchange. Afterwards the expected power loss is calculated from it, resulting in our overall key. Thus, obtaining Fig 4.

For the QBER we have considered Equation 2:

$$QBER = \frac{\frac{Y_0}{2} + e_{det}(1 - e^{-\eta L(\theta)\mu(\theta)})}{\frac{Y_0}{2} + 1 - e^{-\eta L(\theta)\mu(\theta)}} \quad (2)$$

Y_0 and e_{det} are the dark count probability and the basis misalignment respectively. L is the optical path which is dependent on elevation (θ), η contains the optical and quantum efficiencies. Finally, $\mu(\theta)$ is the generalized loss function which is also geometrically dependent on elevation.

Thus, obtaining respectively for each altitude at zenith $QBER = 3.33\%, 3.34\%, 3.35\%, 3.38\%$ for $400, 500, 600$ and 750 km orbits as seen in Fig 5

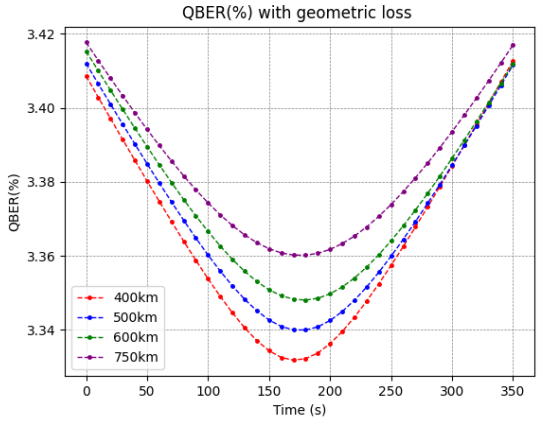

Figure 5: QBER for 400, 500, 600 and 750 km in altitude. Considering only the geometric loss, all the results for BB84 protocol are below the limit of 11%.

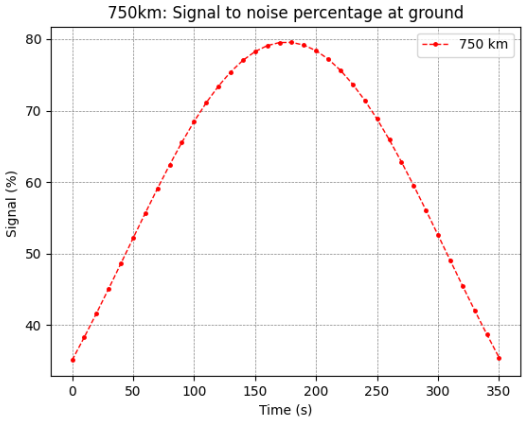

Figure 6: SNR received at GS during active time. At zenith a SNR of 79.8% is achieved.

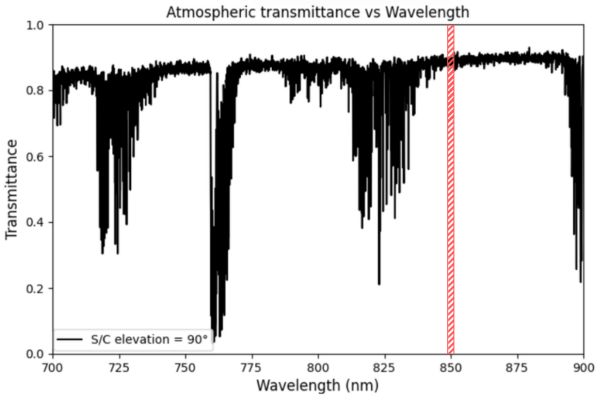

Figure 7: S/C photon transmissivity at zenith propagating along the atmosphere at different wavelengths.

6. Background Noise

For the background we used the VIIRS open source data which provides satellite imagery of Earth in different ranges of wavelength along time, we choose the day and night band obtaining the total artificial and natural brightness at zenith of $B_{Total} = 0.000222 \pm 0.000011$ cdm^{-2} and $B_{Natural} = 0.000051 \pm 0.000005$ cdm^{-2}, respectively. However, at different elevations of the S/C the brightness intensity varies due to the atmospheric airmass. Thus, we account for that by considering the Rayleigh airmass density and the change in magnitude due to its increase. Afterwards, the respective photon number from background sources may be calculated following Equation 3:

$$N_{tot} = \frac{1}{E_\lambda}\{(H_{nat} + H_{art}) \times \pi(FoV)^2 \times \\ \times q_{eff} \times \frac{\pi}{4} D_R^2\} \quad (3)$$

Hence, obtaining as seen in Fig 11 a background rate reaches up to an order of $B \in [3.0 \times 10^4, 5.3 \times 10^4]$ cps leading to a signal ratio of $S_F \in [36.1, 79.8]\%$.

All results were compared with SkyCalc[1] simulator for the sky brightness which considers the Cerro Paranal Sky Model as well as ESO-Paranal experimental data, obtaining results within the same order of magnitude.

7. Atmospheric losses

For this section we pretend to obtain the attenuation coefficients from the atmosphere and the depolarization ratio of the signal when propagating towards the GS. To construct the atmosphere we shall use an open source software called libradtran 2.0.4 [2]. This tool allows us to use MonteCarlo to solve the polarized radiative transfer equation in 1D geometry. By using Mystic we perform photon forward tracing, where individual photons are traced from their source to their random paths.

Attenuation

We consider an albedo ratio of 0.2, an aerosol visibility of 23 km, a mid-latitude summer atmospheric file containing the molecular profile of particles of the atmosphere as well as a band parametrization at the top of the atmosphere with a fine bandwidth resolution of 1.0 $cm^{-1}bin$. Subsequently, we can solve the radiative equation for our system and find the transmissivity ratio at zenith as seen in Fig 7.

We obtain a transmissivity of the signal for this atmosphere along zenith of $\tau_{atm} = 0.8508^{+0.0374}_{-0.0178}$. The uncertainty is calculated based on the bandwidth filtering margin of ± 1.0 nm.

As seen in Fig 8, we reached similar results for the atmospheric transmissivities along the el-

[1] SkyCalc is an open source software which allows to simulate at a certain bandwidth the natural background at the ESO-Cerro Paranal ground site

[2] Documentation for the 2.0.4 version is available.

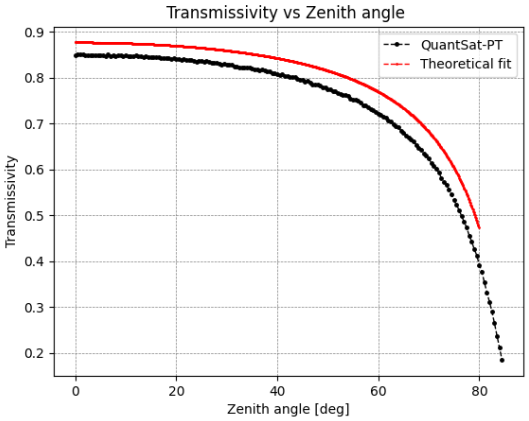

Figure 8: Photon transmissivity along the atmosphere for different S/C elevations. A theoretical model is presented in red to verify the results.

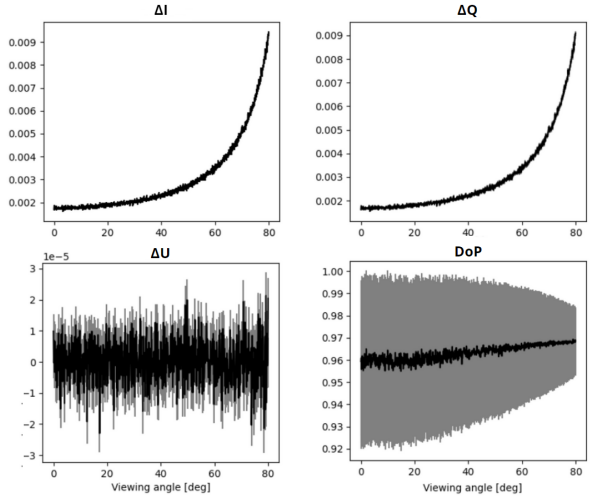

Figure 9: Variance for the Stokes parameters and degree of photon depolarization in terms of S/C elevation.

evation with a theoretical model which considers: $\tau_{atm} = \tau_{zen}^{sec(\theta_{zen})}$. Here τ_{zen} is the optical transmissivity at zenith, and θ_{zen} the corresponding zenith angle.

Degree of Depolarization

For the Degree of Polarization (DoP) we consider that all our sent photons are linearly polarized $\gamma = (1, 1, 0, 0)$ during a timestep of 10 s between acquisitions for each S/C elevation. The Monte Carlo method is propagated considering a single photon source frequency of 100 MHz. The obtained results for the variance of the Stokes parameters $(\Delta I, \Delta Q, \Delta U, \Delta V)$ and DoP in terms of the S/C elevation can be seen in Fig 9. We obtain at the horizon $DoP(\%) = 96.1 \pm 3.9\ \%$ which means that depolarization can disturb the signal within a range of $[0.2, 8.1]\%$. By increasing the elevation, we observe a decrease in the Monte Carlo root MSE reaching a $DoP(\%) = 96.8 \pm 1.6\%$ at zenith. Our results reach up to the same order of magnitude of error to the experimental work from Toyoshima et al [14].

7.1. Turbulence losses

Turbulence is one of the main reasons for high degree deviations (up to 10 dB) between simulations and the experimental set up. For that reason we studied the three most relevant turbulent effects seen below. Their dominance in the S/C mission is dependent on the size of beam width and the eddies size. For our mission scintillation is the most dominant effect.

7.1.1 Beam spreading

For this section we have considered three different models A [5], B [5] and C [13] for low perturbation theory, high turbulence and generalized non-Kolmogorov theory, respectively. By defining that the turbulent profile follows the $H - V_{5/7}$ model,

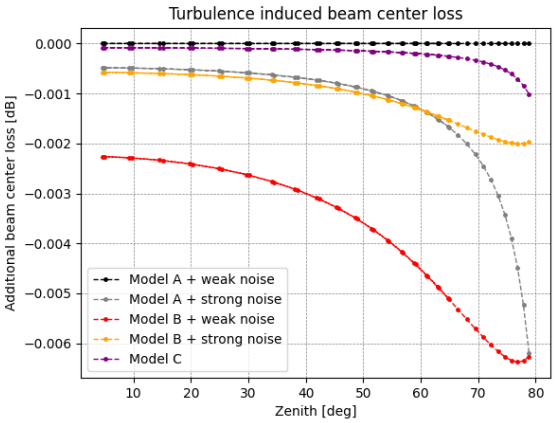

Figure 10: Additional signal loss considering different models (A, B, C) and fluctuation environments (weak and strong theories) for turbulence.

we can compute the respective added loss for the beam width as seen in Fig 10.

As seen in Fig 10, the influence from the spreading effect is minimal, only differing our results up to an order of 10^{-2} m for the beam divergence. At high zenith angles when considering a strong turbulent environment we obtain a maximum added beam width of $w_{turb} = 0.0634$ m from the turbulent influence.

7.1.2 Scintillation

Scintillation effect is described by an oscillation in the intensity of the received signal resulting in a sparkling of the target over space and time. Using weak turbulence theory, we can describe the effect with a log normal loss profile by considering an irradiance mapping at the receiver from the S/C view. Adapting it to our S/C elevation profile we obtain the intensity mapping as seen in Fig 11 at zenith.

By comparing the supposed Gaussian profile

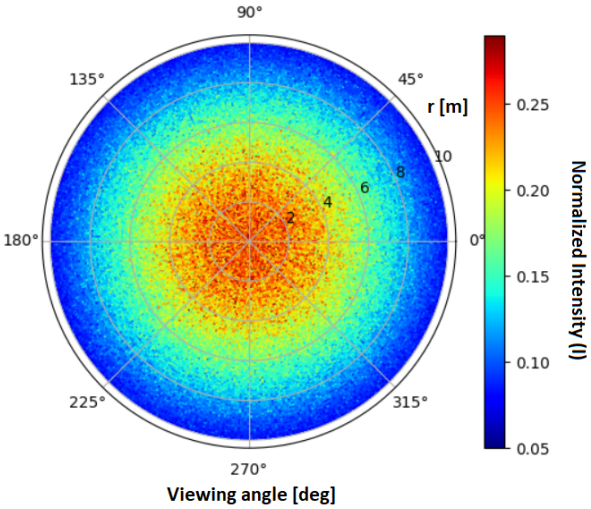

Figure 11: Normalized intensity profile with the scintillation effect viewed when S/C is at zenith right above the GS.

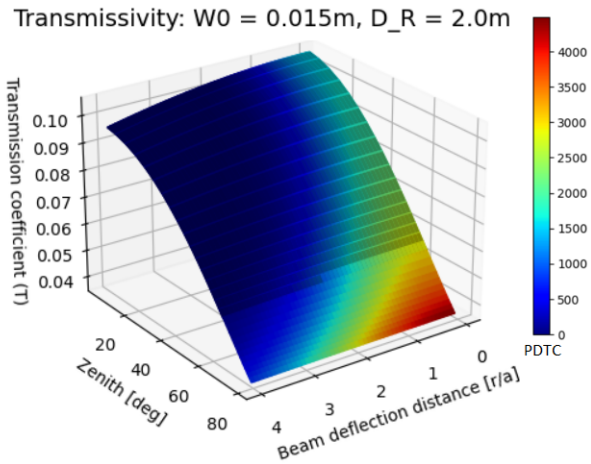

Figure 12: Transmission coefficient in terms of S/C elevation, the PDTC and deflection distance r/a.

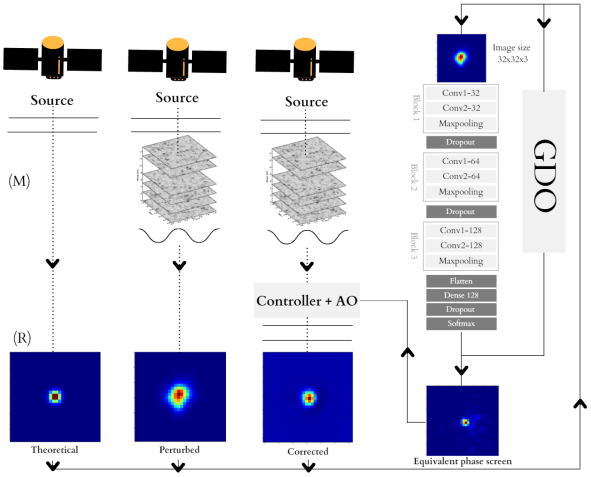

Figure 13: Schematic of the turbulence mitigating network, which is composed of adaptive optics, a source, medium with turbulence (M), a receiver (R), and a feedback network with a CNN and a GDO. The optical profiles correspond to the desired image (left), the distorted image due to turbulence (middle), and the turbulence-corrected image at the receiver (right).

with the scintillated one we obtain an error that deviates up to 30% in the total intensity.

7.1.3 Beam wandering

We also considered the effect of beam wandering which describes how the atmospheric turbulence creates time-dependent random lateral beam displacements. We have compared the S/C and turbulence induced offpointing, by usuing the Weibull distribution where its standard deviation (σ_r) is composed by both terms: $\sigma_r = \sqrt{(\theta_p L)^2 + \sigma_w^2}$. Where θ_p is the pointing error of the S/C and σ_w is the variance of the beam center due to turbulence. In weak turbulence enviroment considering a collimated beam in Kolmogorov theory with infinite outer scale, the σ_w term can be defined by $\sigma_w = 1.919 C_n^2 z^3 (2w_0)^{-\frac{1}{3}}$. Here, C_n^2 is the index structure coefficient defined by the $H - V_{5/7}$ model, z is the optical path in the atmosphere and w_0 is the beam waist when entering the atmosphere. We consider $\theta_p = 1.0\ \mu m$ from the precision of the Micius mission S/C . Thus, obtaining $(\theta_p L)^2 = 0.56 m^2 >> 10^{-3} m^2 = \sigma_W^2$. As seen the results from this effect are near to negligible.

8. PDTC model

To account for the statistical behaviour of the turbulence as well as the offpointing of the satellite, we propose to update the geometrical method to a more refined one, defined by the Probability Distribution of the Transmission Coefficient (PDTC). Considering the S/C distance profile as well as our current attenuation coefficients and following the work of D. Yu. Vasylyev et al. [15] we have obtained in Fig 12 the transmission coefficient, in terms of the satellite zenith angle, the beam deflection distance and the respective normalized probability.

We are able to apply a polynomial regression to our data for a $\mathcal{O}(3)$ order polynomial. Hence, allowing to obtain a correspondence of $\chi^2 = 9.8032 \times 10^{-04}$ and $\chi_\gamma = 2.2798 \times 10^{-05}$ for the Chi-Square and reduced Chi-Square parameters, respectively.

A mean beam deflection of $\frac{r}{a} = 0.60$ is obtained for low zenith angles increasing up to $\frac{r}{a} = 1.51$ for high zenith angles.

The results shown achieve the same order of magnitude for the transmissivity coefficent (T) being in accordance to the work of D. Yu. Vasylyev et al. [15] and Daniele Dequal et al. [3], as well as with the equivalent eliptical model for QKD from the work of Carlo Liorni et al. [7].

9. New CNN method

For this section we propose a new method for intensity profiles correction of phase-dependent pro-

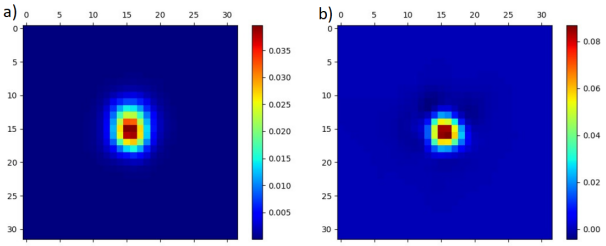

Figure 14: Target intensity pattern at the receiver: **a)** With turbulence. **b)** Corrected via Controller.

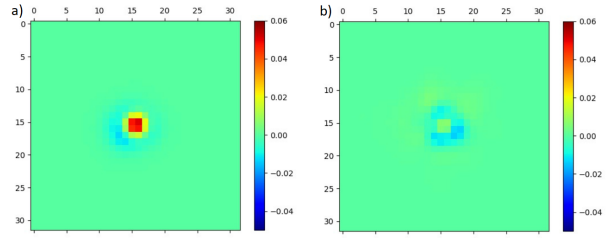

Figure 15: Target Mean Error profile compared to the theoretical Gaussian profile with no perturbations: **a)** Before correction. **b)** After correction.

tocols, which wavefront aberrates intensely due to turbulent effects. Fig 13 from left to right show the main method. We start by obtaining the intensity profile of the distorted object, and we also get the non-perturbed data from a known reference source within the same FoV of the telescope. Therefore, now we can get a theoretical profile of our reference source with low to zero signal disturbances.

Our algorithm is composed by a Convoluted Neural Network (CNN) with a Gradient Descent Optimizer (GDO) in feedback with adaptive optics. We use a CNN to obtain the strength of the turbulent layers by predicting the Rytov parameter from the deformed images of the signal, based on previously trained data. With a GDO we can obtain the exact complex number responsible for the randomness of the turbulent layer by comparing the perturbed and the theoretical intensity profiles. The turbulent profile is assumed to be composed of multiple layers, being modelled based on the work of M. J. Jee et al. [4]. Here, we use the atmospheric measurements of the site of the Gemini-South telescope located in Cerro Pachón, Chile [10].

We consider the propagation of a Gaussian beam light profile in this environment coming from our S/C to our telescope, whereby using and modifying the package Galsim [3] [11] we obtain the resulting intensity pattern at the receiver.

We test the viability of our method by computing the MSE between the theoretical and real intensity profiles obtaining $MSE_{\text{original}} = 4.42 \times 10^{-3}$ for the perturbed signal. We found that by comparing to the corrected intensity profile, the MSE ($MSE_{\text{corrected}} = 2.05 \times 10^{-4}$) improves up to an order of magnitude. Thus, such a procedure increases the signal performance from 64.61% up to 91.75% using only a training procedure with a small data set of 2000 images. Furthermore, by comparing to the state of the art methods of wavefront correction from W. Xiong et al. [16], H. Ma et al. [9] and S. Lohani et al [8] our algorithm achieves similar results for the recovery ratio but with added complexity by having a more realistic data set for the simulations, once it contains data from the simulated telescope and an improved model for the Earth's atmosphere.

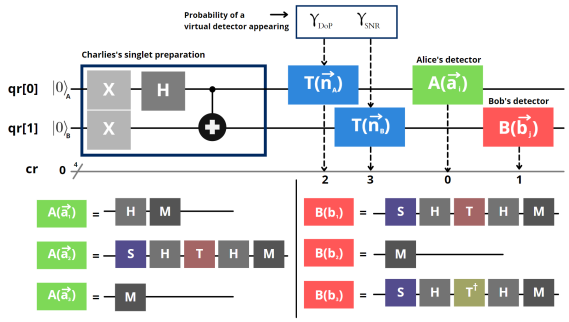

Figure 16: Schematic of the quantum circuit used for the E91 protocol. Below, with the use of quantum gates we can rotate the basis for Alice's and Bob's detection.

10. Results & discussion

E91 protocol

To simulate the E91 protocol we shall use the Qiskit Python toolbox [4], to create a modified E91 protocol which considers the depolarization and attenuation effects. As seen in Fig 16, a quantum circuit has been constructed to perform the E91 protocol and the CHSH test with the respective quantum gates presented below. The loss is introduced by imposing for each photon a probability to shift their basis, hence, acting as an additional detector between Alice and Bob.

As seen in Fig 17, with only γ_{DoP} component present we obtain a valid S parameter of $\in [-2.67 \pm 0.23, -2.44 \pm 0.04]$. By introducing the SNR our CHSH test shifts. Where the E91 protocol is only valid between $\in [46, 321]$ s.

BB84 protocol

For the BB84 protocol, to obtain the key rate, we use the overall loss rate from the different terms in the previous sections. Hence, allowing to obtain Fig 18. Fig 18 shows that the key rate for the mission reaches up to 32.1 kbit/s considering a $MPN = 0.5$. The attenuation effects greatly decrease at high turbulent zenith angles the overall signal performance reaching down to 3 kbit/s at

[3] Documentation for the 2.3 version available.

[4] Documentation for the 0.30.1 version is available.

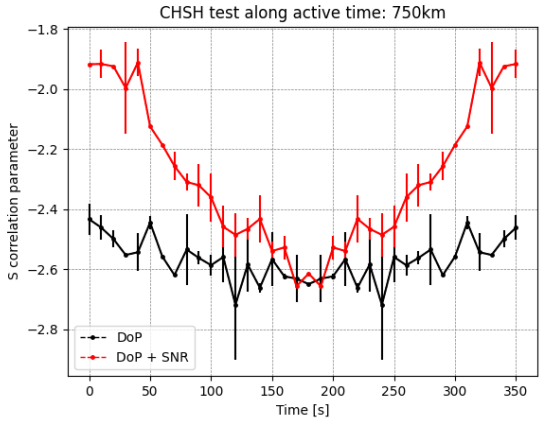

Figure 17: Correlation coefficient S during the active time of the mission. γ_{DoP} and γ_{SNR} parameters are present in order to study the vulnerability of the E91 protocol for our mission.

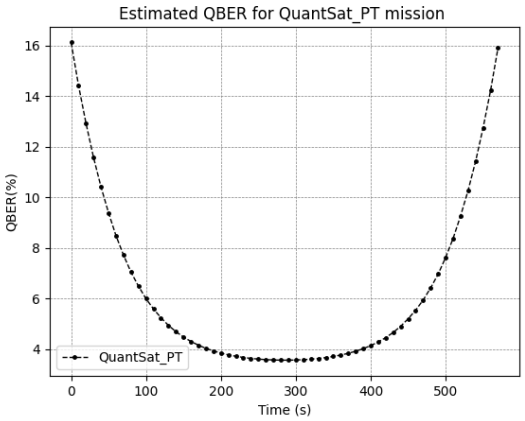

Figure 19: QBER in terms of the S/C elevation for the QuantSat-PT mission.

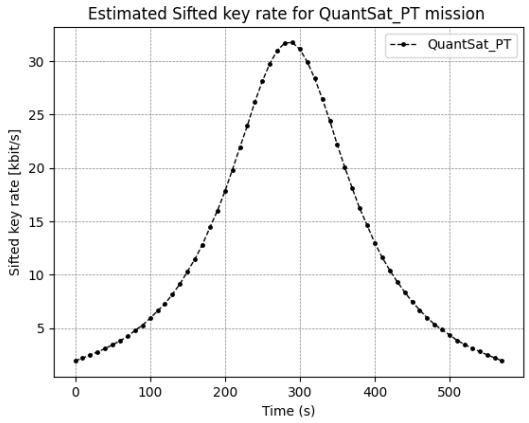

Figure 18: Sifted key rate in terms of the S/C elevation for the QuantSat-PT mission considering all losses calculated up until now for entangled based BB84 protocol.

$\theta_{zen} = 80$ deg. For the QBER we have obtained that at low zenith angles up to $\theta_{zen} = 60$ deg the quality of the BB84 protocol remains practically the same within a range of QBER$\in [3.8, 5.1]\%$. When in high turbulent environment the QBER can reach above the 11%. These results are in accordance to the work of Carlo Liorni et al. [7], J-P Bourgoin et al. [2] and Daniele Dequal et al. [3].

11. Conclusions

This work offers to solve one of the major problems in QKD space missions which is the precise consideration of environmental losses on the signal. The simulator was developed as part of the QuantSat-PT project, that aims to perform the first ever Portuguese QKD space mission on a 2U Cubesat.

In this thesis we have computed the sifted key as well as the QBER for the BB84 protocol which reach up to 32.1 kbit/s and 4% at zenith respectively for a 750 km orbit. For the E91 protocol a similar analysis was performed, however this time, the CHSH test was studied. By creating a quantum circuit for the E91 protocol, we have obtained a correlation factor of $S \in [-2.63 \pm 0.02, -1.91 \pm 0.03]$ for the mission, considering the depolarization and SNR terms. Moreover, in-depth analysis for the turbulent behaviour was performed as well as the depolarization ratio on our signal with the study of the Stokes parameters. A statistical analysis was also proposed for our mission, which considered the mean off-pointing behaviour of the satellite in a turbulent environment. Furthermore, the photon propagation along the atmosphere was simulated with MonteCarlo allowing to obtain the atmospheric transmissivity considering the absorption and Rayleigh scattering effects. At zenith we have obtained a transmissivity of $\tau_{atm} = 0.8508^{+0.0374}_{-0.0178}$. For phase-dependent protocols a new corrective method for disturbed intensity profiles is proposed with the use of a closed feedback CNN method which recovers the signal up to 93.12%.

To improve even further the simulator, we must take into account the hardware behaviour of the optical payload. Thus, by performing the hardware in loop testing we could create a more realistic model for the signal's intensity profile. This would also allow for a more robust modelling for the optical and quantum efficiencies for each optical segment which lead to a more realistic QKD performance.

In order to improve the accuracy of the night sky background behaviour, it is essential to perform a local set of measurements for the brightness of night sky in the Alqueva region. Hence, allowing to realistically calibrate the simulator considering the mean natural and artificial background noise.

For the algorithm presented in section 9, we can increase the algorithm's accuracy by studying the intrinsic brightness fluctuations of the sig-

nal's source. We carry this out, in order to better distinguish the turbulent and intrinsic behaviour of the source. This algorithm, not only is pivotal for phase-dependent protocols but can also be applied for extra-planetary observation missions, which could significantly improve the image quality of faraway objects, helping in that way possible optical systems on board the satellite's telescope.

References

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, and et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, Oct 2019.

[2] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, feb 2013.

[3] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):3, Jan 2021.

[4] M. J. Jee and J. A. Tyson. Toward precision lsst weak-lensing measurement. i. impacts of atmospheric turbulence and optical aberration. *Publications of the Astronomical Society of the Pacific*, 123(903):596–614, 2021/08/21/ 2011. Full publication date: May 2011.

[5] H. Kaushal and G. Kaddoum. Optical communication in space: Challenges and mitigation techniques. *IEEE Communications Surveys Tutorials*, 19:57–96, 08 2016.

[6] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, Sep 2017.

[7] C. Liorni, H. Kampermann, and D. Bruß. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New Journal of Physics*, 21(9):093055, sep 2019.

[8] S. Lohani and R. T. Glasser. Turbulence correction with artificial neural networks. *Opt. Lett.*, 43(11):2611–2614, Jun 2018.

[9] H. Ma, H. Liu, Y. Qiao, X. Li, and W. Zhang. Numerical study of adaptive optics compensation based on convolutional neural networks. *Optics Communications*, 433:283–289, 2019.

[10] F. Rigaut and et al. Gemini multiconjugate adaptive optics system review – I. Design, trade-offs and integration. *Monthly Notices of the Royal Astronomical Society*, 437(3):2361–2375, 11 2013.

[11] B. Rowe, M. Jarvis, R. Mandelbaum, G. M. Bernstein, J. Bosch, M. Simet, J. E. Meyers, T. Kacprzak, R. Nakajima, J. Zuntz, and et al. Galsim: The modular galaxy image simulation toolkit, Jun 2018.

[12] 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*, 11(8):502–508, Aug 2017.

[13] I. Toselli, L. Andrews, R. Phillips, and V. Ferrero. Free space optical system performance for laser beam propagation through non kolmogorov turbulence for uplink and downlink paths. *Proceedings of SPIE - The International Society for Optical Engineering*, 10 2007.

[14] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, Y. Koyama, and H. Kunimori. Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space. *Opt. Express*, 17(25):22333–22340, Dec 2009.

[15] D. Y. Vasylyev, A. A. Semenov, and W. Vogel. Toward global quantum communication: Beam wandering preserves nonclassicality. *Physical Review Letters*, 108(22), Jun 2012.

[16] W. Xiong, D. Fan, P. Wang, M. Cheng, J. Liu, Y. He, X. Zhou, J. Xiao, Y. Li, and S. Chen. Convolutional neural network based atmospheric turbulence compensation for optical orbital angular momentum multiplexing. *Journal of Lightwave Technology*, PP:1–1, 01 2020.