International Conference on Space Optics—ICSO 2022

Dubrovnik, Croatia

3–7 October 2022

Edited by Kyriaki Minoglou, Nikos Karafolas, and Bruno Cugny,

MEO Satellite-to-Ground Decoy-State QKD links Realistic Performance Analysis

MEO Satellite-to-Ground Decoy-State QKD links
Realistic Performance Analysis

Argiris Ntanos[1,2], Nikolaos K. Lyras[1,2], Dimitris Zavitsanos[1,2], Saif Anwar[3], Obada Alia[3], Giannis Giannoulis[1,2], George Kanellos[3], Athanasios D. Panagopoulos[1,2], Hercules Avramopoulos[1,2]

[1]School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece
[2]Institute of Communication and Computer Systems, Athens, Greece
[3]High Performance Network Group, School of Computer Science, Electrical & Electronic Engineering and Engineering Maths (SCEEM), University of Bristol, UK

email: ntanosargiris@mail.ntua.gr, lyrasnikos@mail.ntua.gr, dimizavitsanos@mail.ntua.gr, Saif.Anwar@warwick.ac.uk, obada.alia@bristol.ac.uk, jgiannou@mail.ntua.gr, gt.kanellos@bristol.ac.uk thpanag@ece.ntua.gr, hav@mail.ntua.gr

Abstract-In this study a feasibility analysis of a satellite-to-ground QKD link employing the Decoy-State BB84 protocol for both LEO and MEO satellite constellations is presented. Considering realistic atmospheric conditions and system assumptions, a comparison of the QKD performance between low and medium satellite orbits over an existing OGS network is reported.

1. INTRODUCTION

Quantum Key Distribution (QKD) as a method of sharing symmetric cryptographic keys between two different end users gains more and more momentum. Since long-distance QKD links are limited due to the exponential loss that light encounters while travelling in optical fibers, satellite-based free space optical links seem to be a promising alternative, allowing for improved loss-distance scaling [1]. Towards global scale quantum secured networks, the long-term vision that should be pursued is to integrate the terrestrial Quantum Communication Infrastructure (QCI) with a space one, where quantum computers, simulators and sensors are interconnected via quantum communication networks [2]. Recent research focusing on Low Earth Orbit (LEO) satellite-to-ground QKD has proven the feasibility of such links with high Secure Key Rates (SKR) [3-8], whereas experimental QKD downlink demonstrations have already been successfully performed [9-12]. Even though LEO satellite links provide a better Signal-to-Noise Ratio (SNR), resulting in higher SKRs, Medium Earth Orbit (MEO) satellites, providing an enhanced visibility time window of approximately one hour contact time per MEO satellite [13], might be able to overcome some weak aspects of LEO QKD downlinks, such as the time demanding QKD initialization process and the finite key size effect. Although an experimental demonstration of MEO to Ground QKD link have not been performed yet, studies that focus on the feasibility of such links as well as single photon exchange from medium Earth orbits have been presented [14-16].

We contribute to the above research direction by presenting a MEO satellite-to-ground QKD feasibility analysis for two proposed wavelengths (1550nm, 800nm). In addition, a comparison between LEO and MEO satellite QKD downlinks is discussed by considering in both cases either a single satellite or a satellite constellation. As Optical Ground Station (OGS) terminals three observatories located across Greece which

participate in the European Quantum Communication Infrastructure (EuroQCI) initiative and one observatory located in Spain, Tenerife, are investigated [17]. The atmospheric channel is modeled under nighttime conditions to ensure a low background noise in the receiver, taking into consideration various atmospheric effects such as turbulence and cloud presence, whereas the locations of the LEO and MEO satellites are provided by a developed Python based software tool [19]. The performance of the link is evaluated by employing the Decoy-State BB84 QKD protocol [20] in terms of SKR and total number of distilled yearly key bits. The obtained numerical results confirm that MEO satellites could under certain conditions provide an alternative regarding satellite-to-ground QKD downlinks. Employing the Decoy-State QKD protocol up to 2.88Gbits of secret keys can be distilled over the period of one year between a MEO satellite constellation of 10 satellites and an OGS.

This paper is organized as follows. In Section II, the LEO and MEO satellite constellation's physical structure and the OGS network are briefly presented. Section III provides the overall system architecture, the modeling of the satellite-to-ground QKD downlink, as well as the assumptions for the BB84 Decoy-State QKD protocol. Section IV provides the selection and optimization of the setup components as well the results of this work. Finally, sections V and VI discuss and conclude this work.

2. SATELLITE CONSTELLATION AND OGS ASSUMPTIONS

This study focuses on both low and medium Earth orbits to support the distillation of symmetric encryption keys on optical ground terminals located on Earth. Since LEO satellite QKD downlinks have been thoroughly examined the past few years [3-12], it seems as a natural step to investigate the feasibility and the required conditions of a MEO-to-ground satellite QKD link. LEO satellites provide an enhanced SNR compared to higher orbits, which is an attractive advantage for a QKD link, especially due to minimized free space losses. On the other hand, they exhibit a much shorter visibility time window per satellite, resulting to a need of larger satellite constellations to achieve a continuous communication with at least one satellite at a time. This would not only require for each satellite to be equipped with QKD equipment, but also that the initialization of the QKD link should be realized multiple times every hour. This could be a serious issue for various QKD systems that require several minutes only to initialize the QKD link before the key distillation procedure can begin [11]. On the contrary, MEO satellites have a much broader visibility time window and can therefore provide continuous communications with less satellites employed.

To model the physical parameters and characteristics of the LEO and MEO satellite constellations a V-Python based software tool, which is briefly presented in [17], has been used. By using this software tool, the position of each satellite at any given time can be provided for various orbital heights and inclination of orbital planes. For the modelling of the LEO satellite constellation an orbital inclination of 53° was used with all satellites orbiting at an altitude of 550km. In the results a full constellation of up to one hundred satellites orbiting at ten different orbital planes (ten satellites per orbital plane) is examined. An extended work regarding this large-scale LEO satellite constellation is presented in [17]. For the modeling of the MEO satellites an orbital height of 8063km, with an inclination angle of 0.1^o, similar to the O3b constellation was selected. In the results a full constellation of up to ten satellites over a single orbital plane is examined. Finally, the QKD sender station was selected to be located in the satellite nodes, since the Alice components are usually less complex and bulky than Single Photon Detectors (SPDs) which are required in the receiver's side. The Space segment also establishes classical communication channels (radio frequency or optical) between the satellite and the OGSs for related protocol data exchange [18].

For the reception of the weak coherent states prepared at satellite payload, three

optical ground terminals located across Greece and one in Spain were selected for the needs of our study. The three stations located in Greece also participate in the European Quantum Communication Infrastructure Initiative (Euro-QCI) which focuses on constructing a single European QKD network that spans across various countries in Europe [21,22]. The OGS are located in astronomical observatories which in turn are located far from terrestrial infrastructure and can therefore provide a low background noise radiance which can enhance the SNR of the received quantum signal. Figure 1.a. depicts the location of these OGS and Figure 1.b. shows the elevation angle at which both a LEO and a MEO satellite are seen for a single pass over the Helmos national astronomical observatory, one of the darkest areas in Greece and Europe [23].
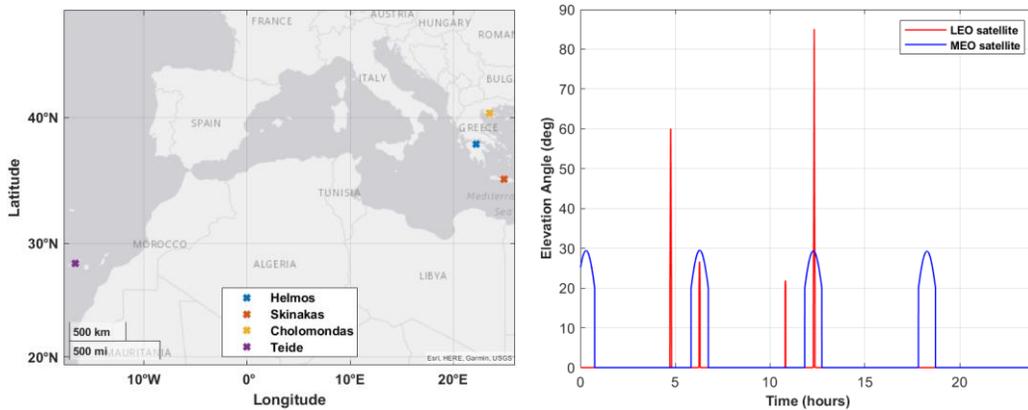

Fig 1. a) Location of the four OGS across Europe. b) Elevation of a single LEO and MEO satellite over 24 hours over the OGS of Helmos.

It is evident by figure 1.b) that a MEO satellite is visible with approximately the same elevation angle at each pass whereas a LEO satellite may appear a different path, resulting in a variation in the elevation angle over time. Finally, the details of the location, altitude of each station as well as the telescope aperture diameter that were assumed are given in Table I.

TABLE I.   OGSs CHARACTERISTICS

#	Ground Station	Country	Latitude, Longitude	Altitude(m)	Aperture diameter(m)
1	Helmos	Greece	37.98, 22.20	2340	2.28
2	Skinakas	Greece	35.21, 24.89	1750	1.3
3	Cholomondas	Greece	40.34, 23.50	850	1.2
4	Teide	Spain	28.29, -16.51	2390	1.52

3. ATMOSPHERIC CHANNEL MODELING AND QKD PROTOCOL

This section provides the formulas that were used for the modeling of both LEO and MEO satellite downlink.

3.1 CFLOS Probability

Cloud presence is one of the main attenuation mechanisms in optical communications which can drastically deteriorate or completely interrupt the transmission of the optical signal [24,25]. Since quantum pulses contain mean intensities of sub-photon level, it is assumed that any cloud presence automatically stops the signal transmission and therefore the distillation of the SKR. To estimate the Cloud Free Line of Site (CFLOS) probability, cloud coverage statistics from ECMWF database over 4 years (2012-2015) are used. The

CFLOS probability is calculated by using the methodology reported in [24,25]. For the four selected OGSs the CFLOS is provided in Table II.

TABLE II.   CFLOS PROBABILITIES PER OGS

#	Ground Station	Country	CFLOS
1	Helmos	Greece	0.625
2	Skinakas	Greece	0.723
3	Cholomondas	Greece	0.3178
4	Teide	Spain	0.813

3.2. Geometrical loss

Geometrical loss increases quadratically as the distance increases. For an orbiting satellite, the satellite to ground distance is dependent on the elevation angle of the satellite and can be calculated according to [26]:

$$d(\theta) = R_e \left(\sqrt{\left(\frac{H + R_e}{R_e}\right)^2 - \cos^2\theta} - \sin\theta \right) \tag{1}$$

,where H(m) is the satellite's altitude above Earth's surface, R_e (m) is the Earth's radius and θ (rad) is the elevation angle. To counter the high loss due to the long satellite to ground links, especially for the case of MEO satellites, large telescope apertures should be employed both in the transmitter and receiver side. The geometrical loss factor can be calculated according to the following expression [27,28]:

$$A_{geo} = \left(\frac{\lambda}{4\pi\, d(\theta)}\right)^2 \times \left(\frac{\pi\, D_r}{\lambda}\right)^2 \times \left(\frac{8}{w_0^2}\right) \tag{2}$$

,where Dr (m) is the receiver's aperture diameter, $w_0 = 2\lambda/\pi\, D_t$ is the half-width beam divergence angle (rad) for a gaussian beam, Dt (m) is the transmitter's aperture diameter and λ is the wavelength of the transmitted signal.

3.3 Pointing loss

The satellite tracking inaccuracy results in an additional pointing loss. To estimate the pointing loss, the Probability Density Function (PDF) of the received intensity is estimated as follows [29,30]:

$$p(I_{pp}) = \beta_p \bar{I}_{pp}^{\,\beta_p - 1}, 0 \leq I_{pp} \leq 1 \tag{3}$$

,where $\bar{I}_{pp} = \beta_p/(\beta_p + 1)$ and $\beta_p = w_0^2/4\,\sigma_p^2$ is the divergence pointing ratio, where w_0 is the half-width divergence angle of the transmitted beam commuted for Gaussian beams and σ_p (rad) is the pointing error variance. The total pointing error loss is calculated for a specific outage probability p_0 according to the following expression [29]:

$$\boldsymbol{L_{pt} = p_0^{\,1/\beta_p}} \tag{4}$$

3.4 Atmospheric transmission

The atmospheric transmittance is also dependent on the elevation angle of the satellite, since for low elevation angles the signal must travel a longer path through the atmosphere. The atmospheric transmittance can be calculated according to the following expression [28,30]:

$$L_a = L_{zen}^{\left(\frac{1}{cos(\zeta)}\right)} \tag{5}$$

,where L_{zen} is the vertical link transmittance for a particular wavelength and ζ (rad) is the zenith angle of the link.

3.5 Scintillation Effect

The effect of scintillation can often deteriorate optical communications by causing fluctuations in the received intensity. This effect is mitigated when larger apertures are employed. The strength of the effect is characterized by the value of refractive index structure parameter Cn^2 $(m^{-2/3})$ as weak, moderate, and strong. In this study the case of weak and moderate turbulence has been taken into consideration. In this case, the fluctuation of the intensity in the receiver can be modeled by the log-normal distribution. The value of the refractive index structure parameter has been calculated according to the Hufnagel-Valley model, by taking into account the altitude of the OGS, as described in [27,31]. The dependence of the scintillation effect to the elevation angle of the link is expressed by the Rytov index which can be calculated as follows [31]:

$$\sigma_R^2 = 2.25 k^{\frac{7}{6}} sec^{\frac{11}{6}}(\zeta) \int_{H_{GS}}^{H_{Turb}} C_n^2(h)(h - H_{GS})^{\frac{5}{6}} dh \tag{6}$$

,where ζ (rad) is the zenith angle, k (rad/m) is the wavenumber, H_{gs} (m) is the OGS altitude and H_{turb} (m) is the turbulence altitude which is set to be 20km. For altitudes higher than 20km, the effect of turbulence can be neglected. The loss in dB due to the effect of turbulence for a given outage probability p_o is calculated according to the Kolmogorov model by including the aperture averaging effect as follows [32]:

$$L_{sci} = 4.343[erf^{-1}(2p_0 - 1)[2 ln(\sigma^2_I + 1)]^{\frac{1}{2}} - \frac{1}{2} ln(\sigma^2_I + 1)] \tag{7}$$

,where σ_I^2 corresponds to the scintillation index for a plane wave approximation [27,31].

3.6 Background Radiance

Since the selected OGSs are located away from the terrestrial environment, it is considered that the background radiance noise that enters the detector is generated by the sky radiance. The background noise power level that is inserted in the detector after fist being filtered in frequency is given in Watt by the following expression [28,33]:

$$P_{back} = H_{rad} \times \Omega_{FOV} \times A_r \times \Delta\lambda \tag{8}$$

where H_{rad} $(W/m^2 sr\ \mu m)$ corresponds to the background radiance energy density, Ω_{FOV} (sr) is the telescope's Field of View (FOV), A_r (m) is the telescope's capture area and $\Delta\lambda$ (μm) is the receiver's band pass optical filter width. The background noise power level is converted into single photon counts per second (cps) and then multiplied by the detectors effective gate opening to result in a probability of receiving a background noise count per gate opening as follows:

$$P_{noise} = t_{gate} \times cps_{background} = t_{gate\times}\left(\frac{P_{back}}{h \times f}\right) \tag{9}$$

,where t_{gate} is the effective gate duration time of the single photon detector and $h \times f$ corresponds to the energy of a single photon of frequency f. It is evident by equation (8) that reducing the duration of the SPD's gate can act as temporal filtering, therefore improving the SNR of the photon signal detection.

3.7 Decoy-State QKD Protocol

In this study the DV-QKD Weak-Vacuum Decoy State BB84 Protocol was used. Whereas the theoretical unconditional security of the BB84 protocol has been proven [34], additional security enhancements should be considered when moving towards real life implementations. To tackle the Photon Number Splitting (PNS) attacks the decoy states are introduced, affording therefore higher mean photon numbers per pulse [20,35]. The normalized SKR (*bps/pulse*) is lower bounded by the following inequation [20]:

$$\frac{SKR}{f_{rep}} \geq q\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu)\} \tag{10}$$

,where q is the protocol efficiency, the subscript μ is the average photon number per signal in signal states, Q_μ and E_μ are the gain and the Quantum Bit Error Rate (QBER) of signal states, respectively, Q_1 and e_1 are the gain and the error rate of the single photon state in signal states, respectively, $f(x)$ is the bi-directional error correction rate and $H_2(x)$ is the binary entropy function.

To continue, considering the finite post processing block size, statistical fluctuations of the visibility have been included. The noise rate is expressed in terms of noise photons per gate duration time. For the calculation of the SKR, we assumed security against restricted collective attacks and followed the methodology reported in [36,37]:

$$SKR \geq f_{rep} \times q\left\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu) - \frac{\Delta}{N_s}\right\} \times \eta_{dead} \tag{11}$$

,where η_{dead} accounts for the reduced detection rate due to SPADs dead time [38], $f(E_\mu)$ accounts for the non-ideal error correction efficiency and N_s for the total number of transmitted signal states, whereas the value of Δ is calculated to be [36]:

$$\Delta = 7 \times \sqrt{N_n \times \log_2\left(\frac{2}{\varepsilon_s - \varepsilon_{pe}}\right)} + 2 \times \log_2\left(\frac{1}{2 \times (\varepsilon - \varepsilon_s - \varepsilon_{ec})}\right) \tag{12}$$

Where N_n is the total number of received signal states and $\varepsilon_s, \varepsilon_{pe}, \varepsilon_{ec}, \varepsilon$ account for the smoothing parameter, parameter estimation parameter, the error correction parameter, and the overall security of the final key parameter respectively.

4. SIMULATION ASSUMPTIONS AND RESULTS

4.1 Simulation Assumptions

In this study, only the downlink case was taken into consideration. The wavelengths of 1550nm and 800nm were examined, which exhibit a good atmospheric transmittance window, with an overall vertical transmittance calculated to be 0.8 and 0.6 respectively according to MODTRAN tool, under good atmospheric visibility conditions [39]. To emulate the effect of turbulence, the refractive index structure parameter on the ground level was set to be 1.7×10^{-14} $(m^{-2/3})$ and the wind speed on ground level to be $10 m/s$. Since only the link is assumed to be operating at nigh-time conditions, the background sky radiance was set to be 1.5×10^{-4} $(W/m^2 sr\,\mu m)$ and 1.5×10^{-5} $(W/m^2 sr\,\mu m)$ at 800nm and 1550nm respectively, which accounts for new moon and clear sky conditions [4,33,40,41].

The satellite nodes are assumed to be equipped with a 200mm telescope aperture transmitter. For the calculation of both pointing loss and turbulence loss the outage probability was set to be 1%, whereas the pointing error variance was set to be 0.6µrad [42]. Finally, the QKD communication was assumed possible only at elevation angles greater than 20 degrees.

On the OGS side, the receiver telescope apertures that were assumed are mentioned in Section 2 and vary between 1.2m and 2.28m, whereas the receiver's telescope FOV was assumed to be reduced to 100µrad as suggested in [5,7], to minimize the effect of the background sky radiance and improve the overall SNR. Regarding the single photon detection, Superconducting Nanowires Single Photon Detectors (SNSPDs) were assumed, with detection efficiencies at 0.85/0.9, dead time at 25/10ns and dark count rate (DCR) of 250/10cps at 1550nm and 800nm respectively [43]. The gate duration time was set to be 1ns and the detector's interferometer visibility was set to 98%. The optical signal is assumed to be coupled into an optical fiber and being filtered with a narrowband optical wavelength bandpass filter with a passband of 0.2nm and 1.5dB insertion loss before entering the SNSPDs [44]. The telescope-fiber coupling efficiency was set to 30% [45]. Finally, an additional 1.5dB loss is considered as detector's setup loss.

Regarding the Decoy-State BB84 parameters, the mean signal and mean decoy photon number were optimized respectively considering the overall link transmittance [20], whereas the signal: decoy: vacuum ratio was set to 2:1:1 [12], resulting in an overall protocol efficiency q=1/4 [20]. To continue, the bi-direction error correction efficiency was set to 1.22. Finally, to account the finite key size effect the smoothing parameter was set to 9×10^{-11}, the parameter estimation parameter to 7.7×10^{-11} the error correction parameter to 8×10^{-11} resulting to an overall security of the final key to 2.47×10^{-10}[46].

4.2 MEO Feasibility Analysis

Since the LEO-to-ground satellite QKD links have been extensively studied, this section focuses on the feasibility analysis of a MEO-to-ground satellite QKD link. For this section the finite key size effect was neglected. Since the simulated MEO satellite constellation orbits around the equator, the resulting elevation angle exhibits an upper limit for every individual station. For OGSs located North the resulting maximum elevation angle is smaller as it is depicted in Figure 2.
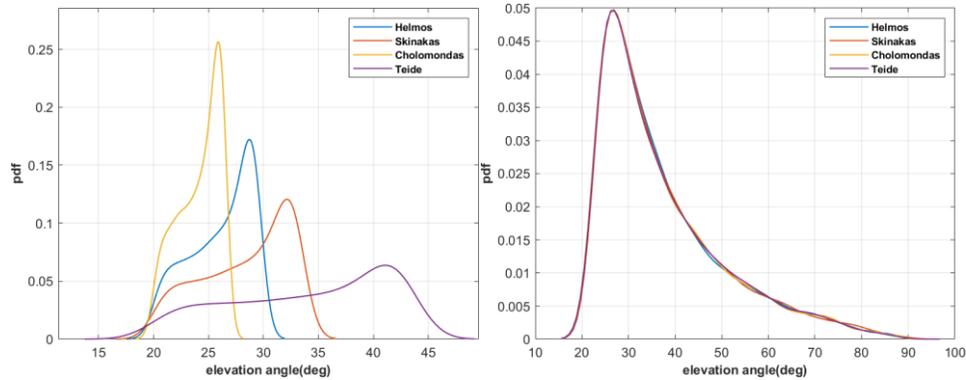
Fig 2. PDF of the elevation angles for various OGSs for a) MEO satellite constellation and b) LEO satellite constellation.

At low elevation angles (e.g., 20°) the Line Of Sight (LOS) distance between the OGS and the satellite can reach up to around 10900 km. To compensate the increased geometrical loss, large telescope apertures need to be employed in the optical ground terminals. Figure 3 depicts the resulting SKR at elevation angles between 20 and 45 degrees for various receiver aperture dimeters at 1550nm and 800nm respectively.
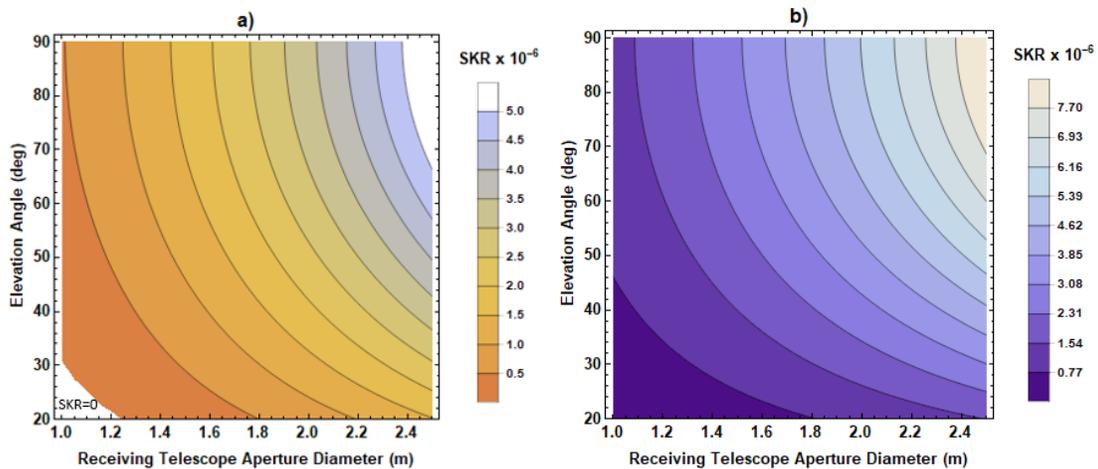

Fig 3. Calculated SKR for a MEO-to-ground link over elevation angle over receiving telescope aperture diameter for a) 1550nm and b) 800nm.

It is evident by Figure 3, that apertures larger than 1.2m are necessary to achieve positive key rates at 1550nm in MEO satellite-to-ground transmission, for the given assumptions. The main cause of the resulting relatively low normalized SKR values is the increased geometrical loss. The minimum and maximum values of the geometrical loss only, for a receiver telescope aperture diameter of 1.5m is calculated, at elevations $20^o - 45^o - 90^0$, to be 34.1-32.6-31.5dB and 28.4-26.9-25.7dB at 1550nm and 800nm respectively. It should be noted that in the current simulation the satellite-OGS LOS distance will be limited to no less than 9200km since the maximum elevation angle that is provided for the selected OGSs is limited to less than 45 degrees (Teide observatory, Tenerife, Spain).

4.3 LEO and MEO Satellite Constellation Performance

In this section the results of the LEO and MEO QKD downlinks over the period of one year are presented in terms of SKR and distilled key bits. During this section it is assumed that for every different satellite-OGS QKD communication an initialization procedure with a duration of 120s precedes, during which the satellite is being tracked and the QKD system is initialized. Furthermore, it is calculated that at least a total number of $N = 3 \times 10^5$ bits need to be exchanged to achieve positive key rates. In general, for every LEO satellite pass

that lasts less than one minute (plus 120s for the initialization stage) the QKD was considered inactive, since the key distillation would have been marginal. Considering this, and by assuming an Alice's repetition rate of 200Mhz, a minimum total number of 12×10^9 bits can be transmitted during a LEO satellite pass, which considering an overall link efficiency of about $10^{-3} - 10^{-4}$ [8] is sufficient to reach a total number of exchanged bits greater than 3×10^5. In the case of MEO-to-ground communication, since the visibility time window is approximately 50 minutes a total number of 6×10^{11} bits can be transmitted, once again assuming a link efficiency of about $10^{-4} - 10^{-5}$ are sufficient to reach the block size limit of 3×10^5 bits.

In the current study it is assumed that every satellite and every OGS is equipped with only one transmitting/receiving telescope respectively. At the time instances when multiple LEO satellites are simultaneously visible by an OGS, the satellite with the higher elevation angle is selected for the QKD communication.

The LEO satellites are visible by the OGSs in various elevation angles at every pass, whereas the MEO satellites are visible with the same elevation angle every time. Figure 4 presents the resulting normalized SKR (bps/f_{rep}) of pass of a 10 MEO and 100 LEO constellation over time.
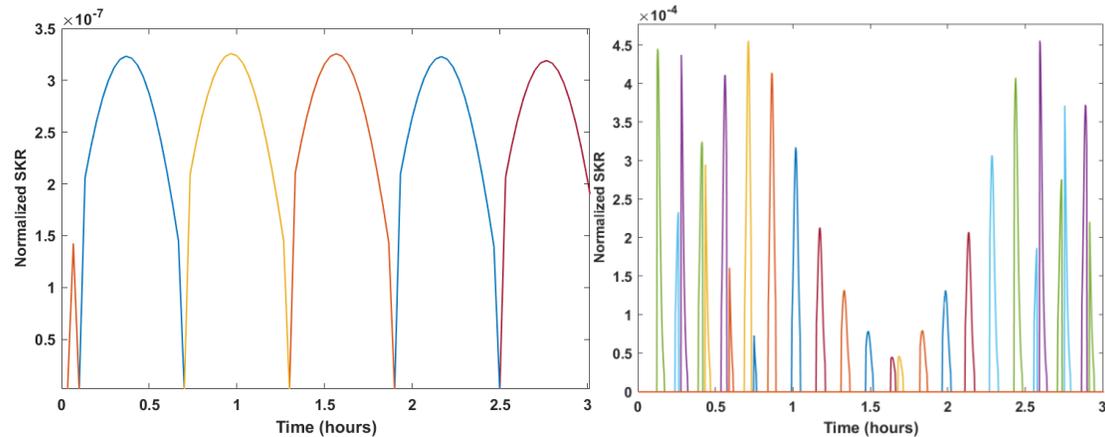

Fig. 4. Calculated normalized SKR over time for a) constellation of 10 MEO satellites and b) constellation of 100 LEO satellites (only part of the consetllation is visible in the current figure) over three hours over the OGS of Skinakas.

Different colors in Figure 4. account for different satellite-to-ground links. As it is evident MEO satellites are able to provide a full-time coverage with ten times less satellite nodes, since they offer a much larger visibility time window of approximately one hour. Assuming a transmitter repetition rate of 200Mhz, the resulting SKR is calculated to be in the order of tens of bps. On the other hand, LEO satellites can momentarily (for a limited time) distill up to 10^3 times higher key rates and can offer a bigger volume of distilled keys over the same period. To better compare the magnitude of secret key that are exchanged employing LEO and MEO satellites, the Gbits of distill secret keys are presented in Table III and Table IV over the period of one year. For this case we examine the keys that are produced with constellations of up to 10 MEO satellites and up to 100 LEO satellites.

TABLE III.   NUMBER OF YEARLY DISTILLED SECRET KEY GBITS AT 1550NM

OGS	# of sat. Orbit	1	10	100
Helmos	LEO	4.15	38.1	244
	MEO	0.4	2.88	-
Skinakas	LEO	1.25	11.4	86
	MEO	0.05	0.43	-
Cholomondas	LEO	1.05	9.55	71.9
	MEO	0	0	-
Teide	LEO	1.71	15.6	153
	MEO	0.28	1.84	-

It is evident by table III, that the total distilled Gbits of secure key for MEO satellites is at about one order of magnitude lower compared to LEO satellites when employing large telescope apertures as it is evident in the case of Helmos OGS. For relatively smaller telescope apertures, and specifically for the OGS of Cholomondas which is located North, thus providing a much lower average elevation angle, the resulting SKR is zero at 1550nm. On the other hand, for OGS that are located South, (Teide, Tenerife, Spain in our case) the volume of the resulting distilled Gbits for MEO satellite is only about six times lower compared to LEO satellites. By employing a telescope aperture that is 0.76m smaller than the telescope aperture diameter that is used in the OGS of Helmos, Teide observatory can distill up to 70% the volume of the keys that are distilled in Helmos, whereas Skinakas OGS, employing a similar receiver telescope diameter can only distill about 13% the volume of Gbits distilled at Helmos.

Table IV provides the calculated amount of the distilled Gbits of secure key over a period of one year for the four selected OGSs for the wavelength of 800nm.

TABLE IV.   NUMBER OF YEARLY DISTILLED SECRET KEY GBITS AT 800NM

OGS	# of sat. Orbit	1	10	100
Helmos	LEO	5.27	47.7	359
	MEO	0.14	1.32	-
Skinakas	LEO	1.61	14.4	123
	MEO	0.07	0.59	-
Cholomondas	LEO	1.35	12.1	103
	MEO	0.01	0.04	-
Teide	LEO	2.19	19.7	175
	MEO	0.29	2.18	-

The results provided in Table IV indicate a slight improvement for both orbits and especially for the case of LEO-to-ground satellite links. This improvement is observed due to the increased divergence of the laser beam when using a shorter wavelength, which in turn leads to a reduction of the geometrical loss. Surprisingly, the overall distilled Gbits for the case of Helmos OGS were reduced, whereas the result for the rest OGSs was improved. This is a result of the increased background solar radiance at the wavelength of 800nm. Since the OGS of Helmos employs a very large telescope, the amount of background noise that enters the detector, according to equation (8), is drastically increased, thus increasing the overall QBER. This side-effect could be mitigated by either narrowing the optical filters passband or by reducing the detectors gate duration time, which can act as temporal filtering. Finally, it is once again, it is evident by Table III, that for the case of MEO-to-ground QKD, OGSs that are located relatively North are barely able to distill any

keys, whereas OGSs located South provide a much better performance.

5. DISCUSSION

In this study, a feasibility analysis of MEO satellite-to-ground QKD was presented along with a comparison with LEO satellite QKD downlinks. Despite that a clear advantage in low orbits is observed, medium orbits can offer a few benefits such as that a smaller number of satellites is required to establish continuous communication, therefore less QKD nodes are sent into space. In turn, the initialization procedure only takes place approximately every one hour, unlike the case of LEO QKD, for which this procedure needs to be realized every several minutes. Furthermore, tracking the many fast-moving LEO satellites might be a challenge for large telescopes that are mainly developed for astronomical purposes [21]. Although the resulting SKR for the MEO satellite-to-ground QKD links is relatively low, it can be sufficient to support the refresh time required when the keys are fed to an AES-256-bit encryption engines [47].

To continue, MEO satellite-to-ground QKD becomes much more efficient when the satellite communicates with OGSs that are located close to the equator. Similarly to Tables III and IV, Table V provides an additional comparison of the total number of the distilled shared key Gbits between a single LEO and a single MEO satellite and three additional OGSs over the period of one year [48]. For the results presented in Table V, a receiving telescope aperture diameter of 1.5m, was assumed for all stations whereas the CFLOS probability was neglected.

TABLE V.   NUMBER OF YEARLY DISTILLED SECRET KEY GBITS AT 1550/800NM

#	Ground Station	Country	Latitude, Longitude	Altitude (m)	Max elev. (deg)	Distilled Gbits LEO 1550/800nm	Distilled Gbits MEO 1550/800nm
1	Singapore	Singapore	1.35, 103.82	55	87.68	1.35/1.7	0.7/0.96
2	Kourou	French Guiana	5.16, -52.65	15	80.94	1.44/1.82	0.69/0.93
3	Panama	Panama	8.54, -80.78	1057	74.97	1.42/1.79	0.67/0.89

The three OGSs that are given on Table V are located closer to the equator offering a much better elevation angle when the MEO satellites are considered, thus enhancing the performance of satellite-to-ground QKD links. Comparing the resulting total volume of distilled Gbits between the two orbits, it is observed that LEO satellites could distill just 1.7 to 2.1 times more key bits compared to MEO satellites depending on the OGSs position. By selecting several system components - such as the transmitter telescope aperture diameter (i.e., 300mm aperture) and pointing accuracy - the overall MEO-to-ground link loss can be further reduced, allowing thereby for increased SKR for the MEO QKD links. By combining this set of parameters with a larger OGS network, MEO QKD links can be a competitive approach compared to LEO QKD links. The above architecture should be further investigated in a larger OGS network to export complete conclusions.

6. CONCLUSION

To conclude, this study aims to contribute towards a broader investigation of the applicability of QKD systems in MEO constellations. A feasibility analysis of MEO and LEO constellation-to-ground QKD has been presented. By modeling both the satellite constellation orbits as well the atmospheric channel including various phenomena such as

cloud presence and turbulence, we numerically estimated the performance of the QKD downlinks for both satellite orbits over four different OGSs. Considering MEO satellites, QKD has proven to be feasible, under nighttime conditions providing an adequate performance which is enhanced if the OGS is located closer to the equator. A comparative study between low and medium Earth orbits has been presented, the outcome of which showed that similar performance can be obtained both by LEO and MEO QKD links. The results are reported in terms of annually distilled key Gbits per ground station.

ACKNOWLEDGMENT

REFERENCES

1. Bedington, R., Arrazola, J.M. & Ling, A. Progress in satellite quantum key distribution.npj Quantum Inf 3, 30 (2017).
2. Kaltenbaek, Rainer, et al. "Quantum technologies in space." Experimental Astronomy 51.3 (2021): 1677-1694.
3. Takenaka, H., Carrasco-Casado, A., Fujiwara, M. et al. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. Nature Photon 11, 502–508 (2017).
4. Bonato, C.; Tomaello, A.; Da Deppo, V.; Naletto, G.; Villoresi, P. Feasibility of satellite quantum key distribution. New J. Phys. 2009, 11, 045017.
5. Tomaello, A.; Bonato, C.; Da Deppo, V.; Naletto, G.; Villoresi, P. Link budget and background noise for satellite quantum key distribution. Adv. Space Res. 2011, 47, 802–810.
6. Mazzarella, L.; Lowe, C.; Lowndes, D.; Joshi, S.K.; Greenland, S.; McNeil, D.; Mercury, C.; Macdonald, M.; Rarity, J.; Oi, D.K.L. QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication. Cryptography 2020, 4, 7.
7. Er-Long, M.; Zheng-Fu, H.; Shun-Sheng, G.; Tao, Z.; Da-Sheng, D.; GuangCan, G. Background noise of satellite-to-ground quantum key distribution. New J. Phys. 2005, 7, 15.
8. Ntanos, Argiris, et al. "LEO Satellites Constellation-to-Ground QKD Links: Greek Quantum Communication Infrastructure Paradigm." Photonics. Vol. No. 12. Multidisciplinary Digital Publishing Institute, 2021.
9. Liao, S.-K.; Cai, W.-Q.; Liu, W.-Y.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; et al. Satellite-to-ground quantum key distribution. Nat. CellBiol. 2017, 549, 43–47.
10. Chen, Y.-A.; Zhang, Q.; Chen, T.-Y.; Cai, W.-Q.; Liao, S.-K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.-G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4600 kilometres. Nat. Cell Biol. 2021, 589, 214–219.
11. Carrasco-Casado, A.; Kunimori, H.; Takenaka, H.; Kubo-Oka, T.; Akioka, M.; Fuse, T.; Koyama, Y.; Kolev, D.; Munemasa, Y.; Toyoshima, M. LEO-to ground polarization measurements aiming for space QKD using Small Optical Transponder (SOTA). Opt. Express 2016, 24, 12254–12266.
12. Liao, Sheng-Kai, et al. "Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab." Chinese Physics Letters 34.9 (2017): 090302.

13. Kourogiorgas, Charilaos I., et al. "Capacity statistics evaluation for next generation broadband MEO satellite systems." IEEE Transactions on Aerospace and Electronic Systems 53.5 (2017): 2344-2358.

14. Dequal, Daniele, et al. "Experimental single-photon exchange along a space link of 7000 km." Physical Review A 93.1 (2016): 010301.

15. Moli, L., et al. "Quantum Key Distribution (QKD) using LEO and MEO satellites and decoy states." 2008 10th International Workshop on Signal Processing for Space Communications. IEEE, 2008.

16. Calderaro, Luca, et al. "Towards quantum communication from global navigation satellite system." Quantum Science and Technology 4.1 (2018): 015012.

17. Lyras, Nikolaos K., et al. "Optimizing the ground network of optical MEO satellite communication systems." IEEE Systems Journal 14.3 (2019): 3968-3976.

18. de Parny, Laurent de Forges, et al. "Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap." arXiv preprint arXiv:2202.01817 (2022).

19. Ntanos, Argiris, et al. "Large-Scale LEO Satellite Constellation to Ground QKD links: Feasibility Analysis." 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS). IEEE, 2022.

20. Ma, Xiongfeng, et al. "Practical decoy state for quantum key distribution." Physical Review A 72.1 (2005): 012326.

21. All Member States Now Committed to Building An EU Quantum Communication Infrastructure. Available online: https://digital-strategy.ec.europa.eu/en/news/all-member-states-now-committed-building-eu-quantum-communication-infrastructure (accessed on 3 November 2021).

22. Sodnik, Zoran, et al. "Greek Chelmos Observatory readies for Optical and Quantum Communication." 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS). IEEE, 2022.

23. https://helmos.astro.noa.gr/en/ Accessed on: 17/8/22

24. N. K. Lyras, C. I. Kourogiorgas, and A. D. Panagopoulos, "Cloud free line of sight prediction modeling for optical satellite communication networks," IEEE Commun. Lett., vol. 21, no. 7, pp. 1537–1540, Jul. 2017.

25. N. K. Lyras, C. I. Kourogiorgas, and A. D. Panagopoulos, "Cloud attenuation statistics prediction from Ka-band to optical frequencies: Integrated liquid water content field synthesizer," IEEE Trans. Antennas Propag., vol. 65, no. 1, pp. 319–328, Jan. 2017.

26. Cakaj, S.; Kamo, B.; Lala, A.; Rakipi, A. The Coverage Analysis for Low Earth Orbiting Satellites at Low Elevation. Int. J. Adv. Comput. Sci. Appl. 2014, 5, 8

27. Andrews, L.C.; Phillips, R.L. Laser Beam Propagation through Random Media; SPIE Optical Engineering Press: Bellingham, WA, USA, 1998;

28. Lyras, Nikolaos K., Athanasios D. Panagopoulos, and Pantelis-Daniel Arapoglou. "Deep-space optical communication link engineering: Sensitivity analysis." IEEE Aerospace and Electronic Systems Magazine 34.11 (2019): 8-19.

29. Hemmati, H. Near-Earth Laser Communications, 71–73; CRC Press: Boca Raton, FL, USA; New York, NY, USA; London, UK, 2009.

30. Hemmati, Hamid, Abhijit Biswas, and Ivan B. Djordjevic. "Deep-space optical communications: Future perspectives and applications." Proceedings of the IEEE 99.11 (2011): 2020-2039.

31. Kaushal, H.; Kaddoum, G. Optical Communication in Space: Challenges and Mitigation Techniques. IEEE Commun. Surv. Tutor. 2016, 19, 57–96.

32. Giggenbach, D.; Moll, F. Scintillation loss in optical Low Earth Orbit data downlinks with avalanche photodiode receivers. In Proceedings of the 2017 IEEE ICSOS, Naha, Japan, 14–16 November 2017;

33. Er-Long, M.; Zheng-Fu, H.; Shun-Sheng, G.; Tao, Z.; Da-Sheng, D.; Guang-Can, G. Background noise of satellite-to-ground quantum key distribution. New J. Phys. 2005, 7, 215.

34. Lo, H.-K.; Chau, H.F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. Science 1999, 283,2050–2056.

35. Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. Phys. Rev. Lett. 2005, 94, 230503.

36. Lucamarini, Marco, et al. "Efficient decoy-state quantum key distribution with quantified security." Optics express 21.21 (2013): 24550-24565.

37. Song, Ting-Ting, et al. "Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources." Scientific Reports 5.1 (2015): 1-11.

38. Eraerds, Patrick, et al. "Quantum key distribution and 1 Gbps data encryption over a single fibre." New Journal of Physics 12.6 (2010): 063027.

39. http://modtran.spectral.com/modtran_home, accessed on 17/8/22

40. Recommendation ITU-R P. 1621, "Propagation data required for the design of Earth-space systems operating between 20THz and 375 THz", 2003

41. Carrasco-Casado, A.; Sanchez-Pena, J.M.; Vergaz, R. CTA Telescopes as Deep-Space Lasercom Ground Receivers. IEEE Photonics J. 2015, 7, 1–14.

42. Zhang, Liang, et al. "Design and in-orbit test of a high accuracy pointing method in satellite-to-ground quantum communication." Optics Express 28.6 (2020): 8291-8307.

43. Single Quantum Eos. Available online: https://singlequantum.com/products/single-quantum-eos/ (accessed on 17/8/22)

44. http://www.opneti.com/uploadfile/20211025/20211025223956757.pdf

45. Jovanovic, N., et al. "Efficient injection from large telescopes into single-mode fibres: Enabling the era of ultra-precision astronomy." Astronomy & Astrophysics 604 (2017): A122.

46. Walenta, Nino, et al. "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing." New Journal of Physics 16.1 (2014): 013047.

47. Zavitsanos, Dimitris, et al. "On the QKD integration in converged fiber/wireless topologies for secured, low-latency 5G/B5G fronthaul." Applied Sciences 10.15 (2020): 5193.

48. del Portillo, Inigo, et al. "Optimal location of optical ground stations to serve LEO spacecraft." Proc. IEEE Aerosp. Conf.. 2017.