



Scheduling of space to ground quantum key distribution

Mateusz Polnik^{1*} , Luca Mazzarella², Marilena Di Carlo¹, Daniel KL Oi², Annalisa Riccardi¹ and Ashwin Arulsevan³

*Correspondence:

mateusz.polnik@strath.ac.uk

¹Department of Mechanical and Aerospace Engineering, University of Strathclyde, Glasgow, United Kingdom

Full list of author information is available at the end of the article

Abstract

Satellite-based platforms are currently the only feasible way of achieving intercontinental range for quantum communication, enabling thus the future global quantum internet. Recent demonstrations by the Chinese spacecraft Micius have spurred an international space race and enormous interest in the development of both scientific and commercial systems. Research efforts so far have concentrated upon in-orbit demonstrations involving a single satellite and one or two ground stations. Ultimately satellite quantum key distribution should enable secure network communication between multiple nodes, which requires efficient scheduling of communication with the set of ground stations. Here we present a study of how satellite quantum key distribution can service many ground stations taking into account realistic constraints such as geography, operational hours, and most importantly, weather conditions. The objective is to maximise the number of keys a set of ground stations located in the United Kingdom could share while simultaneously reflecting the communication needs of each node and its relevance in the network. The problem is formulated as a mixed-integer linear optimisation program and solved to a desired optimality gap using a state of the art solver. The approach is presented using a simulation run throughout six years to investigate the total number of keys that can be sent to ground stations.

Keywords: Quantum Key Distribution; Mixed-Integer Programming; Scheduling; Satellite; Space; Networking

1 Introduction

Communication security is vital for ensuring personal privacy, commercial confidentiality, government integrity, and defence. Current communication network encryption infrastructures are built upon public-key encryption methods^a whose security relies on computational complexity properties of certain mathematical problems. However, their security is increasingly under threat, from advances in cryptanalysis and, most notably, from the imminent arrival of large-scale quantum computers. Even if current public-key encryption methods are not vulnerable now, transmitted information with long-term value will need “forward security” to guard against future threats.

© The Author(s) 2020. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Quantum Key Distribution (QKD) is a quantum cryptography protocol that offers secret communication against current and foreseeable threats by exploiting the quantum properties of light, whose security is guaranteed by the laws of physics. More precisely, the no-cloning theorem ensures that an unknown quantum signal cannot be copied or amplified with arbitrary precision, causing possible eavesdropping activities to leave detectable traces [1].

QKD was first proposed in 1984 in the seminal paper [2] and since then underwent many theoretical developments [3–5] and groundbreaking demonstration in real-world implementations [6–8]. Channel losses which restrict the key rate, increase exponentially at about 0.2 dB/km in optical fibre, limiting the effective range of terrestrial systems. Consequently, quantum repeaters are required to extend the range of fibre systems. Still, these are far from being technologically mature, and the no-cloning theorem itself will severely bound their performance [9–11]. Currently, the maximum ground-based communication range achieved is 421 km in fibre [12] and 144 km in free space [13].

Recently, Satellite Quantum Key Distribution (SatQKD) has proved to be able to overcome these range limits, enabling secure communication globally. The Chinese mission Quantum Experiments at Space Scale (QUESS) [14], also known as Micius, successfully demonstrated various quantum communication protocols in space [15–17]. These groundbreaking results have spurred an international space race aiming not only to establish the first global quantum communication network but also to develop and deploy the architecture to merge different quantum technologies, such as sensing and computing, to build the future quantum internet. Besides China, other countries and space agencies are designing SatQKD missions involving one or more satellites, including Japan [18], Canada (QEYSSat) [19], Luxembourg (QUARTZ led by SES) [20], UK (QKDSat led by ArQit, QUARC) [21], Austria/France (NanoBob) [22], Germany (QUBE) [23], and UK-Singapore (QKD-Qubesat) [24]. The projects mentioned above address mostly Lower Earth Orbit (LEO) satellites, but there is a growing interest for higher orbits as well [25, 26]. Furthermore, satellites smaller and cheaper than Micius, such as nano-satellites (with a mass ~ 10 kg) have been in the spotlight [27–29], for the possibility of establishing quantum communication services using a constellation [30].

1.1 Contributions

The main contributions of the paper are listed below.

1. We propose a formulation for the SatQKD scheduling problem. It aims to schedule an optical downlink from one satellite to the network of ground stations allocating them time suitable to download the number of keys relative to their importance in the system expressed as a weight. To the best of our knowledge, such a problem has not been considered before in the literature. Solving the model indicates optimal performance possible to achieve for the given parameters of the satellite orbit and the location of ground stations. Consequently, the formulation we propose could be used as an evaluation framework for potential designs of a future SatQKD system. In the past, some related studies have been conducted in the field of optical communication to estimate the availability for communication or the amount of data possible to download to a given network of optical ground stations [31, 32]. However, the critical difference in our approach is distinguishing which ground station receives the transmission. The previous studies considered all ground

stations equivalent and it was not important which one communicated with the satellite. On the other hand, the ground stations in our study effectively compete for access to the satellite, and each of them must be supplied with keys for the communications system to remain operational.

2. We include relevant constraints to model the availability of the optical link and its throughput. We disallow the communication when the satellite is in sunlit. To the best of our knowledge, this requirement has not been considered in the literature on the downlink scheduling and the selection of optical ground stations. Furthermore, the transfer rate changes with the elevation angle rather than remaining constant. Modelling that phenomenon was suggested as the future work by [33].
3. We solve the above-mentioned SatQKD formulation and conduct a performance study of a hypothetical but realistic communications system with ground stations located in a single country at high latitudes and profoundly affected by changing cloud cover. We solve the model with a rolling horizon of one year using historical observations of cloud cover available for the period between the years 2013 and 2019. The length of the time frame is sufficient to capture the influence of seasonal weather patterns and changes in satellite illumination on the number of keys transferred to ground stations. Whenever possible, visualisations of the network properties and changes of the environment complement the study.
4. Finally, we perform a design of an experiment to find the parameters of the satellite orbit that provide the best performance of the communications system measured in terms of the keys delivered. Subsequently, we compute the number of keys which could be consumed weekly by each node in the communications system at some predefined service level guarantee, ensuring the number of keys a node owns will not be overdrawn. The example demonstrates that precise selection of the satellite orbit is critical for the performance of the communications system.

1.2 Paper's structure

The paper is structured as follows. Section 2 reviews literature on scheduling satellites' operations. Section 3 describes SatQKD from an optimisation perspective, introduces the network of ground stations selected for the study, and defines the index for quantifying the performance of the communications system. Results and discussion of the numerical study, including the long-term performance evaluation of the system are the subject of Sect. 4. Concluding remarks are given in Sect. 5.

Additional details on problem modelling and formulation of the optimisation problem are provided in the appendix, in Sect. A and Sect. B, respectively. In particular, Sect. A covers aspects related to modelling the dynamics of the system and its environment. We explain the model used to estimate the transfer rate between a satellite and a ground station, the position and the movement of the satellite, the duration of communication windows with ground stations, and the impact of cloud cover on the transfer rate. Section B presents the formulation of the optimisation problem and briefly explains the solution method.

2 Literature review

Concepts and present literature relevant to scheduling tasks for satellites placed in the LEO regime is discussed in this section. Special attention is devoted to schedul-

ing downlinks. We cover both radio and optical communication because the modelling paradigms and the solution procedures are the same.

Researchers and the industry experts agreeably acknowledge the need for optimisation in the scheduling of satellites' operations. The approach currently practised in real applications relies on a human intervention which is not considered sustainable for the number of satellites expected in the future and the complexity of large constellations [34]. The case study [35] describes an example operational system for the management of the satellite optical communication.

Conceptually a task to be executed by a satellite regardless of the details of the operation (i.e. manoeuvre, data collection, health check, commands uplink, payload downlink, etc.) has a release date, due date and estimated duration [36]. The problem of scheduling satellite's operations belongs to the class of Machine Scheduling [37]. Some researchers [34] who consider task scheduling in a constellation of satellites prefer to model a spacecraft as a resource instead of a machine and use the Multiprocessor Scheduling [38] as the baseline problem.

Tasks may have different priorities or rewards for their execution. It reflects a situation when multiple clients of varying importance compete for access to the satellite. If tasks priorities are considered, then the scheduling problem is an example of the Resource-Constrained Project Scheduling [39]. That analogy was suggested by [40], who studied scheduling download of images with priorities and deadlines. The scheduling system considered was oversubscribed, hence postponing deadlines of some tasks or cancelling them was unavoidable. The authors applied the state of the art meta-heuristics to a real problem instance. The number of completed downloads in optimised schedules increased twofold compared to the mission schedule used in practice. It will become apparent shortly that for scheduling downloads which do not require handling priorities optimisation models are effectively solvable to optimality. Hence the lack of priorities can be exploited to derive more computationally attractive problem formulations.

Regardless of the problem taxonomy, what makes the satellite applications unique, are the external constraints which either must be satisfied to commence a task or must remain valid for the entire duration of the task execution [36]. For instance, a ground station must be visible to a satellite to establish and maintain a downlink. Such conditions are commonly defined using time windows.

Historically the dominating techniques for scheduling satellite communication were based on genetics algorithms [41], heuristics and meta-heuristics [36, 40] often combined with Local Search (LS) and constraint propagation. Nowadays, these approaches are incrementally superseded by exact methods, in particular, modelling the scheduling problem as a Mixed-Integer Linear Program (MILP) with time discretisation, which has been demonstrated to have a strong bound of its linear programming relaxation [33, 42, 43]. These models can be solved using commercial solvers without the need for devising custom solution procedures. Such solvers provide a certificate of optimality which is not available for heuristic procedures.

The problem of scheduling downloads from a single satellite to multiple ground stations was studied by [42]. The researchers included the data and energy acquisition, which made the scheduling problem more realistic for the application in Earth Observations (EO) combined with downlink using radio communication. Tacking data and energy dynamics already made the problem NP-hard. The author [42] demonstrated that a Mixed-Integer

Program (MIP) with time discretisation is easy to solve to optimality for problem instances based on real data. Interestingly, the solution process for these instances did not require branching. The formulation was extended to a scenario with multiple satellites by [33] who demonstrated that such a model remains easy to solve.

Apart from generic models considered in the literature, the need to accommodate some specific constraints may arise when a given formulation is adapted to solve a real-world problem. For instance, a satellite may have two antennas and support several operational modes with different energy to bitrate thresholds. Fortunately, the model with time discretisation facilitates incorporation of additional constraints [34]. The initial version of the problem proposed by [42] already supported different power manager configurations.

The model with time discretisation is typically solved standalone, without resorting to reformulations and decompositions [33, 42]. The size of the formulation can be considered its major limitation and was emphasised in an application to the constellation of 30 satellites with a fine discretisation interval solved using a low spec machine. For such a configuration, the researchers devised a heuristic based on Lagrangian relaxation. The heuristic applied a sequence of subgradient minimisations and progressively fixed decision variables. Interestingly, the solution procedure can be used without a MIP solver, albeit with an adverse impact on the cost of the final solution.

If the orientation of a spacecraft can be changed, such a satellite is called agile to emphasise that the attitude control system manoeuvres can be included in the execution of a schedule. This feature is desirable in EO, as the spacecraft can perform image acquisition several times during a single visibility window [43]. The introduction of the attitude manoeuvres elevates the complexity of the scheduling problem. For such problem instances, it has been shown that a better alternative to solving a model standalone is the application of the column generation scheme [43]. The researchers exercised it to the root node of the branch and bound tree and then solved the remaining nodes without extending the pool of columns.

In real-world, the satellites significantly outnumber ground stations which leads to the competition for access to the ground station infrastructure. The process of resolving such conflicts is known as deconfliction. The initial progress in this area was driven by solving the Satellite Range Scheduling [44, 45] which allocates antennas to spacecraft for some desired time within a communication window. The problem instances are defined to accurately illustrate the United States Airforce Satellite Control Network (AFSCN) which operates more than 100 satellites using 16 antennas located in nine ground stations. The scheduling system is oversubscribed, and two variants of the objective function were studied: minimisation of the number of cancelled tasks and minimisation of the total time when any antenna is assigned to more than one task simultaneously. The latter variant allows for scheduling long tasks and is preferable by human operators who resolve remaining conflicts by negotiations with clients [45]. The best results for realistic problem sizes were obtained using a genetic algorithm [44, 45]. Nowadays, human schedulers who supervise operations of AFSCN are supported by a proprietary heuristic algorithm which schedules the most restricted tasks first preventing further depletion of resources [46]. Instead of cancelling requests which initially cannot be satisfied, the system attempts to resolve remaining conflicts automatically by relaxing operational constraints following a set of predefined business rules. A formal study of the computational complexity of a conflict resolution was conducted by [47] using a hypothetical scenario with multiple satellites

competing for access to a single ground station. Interestingly, the complexity of the case allowing task preemption and no setup cost remains an open problem. If the setup cost is present or task preemption is disallowed, the problem is NP-hard in general [47].

For scheduling data transfers, a network of ground stations is given as an input. Such an assumption is also valid for traditional monolithic radio frequency ground stations whose locations worldwide are well known (i.e. Etrack). On the other hand, designing a network of optical ground stations is an open problem and can be the subject of optimisation as well. The practical approach is finding a subset of the ground stations from the list of possible candidates [48]. The available budget restricts the number of ground stations. Consequently, the problem is similar to the Warehouse Selection Problem [49]. A typical objective function applied in the literature is the Maximum Percentage Data Transferred (MaxPDT) [32, 48]. It evaluates how much data collected by an example EO mission can be downloaded using the given network of ground stations. Computing such an objective involves finding a schedule of data transfers. Fortunately, the inner problem admits a pseudopolynomial complexity and can be solved using dynamic programming [31, 32]. The subset of the ground station is found either through direct enumeration for small problem sizes or using LS.

The studies of optical ground station selection have been carried out for different regions, the entire world [31, 48], Europe [31, 50] or Germany [31]. These analyses account for cloud cover over multiple years. However, researchers do not consider satellite illumination, which is relevant to ground stations located at high altitudes. In a similar vein, the transmission rate does not change with the elevation angle between the ground station and the satellite. To increase the performance of the ground station network and make it more resilient to cloud cover, [51] considered more complex setups involving a geostationary satellite as a relay, using a high altitude platform or a combination of both radio and optical communication. So far, such analyses were limited to a single ground station.

3 Problem statement

Satellites are currently the only platform allowing QKD to achieve intercontinental range. SatQKD can be realised using a satellite as a transmitter (downlink configuration) or as a receiver (uplink configuration). A downlink configuration requires the development of a space-qualified optical assembly for precise pointing of the order of few μ -rad, quantum sources such as lasers, and a quantum random number generator [27, 30]. The uplink configuration arguably requires a less complicated payload consisting of single photon detectors. However, in the uplink configuration the optical beam encounters turbulence early during its path leading to larger angular deviation and therefore higher losses, of about 20 dB with respect to down-link [52].

Assuming that the eavesdropper cannot access the satellite, we employ the trusted-node architecture. In trusted-node SatQKD, a satellite distributes keys sequentially, first to a ground station A, then to ground station B. Subsequently, the satellite broadcasts over a public channel the XOR hash of both keys allowing thus the A and B to have a shared key with which they can employ (quantum-safe) symmetric key encryption protocols [52].^b In this work, we will focus on the downlink and trusted node scenario due to its comparative simplicity.

Before proceeding, we wish to highlight that this method may also be applied to the uplink scenario. The link topology and the formulation of the scheduling problem would remain the same. However, attenuation is about 20 dB in that case.

Figure 1 Artist's impression of the communications system. We consider ten locations throughout the UK to represent potential nodes in a national quantum-secured communications network. Conventional communication between these nodes is encrypted with symmetric key pairs distributed via a satellite placed in a Sun-Synchronous Orbit. The satellite has a single quantum transmitter that can send single-photon level signals to optical ground stations. The dashed arc is the ground track the spacecraft follows. The satellite passes over the UK mainland territory South to North around local midnight



On the other hand, the current analysis would need some modification for untrusted node operation. Firstly, keys would need to be generated pairwise between communicating nodes which requires simultaneous visibility by the satellite of both ground stations for an extended portion of the pass. Secondly, the full network traffic graph would be needed for optimisation to establish the pairwise key generation demand, rather than the summed values at each node. Furthermore, the untrusted node SatQKD is a lot more challenging to implement than the trusted node and is not thought to be likely in the near to medium term.

The communication system consists of a QKD satellite and a network of ground stations spread across cities of the United Kingdom. The satellite operates as a “trusted node” to mediate the distribution of secure encryption keys pairwise between ground stations. The locations were selected based on their importance for the country and geographical dispersion. From a practical standpoint, the distance between satellite-linked ground stations should exceed 100 km because communication on shorter distances could be handled using a fibre optic link.^c Ten ground stations were shortlisted. Their geographical dispersion is illustrated in Fig. 1 and the motivation behind establishing a ground station in the particular city is explained below.

- Belfast Largest city in Northern Ireland,
- Birmingham Second largest population in the country,
- Bristol Largest city in south-west England,
- Cambridge Science centre and fibre optic communication hub,
- Glasgow Largest city in Scotland,
- Ipswich British Telecommunication headquarters,
- London Largest population and urban zone in the United Kingdom,
- Manchester Second largest urban zone in the country,
- Thurso Northmost city in the network, it has the weakest correlation of weather conditions with other ground stations,
- York Railway network hub.

A satellite transfers cryptographic keys to ground stations which store them in buffers. The keys will be used later for encrypting ground-to-ground communication between stations. To establish a secure connection between two parties, each has to use the same key for encryption and decryption. Then, after the connection is closed, each party removes the key from its buffer due to the security requirement that a key cannot be reused.

Operational requirements of ground stations for a given week should be satisfied using the keys stored in a buffer of the ground station before the start of the week. Consequently, the keys delivered to the ground station throughout the week will not be used for encryption immediately. Their availability is delayed in time for the next week because the raw transmitted keys require post-processing performed in batches after enough raw keys are collected [53]. Apart from the privacy amplification, buffering keys mitigates scenarios in which overcast or satellite illumination prevent the delivery of new keys to individual ground stations.

Before we present how the SatQKD is modelled as a scheduling problem, let us introduce the assumptions and terminology. A schedule is a sequence of tasks a satellite should execute. We consider a problem setting with one satellite and a set of tasks of the same kind—optical data transfers. Therefore, we use the terms task and data transfer interchangeably. Each task in a schedule has a start time when its execution should commence, duration and the target ground station. Tasks are executed from start to completion without preemption. Consequently, a data transfer is a single continuously attempted optical link between a given ground station and the satellite. The satellite can communicate with at most one ground station at a time. For the convenience of presenting the results and technical considerations explained in Sect. A.1, we aggregate the volume of data transferred into 256 bit unit blocks and refer to them as keys.

The period for which a schedule is computed is called the planning horizon. We are interested in building a long-term schedule and proving its optimality. Doing so for the whole six-year period would lead to a computationally challenging problem due to the size of its formulation. Hence, we restrict our attention to the sequence of one-year-long periods. The final state of the communication system for a given planning horizon, i.e., the position of the satellite and the size of key buffers for each ground station, is the initial state for the subsequent planning horizon. This technique is known as the rolling horizon in the literature on scheduling and inventory control [54]. In scheduling optical satellite communication, the length of a planning horizon usually ranges between two days and one week, which can be justified by the availability of accurate weather forecast. Since we consider scheduling using historical weather information, and our model remains effectively solvable, we prolonged the planning horizon to the period of one year. Ultimately, it leads to more efficient schedules, as the optimization model considers weather seasonality patterns and changes in satellite illumination throughout the entire year. Hence, the solver is capable of making decisions which bring long-term benefits. Such a schedule can then be used to assess the best possible performance that the design of the future communications system allows. It should be a valuable indicator to support decisions involving the locations of ground stations and the selection of the orbital parameters for a satellite. Finally, our model could easily be scaled down to shorter planning horizons without any inherent difficulty and we would obtain the corresponding computational savings.

The objective of the space-to-ground data transfer optimisation is to maximise the minimum usable number of keys buffered by ground stations. To recognise where keys should

Table 1 Importance of ground stations in the network. First two columns contain the name of the city and the number of premises with High-Speed Broadband (HSBB) access located in that administrative area. The third column displays weights proportional to the number of premises from the second column. The last column contains the final weight of the ground station used in the study

City	Premises with HSBB	Inferred Weight	Used Weight
Belfast	288,667	0.08061	0.080
Birmingham	599,540	0.16742	0.166
Bristol	297,599	0.08310	0.082
Cambridge	107,923	0.03014	0.030
Glasgow	381,494	0.10653	0.105
Ipswich	58,093	0.01622	0.016
London	1,421,422	0.39692	0.393
Manchester	353,884	0.09882	0.098
Thurso	118	0.00003	0.010
York	72,418	0.02022	0.020

be distributed, the ground stations are assigned non-negative weights corresponding to the desired activity of a given node in the communication system. The methodology of using weights to measure the importance of nodes in a network was developed for the analysis of graphs with weights assigned to edges, which are known as weighted networks [55, 56]. Several measures for studying interactions between nodes in such systems have been proposed. For instance, the sum of weights assigned to incident edges referred to as vertex's strength [56] is considered a generalisation of a vertex's degree in an unweighed graph.

Table 1 presents the weights assigned to the nodes in the hypothetical network we consider. Their values are proportional to the number of premises with high-speed broadband access (300 MBit/s download speed or higher) located in a given city. The numbers were derived from datasets compiled by the Office of Communications [57], which is the governmental body that regulates the telecommunication sector in the UK. We assigned Thurso a higher weight than data indicates (0.01 v.s. $3E-5$) because the city could be the hub for the Highlands and Islands region. The economic development of these remote areas increasingly depends on reliable and secure communication links [58]. The final weights were normalised, so the sum of all weights assigned to nodes equals one and then rounded to three digits after the decimal point.

We aim to distribute key maximising the network traffic uniformly on all links. For that reason, we are interested in a measure which quantifies the traffic globally for the entire communication network. Maximising such a performance index could become the objective of an optimisation problem. Furthermore, maintaining its value above a certain threshold could be subject to a service level agreement. In the following subsection, we provide a possible definition of such an index. For the sake of convenience, we call it the traffic index.

3.1 Traffic index

To formally define the traffic index, we adopt the following notation and symbols. Capital letters represent sets. The syntax $|S|$ stands for the cardinality of the set S . Small bold-face letters denote vectors. The i -th element of a vector \mathbf{v} is accessed using a subscript notation v_i .

Consider the following symbols.

N Set of ground stations in the problem definition. We refer to them as regular ground stations. Besides, there is an auxiliary station 0 observed by the satellite when no data transfer can be in progress. \bar{N} refers to the set of all ground stations including the auxiliary one, i.e., $\bar{N} := N \cup \{0\}$.

\mathbf{b}^n Vector indexed by time $t \in T$ tracking the number of keys the ground station n stores in its buffer.

\underline{b} Number of keys reserved for authentication of a ground station by the satellite.

\mathbf{w} Vector indexed by ground stations $n \in N$ storing the assigned weights.

T Set of points partitioning the planning horizon into smaller periods. We evaluate the traffic index for each element of T . The sum of traffic indices over T is the objective function of the optimisation problem to maximise. For example, with no loss of generality, the traffic index could be evaluated every Monday throughout the planning horizon.

α Desired service level defined as the probability that the size of the key buffer of every ground station does not fall beyond the threshold \underline{b} at the time $t \in T$.

A feasible solution to the following optimisation problem, parametrised by α , satisfies properties of the index described in the previous section. Henceforth, we refer to it as the traffic index and denote using the symbol $\lambda_{\alpha,t}$, where $t \in T$.

$$\begin{aligned} \max \quad & \sum_{t \in T} \lambda_{\alpha,t} \\ & \mathbb{P}(b_t^n - w_n \lambda_{\alpha,t} \geq \underline{b}) \geq \alpha \quad \forall n \in N, \forall t \in T \\ & \lambda_{\alpha,t} \in \mathbb{R}^+ \cup \{0\} \quad \forall t \in T \end{aligned} \quad (1)$$

Let λ_{α}^* be the vector of the optimal values for the problem above indexed by time $t \in T$. Intuitively, $\frac{w_n}{|T|} \sum_{t \in T} \lambda_{\alpha,t}^*$ is an upper bound on the constant, periodic key consumption rate at the node $n \in N$ which can be maintained at the service level α . Note, that maximising $\sum_{t \in T} \lambda_{\alpha,t}$ goes alongside maximising the number of keys a ground station receives and simultaneously ensuring this number is consistent with the weight assigned to the communications node. In some sense, what we are doing is we are maximising the minimum number of keys sent to any ground station at any given time period. The minimum number of keys is what we call as usable keys that is also weight adjusted.

The complexity of solving Problem 1 increases by considering the probability distribution of its constraint, which can be unknown or imprecise. However, to find the maximum key consumption rate for a given communications node, there is no need to handle probabilistic constraints directly. Instead, we reformulate the optimisation problem by removing the dependence on the service level α and replacing the probabilistic constraints by their deterministic equivalents, leading to the following formulation.

$$\begin{aligned} \max \quad & \sum_{t \in T} \lambda_t \\ & b_t^n - w_n \lambda_t \geq \underline{b} \quad \forall n \in N, \forall t \in T \\ & \lambda_t \in \mathbb{R}^+ \cup \{0\} \quad \forall t \in T \end{aligned} \quad (2)$$

To stress the independence of the service level α , we removed the subscript from the traffic index notation λ_t . Now suppose, we temporarily ignore the key consumption. Con-

sequently, buffers' sizes are non-decreasing over time. Then, the maximum constant periodic key consumption rate for a given node $n \in N$ guaranteed at some desired service level α can be found by analysing the marginal increase rates of b_t^n over time, which is the approach we adopted in Sect. 4. For the complete model of the optimisation problem, including the formal definition of all relevant constraints, see Sect. B.2.

3.2 Impact of the environment

Some current physical and technological limitations restrict opportunities for a successful space to ground data transfer. Section A.1 explains the key transfer rate estimation model in the cloud-free line of sight. For simplicity, we assume the satellite transfers keys at the rate a ground station can receive them, and all ground stations have the same transmission capabilities.

A transmission must happen during night hours due to stray light restrictions, and only when a ground station is visible to a satellite. We assume that the satellite can connect to the ground station when its elevation angle, relative to the ground station, is greater than 15° . The larger the elevation angle, the higher is the transmission rate. Section A.2 describes the satellite propagation model and the procedure to calculate the elevation angle. The opportunity for communication is further restricted to periods when the satellite experiences a total eclipse in Earth's shadow (umbra). Sect. A.3 provides some insights on the duration and the frequency of communication windows.

Besides sunlight, local weather conditions, cloud coverage, in particular, may adversely impact the transmission rate. The periods of clear sky are intermittent in the weather patterns observed in the UK. As a result we assume the communications system remains operational in presence of clouds and the transfer rate declines linearly as cloud cover percentage increases. We explain the relationship between cloud cover and the transmission rate in more detail in Sect. A.4.1. This simplistic approximation scheme was taken for the ease of exposition because it is commonly used to evaluate amount of data possible to download in the optical ground station selection problem [32, 48]. The formula is not exploited to make the optimisation process easier or more efficient. Finally, the formulation of the problem and the solution procedure could remain unchanged after the transfer loss function is updated to a different model.

4 Results and discussion

In this section, we analyse results of the space-to-ground data transfer optimisation for the network of ground stations introduced in Sect. 3.

After explaining the configuration parameters of the optimisation problem, we present an example solution of a one-week scheduling problem. This should help the reader to develop an understanding of the behaviour of the communications system at the level of individual data transfers. Next, we analyse aggregated results of scheduling data transfers over six years. In particular, we focus on the performance of the communications system considering the number of keys which can be consumed weekly by a ground station at the desired service level. We conclude the section by providing empirical evidence that our solution method and the results discussed are resilient to random perturbations of the input data in the definition of the optimisation problem. All results presented below were obtained by solving the formulation described in Sect. B. The dataset of problem instances is available for testing and benchmarking purposes [59].

4.1 Configuration parameters

The schedules were computed for six years starting from the 1st of January 2013 with the rolling horizon of one year. The planning horizon T was partitioned into one-week long segments. Keys delivered to a ground station in a given week were released on Monday the following week. The time was indexed into 15 seconds long periods.

Every city received an initial buffer of 64 keys reserved for authentication. These keys were not allowed for communication between ground stations, and the actual threshold of the authentication reserve did not affect the service levels computed in the simulations.

The formulation was solved using a workstation with AMD Ryzen 7 2700X eight-core processor and 32 GB of RAM. The criterion for stopping computations was reaching optimality gap between the objective value of the current best solution and the estimated upper bound below 1%. Hence, it can be shown that improving the final cost by more than that amount is impossible. The total time for computing a schedule for one year ranged between 2 and 43 minutes. The theoretical computational complexity of solving the formulation follows its definition presented in Sect. B.2.

4.2 Orbital parameters

The satellite's orbit is circular with an altitude of 566.897 km above Earth's surface. As a result, the spacecraft makes exactly 15 complete passes of the orbit within 24 hours. One revolution takes 96 minutes. The inclination for the selected altitude is 97.658° to counterbalance the Earth's nodal precession causing the drift in the Right Ascension of the Ascending Node (RAAN). For the given inclination, the cumulative RAAN drift throughout a year is 360° . Hence, the precise characteristics of the time windows when a ground station is visible to the satellite observed a given night occurs every year. An orbit with such a property is called a Sun-Synchronous Orbit (SSO). The argument of the latitude set to 46° together with the initial epoch at 00:00:00 UTC, the 1st of January 2013 align one of the visibility windows around midnight. It is crucial during summer months, as throughout the visibility periods shifted off midnight the spacecraft may remain in sunlit despite night observed by the ground station. This phenomenon significantly affects the ability to communicate with ground stations located at high altitudes, such as Thurso, which has no contact with the spacecraft for several weeks during summer.

It was not immediately apparent to us how the RAAN parameter should be set to obtain the configuration that yields the most efficient schedules. To answer this question, we narrowed the RAAN values to the interval $[90.5^\circ, 115.5^\circ]$ and computed a Service Level (SL) for every configuration obtained by incrementally iterating over values within that interval with the step of 1° . The Service Level at a given threshold, e.g. 99%, is defined as the maximum number of keys a ground station may consume weekly without depleting its keys reserved for authentication for the number of weeks proportional to the given level in the time frame considered. The service level is estimated by analysing marginal changes in the size key buffers of all ground stations in the network. Therefore, every ground station could consume a similar number of keys relative to its weight. Furthermore, whichever ground station is selected, its SL gives the same perspective on the performance of the system.

Table 2 contrasts the initial RAAN value with the maximum weekly key consumption in London maintainable at 99% global service level over six years. The difference in the output service level between configuration variants is significant. Setting the initial RAAN

Table 2 Sensitivity analysis of the initial RAAN on the performance of the communications system. Columns display the value of the RAAN at the initial epoch and the maximum weekly key consumption in London maintainable at 99% SL throughout six years

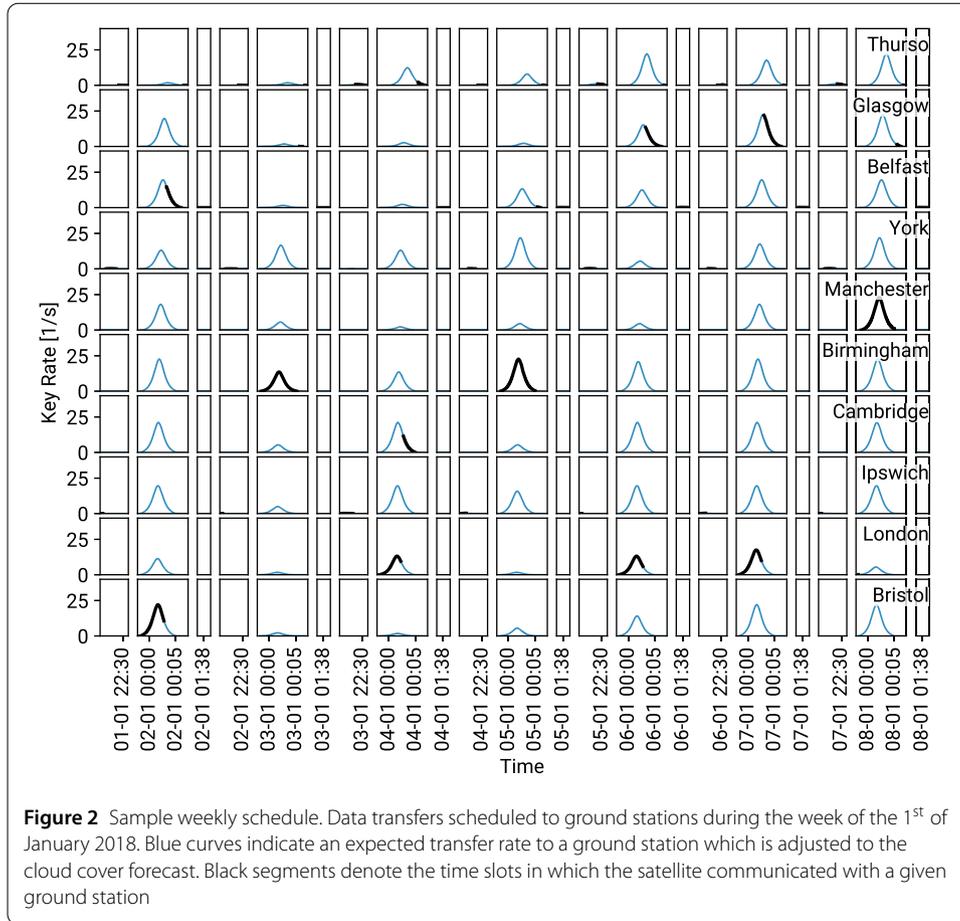
	RAAN	London 99% SL
1	90.5	5851
2	91.5	5446
3	92.5	5053
4	93.5	4637
5	94.5	4346
6	95.5	4102
7	96.5	3918
8	97.5	3843
9	98.5	3898
10	99.5	4063
11	100.5	4299
12	101.5	4641
13	102.5	5097
14	103.5	5631
15	104.5	6236
16	105.5	6869
17	106.5	7478
18	107.5	8025
19	108.5	8229
20	109.5	8327
21	110.5	8068
22	111.5	7785
23	112.5	7518
24	113.5	6920
25	114.5	6472
26	115.5	5993

to 109.5° yields the best performance, and the decrease in efficiency would be more than twofold if the value of 95.5° was used instead. The example demonstrates the utility of schedule optimisation to evaluate the best possible performance of the system to rule out suboptimal configurations. In the remaining text, we use the RAAN setting that allows the best performance.

4.3 Weekly scheduling

Figure 2 illustrates a fragment of the optimal schedule for the first week of the year 2018.

The visualisation helps to develop intuition about communication windows, their duration and the behaviour of the transfer rate. The length of a communication window varies significantly within the week. The shortest windows are less than 2 minutes whereas the longest exceed 6 minutes. The highest transfer rate is attained in the centre of a communication window. Furthermore, in the same cloud cover conditions, the longer the communication window, the higher the maximum value of the transfer rate is reached. Some communication windows are adversely affected by weather conditions, for instance, the 2nd of January around 10 PM cloud cover was at least 75% across all locations. Finally, during a communication window, the satellite switches between no more than a few ground stations. In the presented example, at most four data transfers were performed (London, Manchester, Glasgow and Thurso the 8th of January around midnight). Similar considerations can be generalised to any other week of a year.

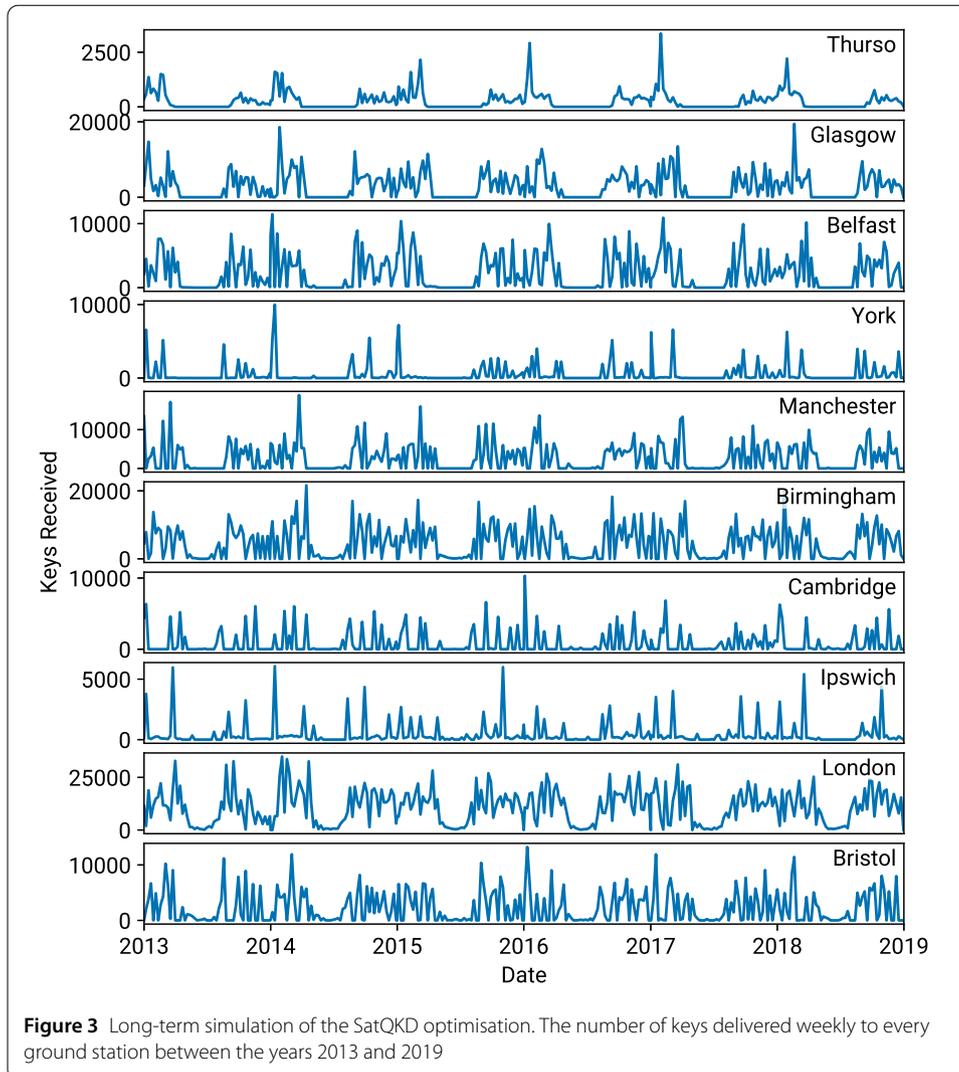


4.4 Long-term scheduling

The long-term performance profile of the communications system was obtained by solving scheduling problems with a rolling horizon between the years 2013 and 2019.

Figure 3 displays the number of the keys transferred to a ground station every week. The plot presents results of a single run of the schedule optimisation for every year. There was no point in repeating optimisation for the same input problem because the solution method is deterministic. Consequently, solving a given model always returns the same result.

London, which is the most significant ground station, receives a substantial number of new keys compared to the remaining ground stations almost every week. Birmingham, which is the second most important station in the network, has a comparable key delivery profile. York is on the opposite end of the spectrum. The city receives keys only in a few weeks per year. Cambridge and Ipswich, which are also assigned small weights, obtain keys similarly, albeit they experience data transfers more frequently. On the other hand, Thurso, which is the least significant station in the network, does not share such a communication profile. The city benefits from location in a remote area and not sharing some part of its communication windows with any other ground station. Therefore, the satellite can send keys to Thurso because no other city would be able to receive them. Remaining ground stations (Glasgow, Belfast, Manchester, and Bristol) belong to a group of cities whose weight is between 0.08 and 0.105. A distinctive pattern in this group is observed



for Bristol, which is the most southern ground station in the network. Thus, it is also the first location visible to a satellite during its pass around midnight. We elaborate on the frequency and the duration of communication windows in Sect. A.3.

Taken together, ground stations observe different patterns of communication with the satellite, which conceivably depends on the weight assigned in the network. During summer all ground stations experience a notable decrease in the number of keys delivered. In particular, Thurso and Glasgow lose the ability to communicate with the satellite. Consequently, to maintain connectivity with other ground stations over summer, they must be topped up in advance. Roughly, the pattern of key distribution to a given ground station repeats every year.

Due to a vast disproportion in the number of keys delivered to a ground station every week, we computed the maximum constant key consumption rate, which could be maintained over time without exceeding buffer's capacity. Figure 4 displays a relation between the maximum key consumption rate for London and the Service Level obtained. The shape of the plot is similar to any other ground station.

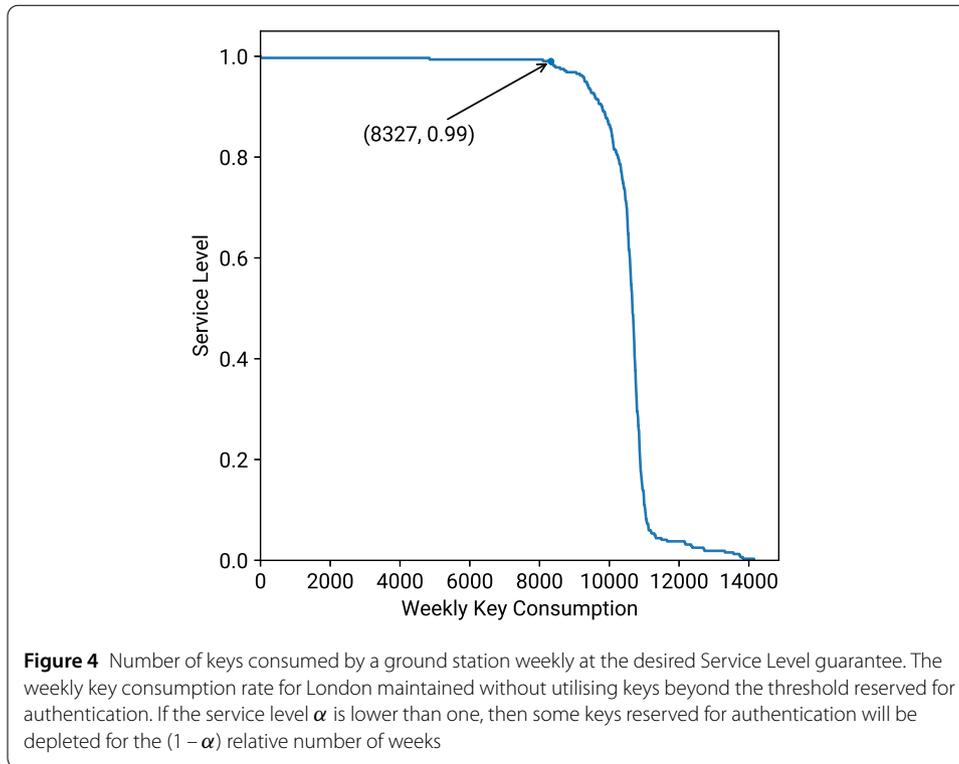


Table 3 Maximum key consumption rate maintainable weekly at 99% Service Level by a given ground station. The key consumption at other levels for the London ground station can be inferred from Figure 4. The graphs for the remaining ground stations follow a comparable trend

City	99% SL
Thurso	211
Glasgow	2224
Belfast	1695
York	423
Manchester	2076
Birmingham	3517
Cambridge	635
Ipswich	339
London	8327
Bristol	1737

Considering the number of keys the ground station received each week, London could consume up to 8327 keys weekly without exceeding the capacity of its key buffer for 99% of weeks. If the key consumption rate is raised above that threshold, then the service level will drop because there will not be enough keys to meet the demand for some additional weeks. It is important to emphasise that the service level is inferred accounting for the size of key buffers of all ground stations in the network. Table 3 reports the maximum number of keys possible to consume weekly at the 99% SL for every ground station.

Intuitively, the weight assigned to the ground station and the key consumption are related. For instance, Glasgow and Manchester, which are assigned similar weights, can consume keys at a comparable rate. However, a stronger observation valid for all ground stations is possible to infer. It can be shown that the 99% SL for a given ground station equals its weight multiplied by the coefficient 21000 ± 75 .

4.5 Evidence of numerical stability

The scheduling problem is defined by the orbital parameters of the satellite, the locations and weights of the ground stations, and the planning horizon. Among these settings, the weights are arguably the most difficult to know precisely, due to their arbitrary nature. For that reason, we study how the introduction of noise to the value of weights affects the final results, in particular, the number of keys a ground station receives every week, and the key consumption at the 99% SL.

Individual weights of nodes in the communications network were perturbed by introducing noise following the formula below.

$$\hat{w}'_i = \hat{w}_i \cdot (1 + r \cdot \tilde{n}).$$

Let \hat{w}'_i and \hat{w}_i be the updated and the initial weight for a ground station i , r is the perturbation threshold, and \tilde{n} is a random variable following the standard normal distribution. The perturbation threshold was set to 0.1. Subsequently, new weights were normalised, so their sum equals one.

Figure 5 presents box-plots of the number of keys London received every week between the years 2013 and 2019 depending on the weight assigned to the station.

The introduction of moderate noise in weights does not seem to affect significantly the number of keys delivered to a ground station. Predictably, the median increases as the weight rises, also the boxes and the whiskers move up.

Conceivably, the perturbation of weights influenced the number of keys which could be consumed by a ground station at some desired service level. Table 4 presents the maximum

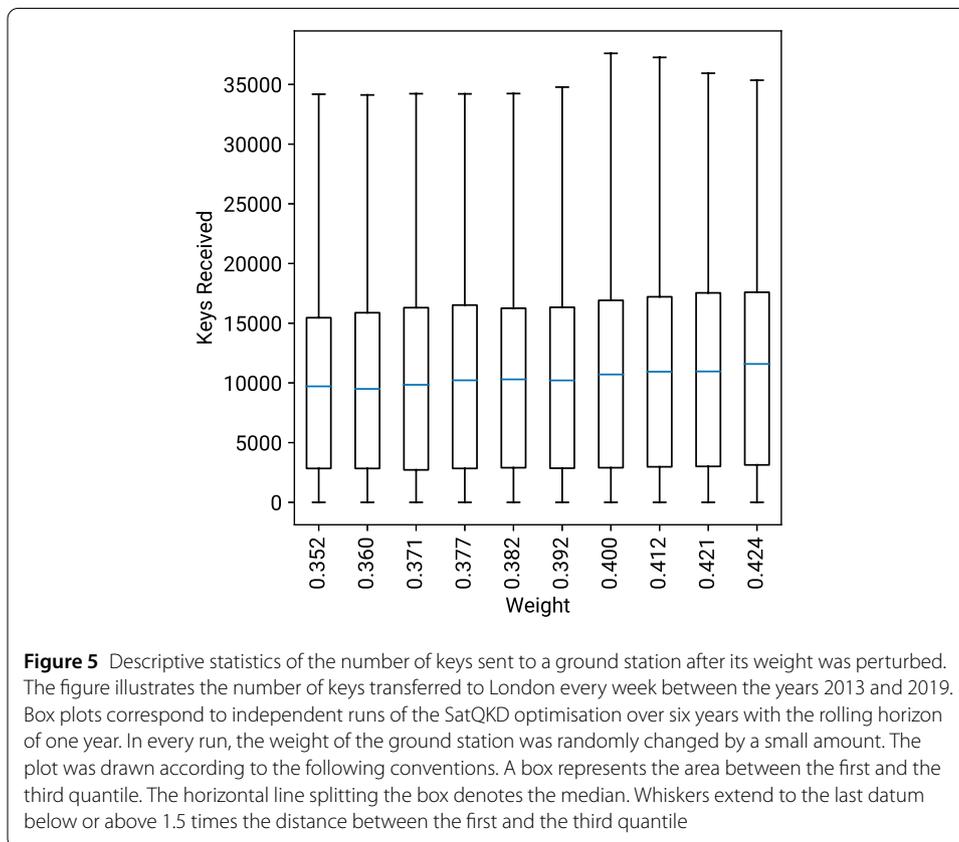


Figure 5 Descriptive statistics of the number of keys sent to a ground station after its weight was perturbed. The figure illustrates the number of keys transferred to London every week between the years 2013 and 2019. Box plots correspond to independent runs of the SatQKD optimisation over six years with the rolling horizon of one year. In every run, the weight of the ground station was randomly changed by a small amount. The plot was drawn according to the following conventions. A box represents the area between the first and the third quantile. The horizontal line splitting the box denotes the median. Whiskers extend to the last datum below or above 1.5 times the distance between the first and the third quantile

Table 4 Weight of the ground station and its impact on the service level. Columns of the table display the weight assigned to the London ground station followed by the maximum number of keys possible to consume at the 99% SL. The box-plots presenting descriptive statistics of the number of keys delivered weekly to the ground station for every weight's setting are displayed in Figure 5

	Weight	London 99% SL
1	0.352	7364
2	0.360	7531
3	0.371	7760
4	0.377	7919
5	0.382	7984
6	0.392	8259
7	0.400	8385
8	0.412	8615
9	0.421	8943
10	0.424	9048

number of keys consumed weekly at 99% SL guarantee in London depending on the weight assigned.

The numbers of keys consumed after the perturbation of weights do not differ significantly from results obtained using the initial weights. Predictably, the key consumption rate changes by a small amount following the weight. Overall, the weekly key consumption remains in the interval of [7364, 9048] for the weights between 0.352 and 0.424. Recall, the key consumption for London at 99% SL with the weight of 0.393 was 8327, which fits approximately in the centre of the interval for the weekly key consumption.

5 Conclusions

We formulated for the first time a SatQKD as a mathematical program. We then modelled a hypothetical but realistic network of optical ground stations and solved the scheduling problem with a rolling horizon of one year for the period between the years 2013 and 2019 using the state-of-the-art commercial solver. Computational results give insights into the number of keys which could be delivered to the network. The provided estimates on the weekly key consumption rate attainable in different locations of the communications system are intended to serve as a guideline on whether future investments in the development of this technology could meet the operational demands of telecommunication providers.

For the interest of the community investigating the optical ground stations selection problem and the optical downlink scheduling, we modelled two additional assumptions, which are relevant but not commonly used in the literature. Firstly, we model a variable transmission rate of the optical link which changes with the elevation angle between the satellite and the ground station. Secondly, we disallow communication when the spacecraft is in sunlit. Furthermore, we believe the key concepts applied in our formulation which allocate a downlink time proportionally to the importance of a given node in the communications system, can be translated to optical downlink scheduling for independent clients with different priorities.

The short computation times are due to the strong linear programming relaxation of the model with time discretisation that we have applied. As a result, reaching the optimality gap below 2% requires no branching for the problem instances used in this study. The exploration of the branch-and-bound tree was necessary to achieve the optimality gap of 1%. The observed computation time follows results reported by researchers who consider downlink scheduling using models with time discretisation [33, 42, 43]. Since these

problems are effectively solvable to optimality, we suspect the community will eventually deprecate applications of heuristic, metaheuristic and evolutionary algorithms which do not provide information about the optimality gap and are inherently prone to premature convergence.

Our future work is focused on moving from historical weather observations to medium term weather forecasts. This step requires changes in the problem formulation to incorporate the uncertainty of cloud cover predictions and the development of an optimisation approach to solve the new problem definition in a reasonable computational time. Another research direction could explore the benefits of considering a constellation of satellites.

Appendix A: Modelling

A.1 Estimation of the transmission rate

Quantum computers will render existing public-key encryption methods based on RSA and Elliptic Curve protocols vulnerable to attack within the foreseeable future. Symmetric key encryption methods such as the Advanced Encryption Standard (AES) are thought still to be “quantum-safe” with minor modifications. Even with the use of quantum attack strategies such as Grover’s Algorithm [60], a doubling of key size from 128 bits to 256 bits should provide adequate security margin. Hence, we consider distributing 256-bit keys to encrypt network transmissions for sensitive traffic. Where high levels of security are required, a full one-time-pad protocol can be employed where the key size is at least as large as the entire message to be securely transmitted. Henceforth, we specify a key as 256 bits of shared private randomness.

Now we are going to model the atmospheric channel and the resulting key rate. In general, a quantum communication protocol employs a public channel to transmit between two trusted parties, usually called Alice and Bob, and a classical authenticated channel (e.g. radio frequencies) for the post-processing. This work considers the polarisation encoded BB84 protocol with decoy state [61, 62]. In this protocol, random bits are encoded in the polarisation direction of weak coherent optical pulses due to their technological readiness compared with true single-photon sources [63, 64]. The decoy state method allows Alice and Bob to catch eavesdropping on the coherent pulse’s Poissonian photon number statistics, in particular, the so-called photon number splitting attack [65], by precisely estimating the gain, Q_n , and the error rate, e_n of different photon number components. The *gain* of the n -photons state is defined as the ratio between the number of events detected by Bob and the number of n -photons state emitted by Alice. Precise gain estimation for all the photon number components can be achieved if Alice sends an additional set of states called decoy states with different amplitudes from the signals one. Such a set is used to monitor the channel and to detect eavesdropping activities while the signal state is used to generate the key. It is important to note that the signal and decoy are chosen at random by Alice, so an attacker does not have the information on the current states of the signal and decoy. Decoy state-based protocols allow for improved performance when compared to the standard BB84 over high loss channels, and therefore they are suitable for space-based QKD. In what follows, we neglect the finite key-size effects and assume that enough raw key can be buffered to allow for efficient privacy amplification. The Gottesman-Lo-Lütkenhaus-Preskill can be used [66] to derive a lower bound on the key generation rate. Furthermore, we ignore the classical communication required for post-processing as it is

not the material to optimisation. The expression for the rate of secret key for the BB84 protocol with decoy state is given by [61, 62]:

$$K > Rq(Q_1(1 - H_2(e_1)) - Q_\mu f H_2(e_1)), \quad (3)$$

where q is a parameter that accounts for the choice of the BB84 basis, R is the repetition rate, f is a factor related to the error correction efficiency and H_2 is the binary entropy. Furthermore, Q_1 and e_1 can be bounded using experimentally measured quantities, such as the gain and error rate of the signal and decoy states (Q_μ , Q_ν and E_μ , E_ν):

$$Q_1 > \frac{\mu^2 e^{-\mu}}{\nu(\mu - \nu)} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right) \quad (4)$$

and

$$e_1 < \frac{\mu(E_\nu Q_\nu e^\nu - e_0 Y_0) e^{-\mu}}{Q_1 \nu}. \quad (5)$$

Once the repetition rate and the signal and decoy state intensities are fixed, the key rate can be regarded as a function of the total channel loss, and the background counts Y_0 , both of them contribute to the decrease of the overall communication rate. The former decreases the detection probabilities of the signal and the decoy state, while the latter increases the error rate. In what follows, we review the primary source of losses and background counts in a SatQKD scenario.

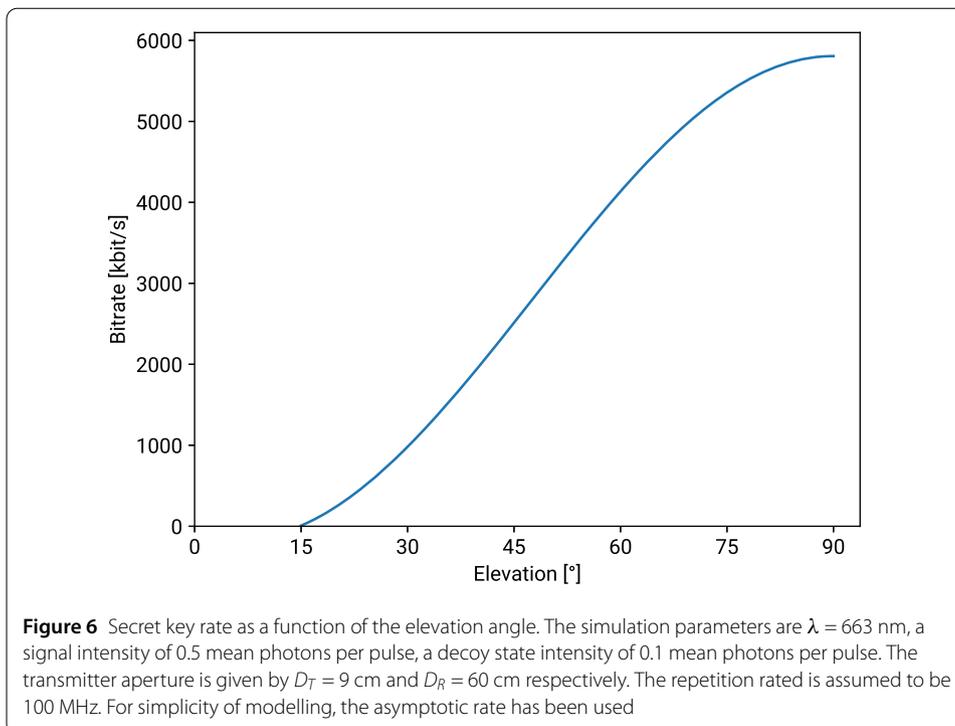
Contrary to the fibre case, in the satellite-based communication scenario, the leading source of loss is diffraction [67]:

$$L_G = -20 \log \frac{D_R}{D_T + \omega_{\text{div}} R}, \quad (6)$$

where D_T (D_R) is the transmitter (receiver) aperture, ω_{div} the beam divergence and R the range between the transmitter and the receiver. The latter expression leads to a quadratic decrease of the coherent state intensity with the distance travelled by the optical beam. Atmospheric scattering and absorption can be expressed as [67]:

$$L_\lambda = T_\lambda \csc \theta, \quad (7)$$

where T_λ is the transmissivity that depends on the wavelength of the signal, and θ is the elevation angle. Fluctuations of the local atmospheric refractive index due to turbulence also cause losses especially close to the horizon, but they are less significant compared to the uplink scenario [68] and can be ignored in the initial approximation. For the simulation parameters considered, the overall link losses range from ~ 35 dB at the elevation of 15° and decrease to about ~ 25 dB at the zenith, this is due to the fact that the length of the slant path travelled by the beam in the atmosphere decreases with increasing elevation, and so does the thickness of the atmospheric layer. Spurious counts are due to the dark counts of the detectors and electronics and from stray light e.g. light pollution or scattered light from the Moon. A typical value for dark counts is of the order of the tens per second while counts due to stray light depend both on an elevation and a wavelength and can reach the



10^4 counts per second at a low elevation for the visible spectrum. Spurious counts can be mitigated by temporal, spatial and spectral filtering, in what follows we assume 1 ns gating window, a 1 mrad field of view, and a 1 nm spectral bandwidth; after filtering we assume background rate of Y_0 of 10^{-5} counts per pulse.

Overall, the transmission rate is measured in 256-bit keys. Data is transferred using a laser with a wavelength of 633 nm (to reduce diffraction loss compared with longer wavelengths) corresponding to absorption and scattering losses at the zenith of $T_{633} = 1.6$ dB [69], the signal and decoy state of 0.5 and 0.1 mean photon number per pulse respectively, the vacuum state is also used as a decoy state in this context. The repetition rate is set to 100 MHz, similar to that demonstrated on Micius. In a downlink scenario the transmitter aperture is subject to stringent constraints, here we assume an aperture of $D_T = 9$ cm, a value compatible with a CubeSat platform, while the receiver aperture is assumed to be $D_R = 60$ cm corresponding to the aperture of the UK's NERC laser ranging facility of Herstmonceux in East Sussex. Moreover, we assume the elevation angle between the satellite and the ground station needs to be above 15° for an optical connection to be established. Figure 6 shows the assumed secret key rate as a function of the elevation angle used in the simulation. Intuitively the rate vanishes for elevation angles smaller than 15° . The QBER at 15° is about 6% and it decreases to less than 4% at 40° above the horizon. The rate increases with the elevation up to around 6 kbit/s, this is due to the reduced overall losses in the channel as elevation increases.

A.2 Orbital configuration and ground station visibility

The initial orbital parameters are reported in Sect. 4.2. Besides the right ascension of the ascending node and the argument of the latitude, the orbital parameters remain constant.

The right ascension of the ascending node at time t is computed according to Equation (8).

$$\Omega(t) = \Omega_0 - \frac{3}{2} n J_2 \frac{R_{\oplus}^2}{p} \cos i, \quad (8)$$

Equation (9) defines the argument of the latitude at time t .

$$u(t) = u_0 + \omega t. \quad (9)$$

Both equations were derived in [70] and their symbols are explained below:

Ω_0 Initial right ascension of the ascending node, values between 90.5° and 115.5° were evaluated in the design of an experiment to select the most efficient orbital configuration, see Sect. 4.2 for more details.

n Mean motion of the satellite, $n = \sqrt{\mu_{\oplus}/a^3}$, where μ_{\oplus} is the Earth's gravitational parameter, $\mu_{\oplus} = 3.986 \cdot 10^{14} \text{ m}^3/\text{s}^2$.

J_2 Second zonal harmonic of the Earth's gravitational field, $J_2 = 1.0826 \cdot 10^{-3}$.

R_{\oplus} Earth's radius, $R_{\oplus} = 6378.136 \text{ km}$.

p Semilatus rectum, $p = a(1 - e^2)$.

a Semi-major axis, $a = 6945.033 \text{ km}$.

e Eccentricity, $e = 0^\circ$.

i Inclination, $i = 97.658^\circ$.

ω Circular orbit velocity of the satellite on its orbit, computed as $\omega = 2\pi/T$, where $T = 2\pi/n$ is the orbital period of the spacecraft.

u_0 Initial argument of the latitude, $u_0 = 46^\circ$.

The current position of the satellite in an Earth-centered inertial reference frame is then obtained by converting from Keplerian elements to cartesian position \mathbf{r} and velocity \mathbf{v} , at time steps of one second.

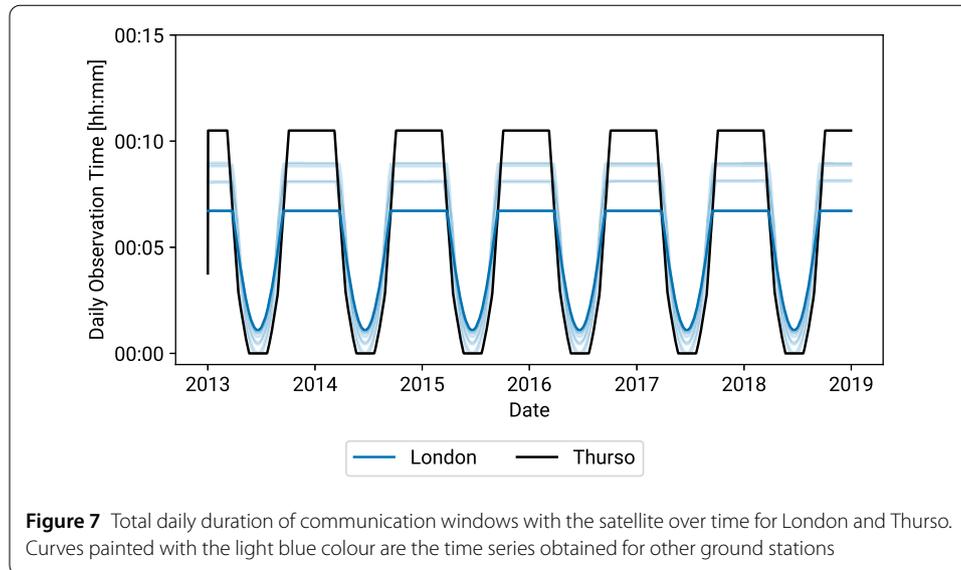
The visibility of the satellite from each ground station, at each time step, is then assessed with the following method:

1. The Greenwich Mean Sidereal Time (GMST), θ_{GMST} , is computed at each time step t [70].
2. Using $\theta_{\text{GMST}}(t)$ and the longitude λ of the considered ground station, the Local Sidereal Time (LST), θ_{LST} , is computed.
3. Using θ_{LST} and ϕ , the latitude of the considered ground station, the position \mathbf{r}_{GS} of the ground station in the Earth-centered inertial reference frame can be computed.
4. From \mathbf{r} and \mathbf{r}_{GS} it is possible to compute the relative position of the spacecraft from the ground station as $\rho_{\text{GS}} = \mathbf{r} - \mathbf{r}_{\text{GS}}$.
5. From ρ_{GS} it is possible to compute the elevation El of the spacecraft with respect to the ground station.
6. If $El > 15^\circ$, then the spacecraft is assumed to be visible from the considered ground station.

Steps 4 and 5 were computed using the SGP4 library [71].

A.3 Communication windows

A communication window for a given ground station is defined as the time interval which occurs at night when the satellite is not in sunlit, and the elevation angle between the station and the spacecraft is greater or equal to 15° . Periods, when the satellite remains



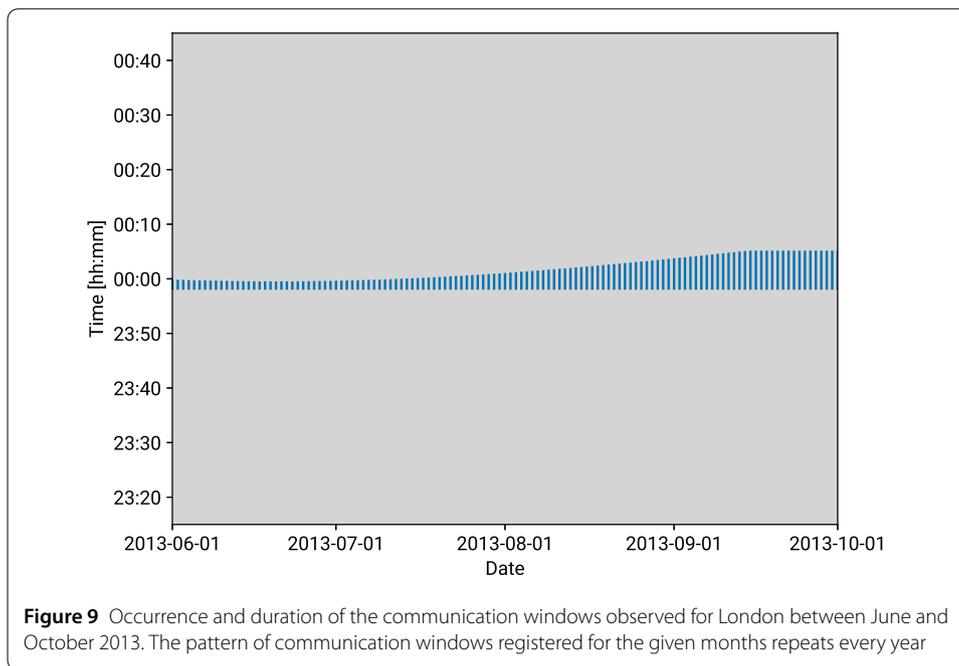
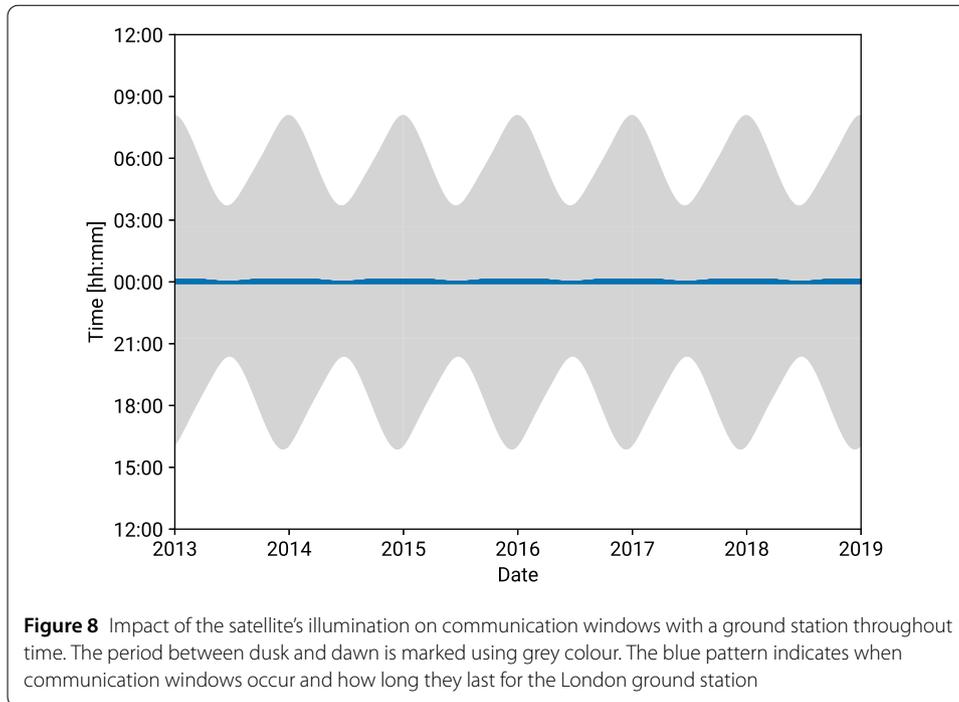
in umbra, were computed using the conical shadow model [72]. Note, the definition does not mention weather conditions which influence the actual data transfer rate. This subject is explored in Sect. A.4.

Figure 7 illustrates the cumulative duration of communication windows aggregated per day for each ground station between the years 2013 and 2019.

The latitude of a ground station determines the number of communication windows with the satellite and their cumulative duration. Stations located at low latitudes, such as Bristol, London and Birmingham, observe one communication window throughout the year. It occurs around midnight. Ground stations at higher altitudes may register another intermittent communication window which disappears in summer due to illumination of the satellite. Consequently, those ground stations experience a longer cumulative duration of communication windows in winter. On the other hand, they are also the most affected by the increase in satellite illumination observed in summer. Overall, that phenomenon causes a notable reduction in the span of communication windows across all locations. For instance, Glasgow and Thurso, in particular, which are the ground stations with the highest latitudes, completely lose the opportunity to communicate with the satellite for some weeks during summer. The period when Glasgow remains disconnected from the satellite lasts between the 7th of June and the 3rd of July. Thurso experiences the blackout from the 22th of May until the 21st of July. The pattern of appearance and the duration of the communication windows observed by a given ground station repeat every year.

Figures 8 and 9 display when communication windows occur and how they change over time for the London ground station due to satellite illumination. The UTC time is presented on the Y-axis instead of the local time to avoid disruptions caused by daylight saving time shifts. Long-term changes in the night time are visualised in Fig. 8, whereas the variable duration of communication windows is illustrated in Fig. 9, which presents the same data but is zoomed in a particular region of the timeline.

Several phenomena governing the behaviour of communication windows could be inferred from both figures. Communication windows commence at the same time every night. The lack of the drift is a consequence of the precise setting of the orbit altitude. The duration of communication windows varies over summer due to changes in satellite



illumination. The shortest communication window is observed during nights from the 17th until the 23rd of June and lasts 67 sec. On the other hand, the longest communication window lasts 403 sec, and it remains stable for more than six months, between the 15th of September and the 26th of March. Although the exact values are different, the overall trend in communication windows' behaviour presented here is observed for every ground station. Due to setting the orbit inclination to eliminate the drift in RAAN accumulated throughout a year because of Earth's precession, the same pattern of communication win-

dows repeats over time. To conclude, the seasonal changes in satellite illumination increase the importance of selecting appropriate orbital parameters of the satellite to obtain the desired timing and frequency of communication windows.

A.4 Weather model

To model the influence of weather conditions on the transfer rate, we were interested in cloud cover recorded over the ground stations considered in the study between the years 2013 and 2019. Weather information as a bulk of historical observations was purchased from OpenWeatherMap [73]. The company redistributes data collected from a network of privately owned weather stations connected to the OpenWeatherMap platform. The data set was normalised to a single stream of records for each city updated every hour. Cloud cover was encoded as an integer value in the interval $[0, 100]$. The cloudless sky was represented as 0, whereas overcast corresponds to 100. Additional comments in the data set, such as *moderate rain* or *scatter clouds* indicated more precisely the exact weather conditions at any given moment. For our purpose, we consider measuring cloud cover as a percentage value more convenient than using Oktas units, whose coarse-grained resolution follows a discrete scale ranging from 0 to 9. Meteorological offices [74] adopt the latter approach.

Time series of cloud cover observed by ground stations during communication windows between 2016 and 2019 are presented in Fig. 10. We limit the displayed period to the second half of the six years time frame considered in the study. Otherwise, the plot may be difficult to read because of swift changes in cloud cover.

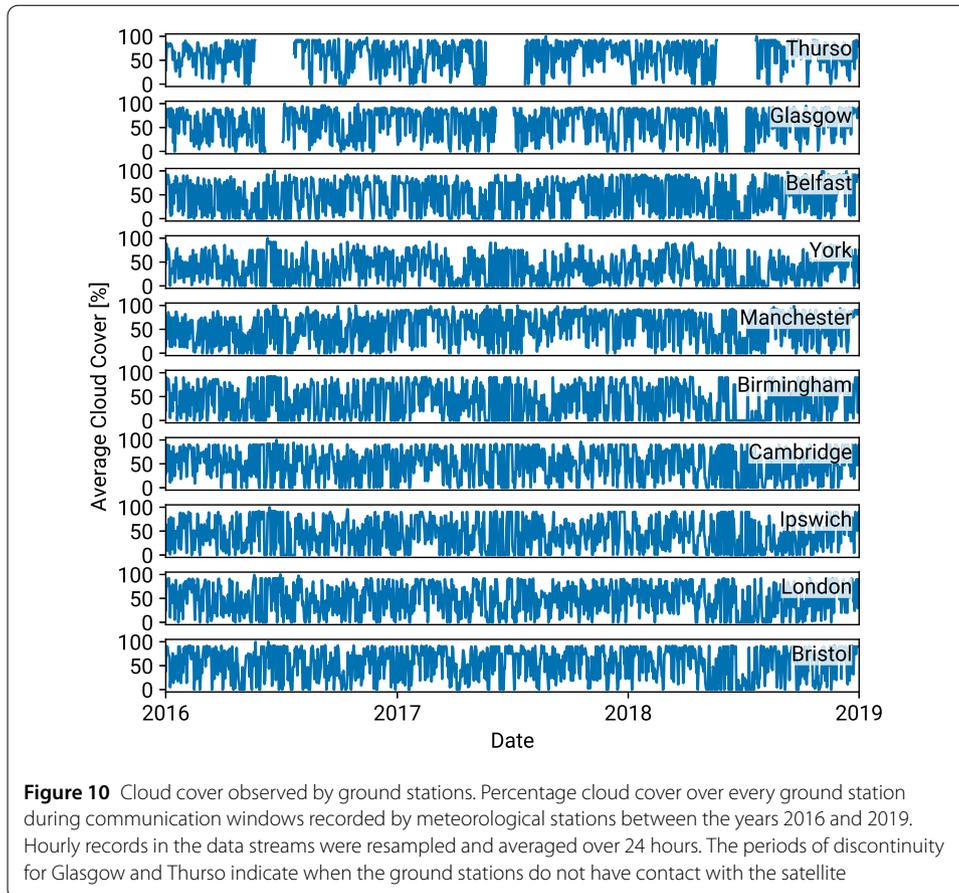
Having analysed the figure, it is immediately apparent that the sky over the UK is seldom transparent, and rapid changes which alternate between cloudless sky and overcast are frequent. Intuitively, since all ground stations are located in the same country, the cloud cover measurements are correlated.

Figure 11 illustrates Pearson's correlation coefficient of the cloud cover measurements between each pair of ground stations. Several phenomena are worth pointing out. Firstly, ground stations located nearby, in particular, those based in South and East England (London, Ipswich and Cambridge) exhibit strong correlation (above 0.5). Secondly, every ground station besides Thurso has a neighbour with whom it is at least moderately correlated (above 0.3). Finally, Thurso observes a distinctive pattern of cloud cover, which is not replicated by any other ground station. It is conceivable, as the city is located in a remote area and does not have a close neighbour.

A.4.1 Impact of cloud cover

The assumption that the sky must be completely unobstructed by clouds as a prerequisite for a successful transmission seems to be overly restrictive for a space-to-ground communications system located in the UK. Therefore, we assume that the communication system in our study continues being operational in the event of partial cloud cover. However, its efficiency in terms of the transmission rate deteriorates as cloud cover increases. The following formula governs the relationship between cloud cover and the transmission rate.

Formally, let $t(El)$ be the expected key transmission rate for the elevation angle El and the clear sky. We assume that in the presence of some cloud cover $\gamma \in [0, 100]$ Formula (10)



approximates the key transfer rate.

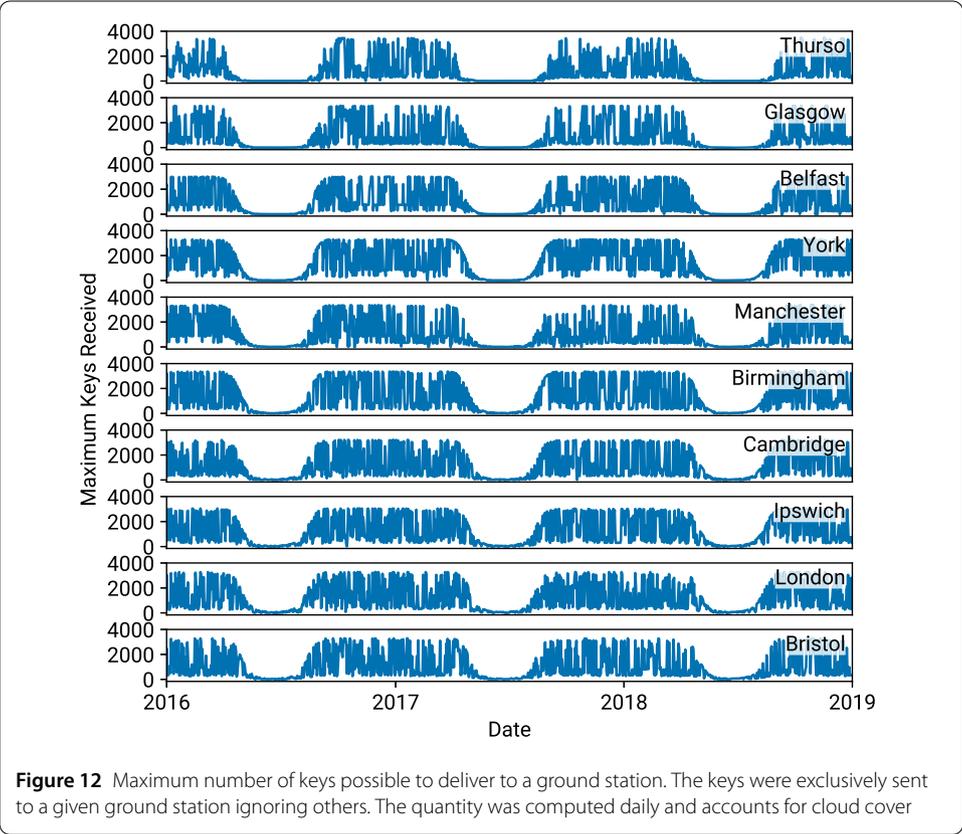
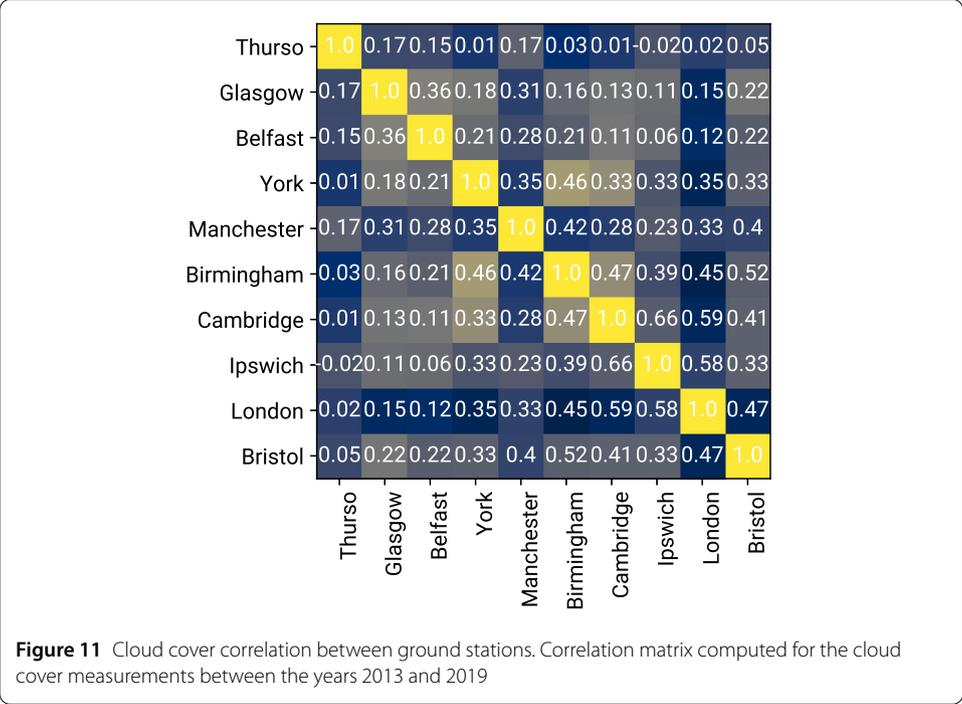
$$t'(El, \gamma) = \frac{100 - \gamma}{100} \cdot t(El). \quad (10)$$

Therefore, the transmission rate decreases linearly as cloud cover increases. The same formula for the loss of the transfer rate due to cloud cover was used by [32, 48] who studied the problem of selecting the network of optical ground stations. In a similar vein, the decay of solar irradiance can also be modelled as a linear function of cloud cover [75].

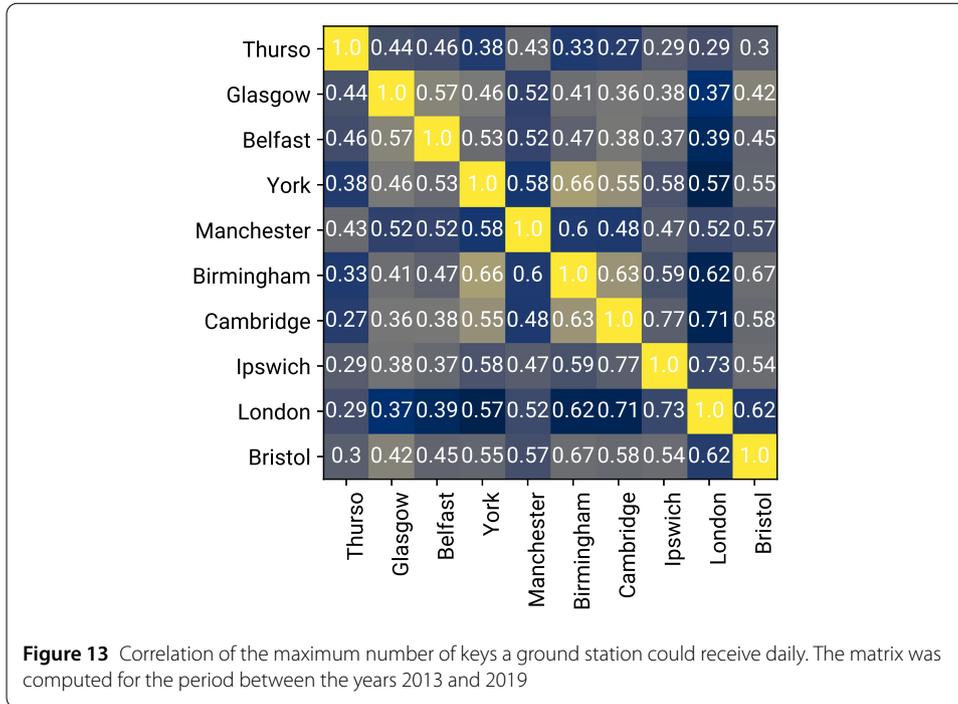
Figure 12 illustrates the maximum number of keys that is possible to deliver to a ground station, taking into account the influence of cloud cover exerted on the transfer rate. As in Fig. 10, we limit the time frame displayed to the last three years considered in the study to improve the readability of the plot. It does not incur any loss of information because the same pattern is observed also during the first three years.

Overall, there are no visually discernible differences between ground stations in the number of keys that is possible to deliver. Increased satellite illumination observed from April until September causes a significant reduction in communication capability. The higher the latitude of the ground station, the more affected it is. For instance, grounds stations above Belfast are disconnected for at least one month in summer. The system achieves optimal performance between October and March. During that period, adverse weather conditions cause intermittent fluctuations in the number of keys delivered.

Figure 13 displays the correlation matrix for information presented in Fig. 12.



The correlation coefficient evaluated for every pair of ground stations assumes values in the range [0.27, 0.77]. Consequently, every pair of ground stations is at least weakly



correlated. Furthermore, if we consider only ground stations located in England, the correlation will be moderate or strong (0.48 and above). Similar to Fig. 11, Thurso is the least correlated ground station. To conclude, the periods of either favourable or adverse conditions affecting the number of keys possible to deliver are observed for all ground stations roughly at the same time.

Appendix B: Optimisation problem formulation

The section opens with the outline of the approach adopted to model the scheduling of data transfers to ground stations. The definition of the notation and symbols, which are used to describe a feasible schedule, follows next. Finding the best schedule according to the number of keys possible to use is the objective of the optimisation problem, which is described in the final part.

The main idea behind the problem formulation is splitting the planning horizon into intervals which denote periods allocated for transferring data to a given ground station. An interval assigned to the auxiliary station models the time spent on switching between consecutive data transfers to regular ground stations. Since in practice the amount of data transferred to a ground station in a long continuous interval will be the same if the interval is partitioned into subintervals and replaced by them, we can assume the intervals of regular ground stations do not overlap. On the other hand, elements in the set of intervals that can potentially be allocated to the auxiliary station do overlap because it simplifies the formulation as one interval can be used to model the switching period preceding a data transfer. Without loss of generality, intervals may have a variable length duration.

Let us extend the notation and symbols introduced to define the traffic index in Sect. 3. The syntax $[i, j)$ indicates an interval starting at the time point i and ending before the time j . Therefore, intervals are always considered opened on the right side. Intervals of

zero length, such as $[i, i]$, begin and end at the same time. The notation $t \in [i, j]$ denotes enumeration over the set of time points $i, \dots, j - 1$ contained within the interval.

Consider the following symbols.

- I^n Set of time intervals available for an assignment to a ground station $n \in \bar{N}$.
- x_{ij}^n Binary decision variable indicating whether the interval $[i, j]$ is assigned to the ground station n .
- $k^n(i, j)$ Function returning the number of keys that could be sent to the ground station n during the interval $[i, j]$.
- $s(t)$ Function returning the start of the switching period required to commence the data transfer at the time t . For instance, if the interval $[i, j]$ opens a sequence of intervals tracking a data transfer to a ground station $n \in N$, then the interval $[s(i), i]$ must be scheduled as the switching period.
- t_{\min}, t_{\max} Begin and end of the planning horizon.

B.1 Schedule instance

The following constraints define the set of valid schedules.

$$X = \begin{cases} \sum_{n \in \bar{N}} \sum_{[i,j] \in I^n: i \leq t < j} x_{ij}^n \leq 1 & \forall t \in T : t_{\min} \leq t < t_{\max} & (11) \\ x_{jk}^n \leq x_{ij}^n + x_{s(j)j}^0 & \forall [i, j], [j, k] \in I^n, \forall n \in \bar{N} & (12) \\ \mathbf{x} \in \mathbb{B}^{|\mathcal{N}|} & & \end{cases}$$

Variables x_{ij}^n encode whether an interval $[i, j] \in I^n$ is selected for the given station $n \in N$, hence they are binary. Constraint (11) ensures every time in the planning horizon at most one interval is active. Constraint (12) asserts that the required switching period before starting the next data transfer is respected. In particular, if data is sent to the ground station n at the interval $[j, k)$, then either the preceding interval $[i, j)$ is also scheduled for the same transmission, or the requested switch is executed for the entire duration of the interval $[s(j), j)$.

The families of constraints above do not include restrictions on the value of the elevation angle and the time of a day required for a successful data transfer to happen. Both constraints are handled implicitly in the definition of the functions $k^n(\cdot) \forall n \in N$ and by considering only these intervals in which data transfer is possible. Therefore, periods during which elevation angles for all ground stations are below the minimum threshold are removed. The same holds for day time overlapping for all ground stations and the periods when the satellite is illuminated. The scenarios in which a data transfer is possible to some, but not all, ground stations are handled in the definition of functions $k_n(\cdot) \forall n \in N$. For example, if at midnight in London the elevation angle is above the minimum allowed value, but it remains below that threshold in Thurso, the function $k^{\text{Thurso}}(t)$ will return zero because initial conditions for a successful data transfer are not satisfied. Furthermore, the functions $k^n(\cdot)$ account for cloud cover by lowering the number of keys accordingly.

For succinctness and convenience, the set of schedules which satisfy Constraints (11), (12) is referred to as X .

B.2 Optimisation problem

The optimisation problem is formulated as a Mixed-Integer Program with a linear objective function, linear constraints and binary variables. The optimisation objective is finding

a schedule which performs a distribution of keys that maximises the number of usable keys in the communications system measured by the traffic index.

The optimisation model is formulated below.

$$\max \sum_{t \in T} \lambda_t$$

$$b_t^n = \sum_{[i,j] \in I^n; j \leq t} k^n(i,j) x_{ij}^n + \underline{b} \quad \forall n \in N, \forall t \in T \quad (13)$$

$$w_n \lambda_t \leq b_t^n - \underline{b} \quad \forall n \in N, \forall t \in T \quad (14)$$

$$\mathbf{x} \in X \quad (15)$$

$$\mathbf{x} \in \mathbb{B}^{\bar{N}|I^n|}, \quad \lambda \in \mathbb{R}_+^{|T|} \cup \{0\} \quad (16)$$

Constraint (13) updates the size of the key buffer a ground station holds by the number of keys delivered to the ground station until the time t . Constraint (14) bounds the product of the traffic index λ_t and the weight assigned to the ground station n , which is the usable number of keys the ground station holds, by the number of keys available in the ground station's buffer at the time t . Constraint (15) ensures only valid schedules are considered. Finally, Constraint (16) declares types of variables used in the formulation.

The formulation has $\sum_{n \in \bar{N}} |I^n|$ binary decision variables, $|T|$ continuous decision variables and $2|\bar{N}||T| + 1$ constraints, including Constraint (15), which is not a linear inequality. It can be decomposed into $\sum_{n \in \bar{N}} |I^n| + |\bigcup_{n \in N} I^n|$ linear inequalities. Solving the formulation by naïve enumeration has the complexity of $O(|\bar{N}|^{|\bigcup_{n \in N} I^n|})$. It corresponds to the selection of one out of \bar{N} conflicting ground station for each of $|\bigcup_{n \in N} I^n|$ time segments. Nonetheless, the linear programming relaxation of the model, which is solvable in polynomial time, in conjunction with cuts automatically generated by the MIP solver, consistently derived strong upper bounds at the root node of the branch-and-bound tree for all of the problem instances considered. Overall, we evaluated 26 orbital configurations and 10 variants with weights perturbations. For each setting, it involved solving six scheduling problems, which yields 216 instances solved in total. Overall, the average and the worst case gap at the root node were 1.00% and 1.84%, respectively. This result demonstrates the strength of the formulation, and it is independent of the hardware used to solve the model.

B.3 Implementation details

The model was implemented in C++ using Gurobi MIP solver [76]. Time intervals for encoding a transfer to a regular ground station were 15 seconds long and aligned with the UTC time, so four such intervals fully covered one minute. On the other hand, switching between data transfers was modelled using continuous intervals whose duration exactly matched the period required to complete the switch. Consequently, such intervals were of variable length. Depending on the location within a communication window, their span could vary from zero at the beginning of the window to at most 30 seconds as the distance from the start of the window increased. For more implementation details, see the source code repository [77] which contains all software developed for this study.

Acknowledgements

The authors are grateful to anonymous referees for their insightful comments which led to significant improvements of the paper. The authors also thank Cristian Greco for his useful suggestions in the implementation of the simulation environment.

Funding

MP was funded by a stipend from the University of Strathclyde. DO is supported by EPSRC grant EP/T517288/1. The work is supported by the EPSRC Quantum Technology Hub in Quantum Communications under the Partnership Resource, the Quantum Communications Hub Grant No. EP/M013472/1, the UK Space Agency under grant NSTP3-FT-063, and the COST Action QTSpace (CA15220). The sixth author was supported by United States Air Force (Grant No. FA9550-17-1-0105).

Abbreviations

AES, Advanced Encryption Standard; AFSCN, Airforce Satellite Control Network; EO, Earth Observations; GMST, Greenwich Mean Sidereal Time; HSBB, High-Speed Broadband; LEO, Lower Earth Orbit; LS, Local Search; LST, Local Sidereal Time; MaxPDT, Maximum Percentage Data Transferred; MILP, Mixed-Integer Linear Program; MIP, Mixed-Integer Program; QKD, Quantum Key Distribution; RAAN, Right Ascension of the Ascending Node; RSA, Rivest-Shamir-Adleman; SatQKD, Satellite Quantum Key Distribution; SL, Service Level; SSO, Sun-Synchronous Orbit; UTC, Coordinated Universal Time.

Availability of data and materials

Software developed for the study [77] is available open-source under the MIT License. The data sets generated for this work and analysed in the article are available for download using the link [59].

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

MP implemented software, performed numerical simulations and was a major contributor in writing the manuscript. LM contributed to the initiation of the research, simulated the channel model key rate, and contributed to writing and revising the manuscript. MDC contributed to the definition of the dynamical model of the satellite and the ground stations' visibility analysis. DO contributed to the initiation of the research, introduction, comment and revision of the paper. AR contributed to the initiation of the research, formulation of the optimisation problem, comment and revision of the manuscript. AA contributed to the formulation of the optimisation problem, comment and revision of the manuscript. All authors read and approved the final manuscript.

Author details

¹Department of Mechanical and Aerospace Engineering, University of Strathclyde, Glasgow, United Kingdom. ²SUPA Department of Physics, University of Strathclyde, Glasgow, United Kingdom. ³Strathclyde Business School, University of Strathclyde, Glasgow, United Kingdom.

Endnotes

- ^a The Rivest-Shamir-Adleman (RSA) public-key cryptosystem or Elliptic Curve protocols [78].
- ^b Untrusted-node SatQKD is possible by distributing entangled photon pairs simultaneously to both parties who can then extract a secure key from the measured quantum correlations without assuming that the satellite is secure. The secrecy of the distributed key can be tested by the violation of a Bell inequality [79, 80].
- ^c We note that the UKQNTel link between Cambridge and Ipswich has been established and will form part of a planned QKD fibre-based network connecting to London and Bristol using intermediate trusted nodes. One could consider treating such subsets of ground station sites as a super-node. Such techniques have been proposed for conventional satellite-Earth laser communications for weather mitigation. In this study, we have chosen to keep the problem simple and consider each site as independent.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 17 July 2019 Accepted: 21 January 2020 Published online: 31 January 2020

References

- Wootters WK, Zurek WH. A single quantum cannot be cloned. *Nature*. 1982;299(5886):802–3. <https://doi.org/10.1038/299802a0>.
- Bennett C, Brassard G. In: *Withdrawn: quantum cryptography: public key distribution and coin tossing*. vol. 560. 1984. p. 175–9. <https://doi.org/10.1016/j.tcs.2011.08.039>.
- Zhang Z, Zhao Q, Razavi M, Ma X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys Rev A*. 2017;95:012333. <https://doi.org/10.1103/PhysRevA.95.012333>.
- Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. *npj Quantum Inf*. 2016;2(1):16025. <https://doi.org/10.1038/npjqi.2016.25>.
- Lim CCW, Curty M, Walenta N, Xu F, Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. *Phys Rev A*. 2014;89:022307. <https://doi.org/10.1103/PhysRevA.89.022307>.
- Wonfor A, Qin H, Kumar R, Tang X, Dynes JF, Shields AJ, Pentry RV, White IH. Field trial of a QKD and high-speed classical data hybrid metropolitan network (conference presentation). In: Dingel BB, Tsukamoto K, Mikroulis S, editors. *Broadband access communication technologies XII*. SPIE, vol. 10559. San Francisco: International Society for Optics and Photonics; 2018. <https://doi.org/10.1117/12.2290544>.

7. Valivarthi R, Puigibert MIG, Zhou Q, Aguilar GH, Verma VB, Marsili F, Shaw MD, Nam SW, Oblak D, Tittel W. Quantum teleportation across a metropolitan fibre network. *Nat Photonics*. 2016;10:676. <https://doi.org/10.1038/nphoton.2016.180>.
8. Mao Y, Wang B-X, Zhao C, Wang G, Wang R, Wang H, Zhou F, Nie J, Chen Q, Zhao Y, Zhang Q, Zhang J, Chen T-Y, Pan J-W. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt Express*. 2018;26(5):6010–20. <https://doi.org/10.1364/OE.26.006010>.
9. Azuma K, Tamaki K, Lo H-K. All-photon quantum repeaters. *Nat Commun*. 2015;6(1):6787. <https://doi.org/10.1038/ncomms7787>.
10. Donaldson RJ, Mazzarella L, Collins RJ, Jeffers J, Buller GS. A high-gain and high-fidelity coherent state comparison amplifier. *Commun Phys*. 2018;1(1):54. <https://doi.org/10.1038/s42005-018-0054-z>.
11. Mazzarella L, Donaldson RJ, Collins RJ, Zanforlin U, Tatsi G, Buller GS, Jeffers J. Quantum state comparison amplifier with feedforward state correction. In: Stuhler J, Shields AJ, Padgett MJ, editors. *Quantum technologies 2018*. SPIE vol. 10674. Strasbourg: International Society for Optics and Photonics; 2018. p. 153–61. <https://doi.org/10.1117/12.2307818>.
12. Boaron A, Boso G, Rusca D, Vuilliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussi eres F, Li M-J, Nolan D, Martin A, Zbinden H. Secure quantum key distribution over 421 km of optical fiber. *Phys Rev Lett*. 2018;121:190502. <https://doi.org/10.1103/PhysRevLett.121.190502>.
13. Ursin R, Tiefenbacher F, Schmitt-Manderbach T, Weier H, Scheidl T, Lindenthal M, Blauensteiner B, Jennewein T, Perdigues J, Trojek P,  mer B, Furst M, Meyenburg M, Rarity J, Sodnik Z, Barbieri C, Weinfurter H, Zeilinger A. Entanglement-based quantum communication over 144 km. *Nat Phys*. 2007;3(7):481–6. <https://doi.org/10.1038/nphys629>.
14. Gibney E. Chinese satellite is one giant step for the quantum Internet. *Nature*. 2016;535(7613):478–9. <https://doi.org/10.1038/535478a>.
15. 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, Jia J-J, Ren G, He D, Zhou Y-L, Zhang X-X, Wang N, Chang X, Zhu Z-C, Liu N-L, Chen Y-A, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-based entanglement distribution over 1200 kilometers. *Science*. 2017;356(6343):1140–4. <https://doi.org/10.1126/science.aan3211>.
16. Ren J-G, Xu P, Yong H-L, Zhang L, Liao S-K, Yin J, Liu W-Y, Cai W-Q, Yang M, Li L, Yang K-X, Han X, Yao Y-Q, Li J, Wu H-Y, Wan S, Liu L, Liu D-Q, Kuang Y-W, He Z-P, Shang P, Guo C, Zheng R-H, Tian K, Zhu Z-C, Liu N-L, Lu C-Y, Shu R, Chen Y-A, Peng C-Z, Wang J-Y, Pan J-W. Ground-to-satellite quantum teleportation. *Nature*. 2017;549:70. <https://doi.org/10.1038/nature23675>.
17. 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, Zhou Y-L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y-A, Liu N-L, Wang X-B, Zhu Z-C, Lu C-Y, Shu R, Peng C-Z, Wang J-Y, Pan J-W. Satellite-to-ground quantum key distribution. *Nature*. 2017;549:43. <https://doi.org/10.1038/nature23655>.
18. Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M, Toyoshima M. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nat Photonics*. 2017;11:502. <https://doi.org/10.1038/nphoton.2017.107>.
19. Jennewein T, Bourgoin JP, Higgins B, Holloway C, Meyer-Scott E, Erven C, Heim B, Yan Z, H ubel H, Weihs G, Choi E, D'Souza I, Hudson D, Laflamme R. QEYSSAT: a mission proposal for a quantum receiver in space. In: Hasan ZU, Hemmer PR, Lee H, Santori CM, editors. *Advances in photonics of quantum computing, memory, and communication VII*. SPIE, vol. 8997. San Francisco: International Society for Optics and Photonics; 2014. p. 21–7. <https://doi.org/10.1117/12.2041693>.
20. Payer M. SES Announces 10 Project Partners in QUARTZ Satellite Cybersecurity Consortium. Last accessed 9/6/2019. <https://www.ses.com/press-release/ses-announces-10-project-partners-quartz-satellite-cybersecurity-consortium>.
21. Pultarova T. Unleashing Quantum Into the World. Last accessed 9/6/2019. <https://eandt.theiet.org/content/articles/2019/04/unleashing-quantum-into-the-world/>.
22. Kerstel E, Gardelein A, Barthelemy M, The CSUG Team, Fink M, Joshi SK, Ursin R. Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technol*. 2018;5(1):6. <https://doi.org/10.1140/epjqt/s40507-018-0070-7>.
23. Haber R, Garbe D, Busch S, Rosenfeld W, Schilling K. Qube—a cubesat for quantum key distribution experiments. Logan, United States. 2018. <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4081>.
24. Science and Technology Facilities Council. UK and Singapore Collaborate on  10m Satellite Project to Develop Next Generation Communications Networks. Last accessed 9/6/2019. <https://stfc.ukri.org/news/uk-and-singapore-collaborate-on-10m-satellite-project/>.
25. Calderaro L, Agnesi C, Dequal D, Vedovato F, Schiavon M, Santamato A, Luceri V, Bianco G, Vallone G, Villoresi P. Space quantum communication with higher orbits. In: *Quantum information and measurement (QIM) V: quantum technologies*. Rome: Optical Society of America; 2019. p. S2A.1. <https://doi.org/10.1364/QIM.2019.S2A.1>.
26. Agnesi C, Calderaro L, Dequal D, Vedovato F, Schiavon M, Santamato A, Luceri V, Bianco G, Vallone G, Villoresi P. Sub-ns timing accuracy for satellite quantum communications. *J Opt Soc Am B*. 2019;36(3):59–64. <https://doi.org/10.1364/JOSAB.36.000859>.
27. Oi DKL, Ling A, Vallone G, Villoresi P, Greenland S, Kerr E, Macdonald M, Weinfurter H, Kuiper H, Charbon E, Ursin R. Cubesat quantum communications mission. *EPJ Quantum Technol*. 2017;4(1):6. <https://doi.org/10.1140/epjqt/s40507-017-0060-1>.
28. Neumann SP, Joshi SK, Fink M, Scheidl T, Blach R, Scharlemann C, Abouagaga S, Bamberg D, Kerstel E, Barthelemy M, Ursin R. Q3sat: quantum communications uplink to a 3u cubesat—feasibility & design. *EPJ Quantum Technol*. 2018;5(1):4. <https://doi.org/10.1140/epjqt/s40507-018-0068-1>.
29. Vergoossen T, Loarte S, Bedington R, Kuiper H, Ling A. Satellite constellations for trusted node QKD networks. 2019. [arXiv:1903.07845](https://arxiv.org/abs/1903.07845).
30. Oi DKL, Ling A, Grieve JA, Jennewein T, Dinkelaker AN, Krutzik M. Nanosatellites for quantum science and technology. *Contemp Phys*. 2017;58(1):25–52. <https://doi.org/10.1080/00107514.2016.1235150>.
31. Fuchs C, Moll F. Ground station network optimization for space-to-ground optical communication links. *J Opt Commun Netw*. 2015;7(12):1148–59. <https://doi.org/10.1364/JOCN.7.001148>.

32. Capelle M, Huguet M-J, Jozefowicz N, Olive X. Optimizing ground station networks for free space optical communications: maximizing the data transfer. *Networks*. 2019;73(2):234–53. <https://doi.org/10.1002/net.21859>.
33. Castaing J. Scheduling downloads for multi-satellite, multi-ground station missions. Logan, United States. 2014. <https://digitalcommons.usu.edu/smallsat/2014/FJRStudentComp/4/>.
34. Marinelli F, Nocella S, Rossi F, Smriglio S. A Lagrangian heuristic for satellite range scheduling with resource constraints. *Comput Oper Res*. 2011;38(11):1572–83. <https://doi.org/10.1016/j.cor.2011.01.016>.
35. Herz E, Campagna J. BridgeSat laser communication scheduling: a case study. 2018. <https://doi.org/10.2514/6.2018-2353>.
36. Pemberton JC, Galiber F III. A constraint-based approach to satellite scheduling. In: DIMACS workshop on constraint programming and large scale discrete optimization. Boston: American Mathematical Society; 2001. p. 101–14.
37. Chen B, Potts CN, Woeginger GJ. In: Du D-Z, Pardalos PM, editors. A review of machine scheduling: complexity, algorithms and approximability. Boston: Springer; 1998. p. 1493–641. https://doi.org/10.1007/978-1-4613-0303-9_25.
38. Drozdowski M. Scheduling multiprocessor tasks—an overview. *Eur J Oper Res*. 1996;94(2):215–30. [https://doi.org/10.1016/0377-2217\(96\)00123-3](https://doi.org/10.1016/0377-2217(96)00123-3).
39. Herroelen W, Reyck BD, Demeulemeester E. Resource-constrained project scheduling: a survey of recent developments. *Comput Oper Res*. 1998;25(4):279–302. [https://doi.org/10.1016/S0305-0548\(97\)00055-5](https://doi.org/10.1016/S0305-0548(97)00055-5).
40. Karapetyan D, Minic SM, Malladi KT, Punnen AP. Satellite downlink scheduling problem: a case study. *Omega*. 2015;53:115–23. <https://doi.org/10.1016/j.omega.2015.01.001>.
41. Khafa F, Sun J, Barolli A, Biberaj A, Barolli L. Genetic algorithms for satellite scheduling problems. *Mob Inf Syst*. 2012;8(4):351–77. <https://doi.org/10.3233/MIS-2012-00153>.
42. Spangelo S, Cutler J, Gilson K, Cohn A. Optimization-based scheduling for the single-satellite, multi-ground station communication problem. *Comput Oper Res*. 2015;57:1–16. <https://doi.org/10.1016/j.cor.2014.11.004>.
43. Han C, Wang X, Song G, Leus R. Scheduling multiple agile Earth observation satellites with multiple observations. 2018. [arXiv:1812.00203](https://arxiv.org/abs/1812.00203).
44. Barbulescu L, Watson J-P, Whitley LD, Howe AE. Scheduling space-ground communications for the air force satellite control network. *J Sched*. 2004;7(1):7–34. <https://doi.org/10.1023/B:JOSH.0000013053.32600.3c>.
45. Barbulescu L, Howe A, Whitley D. Afsch scheduling: how the problem and solution have evolved. *Math Comput Model*. 2006;43(9):1023–37. <https://doi.org/10.1016/j.mcm.2005.12.004>.
46. Stottler R, Richards R. Managed Intelligent Deconfliction and Scheduling for Satellite Communication. 2018. p. 1–7. <https://doi.org/10.1109/AERO.2018.8396654>.
47. Arkali G, Dawande M, Srisankarajah C. Scheduling support times for satellites with overlapping visibilities. *Prod Oper Manag*. 2008;17(2):224–34. <https://doi.org/10.3401/poms.1080.0016>.
48. Mecherle GS. Mitigation of atmospheric effects on terrestrial free-space optical communication systems. In: SPIE. vol. 5338. San Jose: International Society for Optics and Photonics; 2004. p. 102–18. <https://doi.org/10.1117/12.537593>.
49. Khumawala BM. An efficient branch and bound algorithm for the warehouse location problem. *Manag Sci*. 1972;18(12):718–31.
50. Lacoste F, Guérin A, Laurens A, Azema G, Periard C, Grimal D. In: FSO ground network optimization and analysis considering the influence of clouds. 2011. p. 2746–50.
51. Giggenbach D, Epple B, Horwath J, Moll F. In: István F, Bitó J, Bakki P, editors. Optical satellite downlinks to optical ground stations and high-altitude platforms. Berlin: Springer; 2008. p. 331–49. https://doi.org/10.1007/978-3-540-79041-9_18.
52. Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. *npj Quantum Inf*. 2017;3(1):30. <https://doi.org/10.1038/s41534-017-0031-5>.
53. Hayashi M. Finite-block-length analysis in classical and quantum information theory. *Proc Jpn Acad Ser B*. 2017;93(3):9–124. <https://doi.org/10.2183/pjab.93.007>.
54. Chand S, Hsu VN, Sethi S. Forecast, solution, and rolling horizons in operations management problems: a classified bibliography. *Manuf Serv Oper Manag*. 2002;4(1):25–43. <https://doi.org/10.1287/msom.4.1.25.287>.
55. Newman MEJ. Analysis of weighted networks. *Physical Review E*. 2004;70(5). <https://doi.org/10.1103/physreve.70.056131>.
56. Barrat A, Barthélemy M, Pastor-Satorras R, Vespignani A. The architecture of complex weighted networks. *Proc Natl Acad Sci*. 2004;101(11):3747–52. <https://doi.org/10.1073/pnas.0400087101>.
57. The Office of Communications: Connected Nations 2018. Last accessed 15/10/2019. <https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2018>.
58. Highlands and Islands Enterprise: Superfast Broadband. Last accessed 15/10/2019. <http://www.hie.co.uk/regional-information/digital-highlands-and-islands/default.html>.
59. Polnik M. Data Set for Scheduling of Space to Ground Data Transfers. <https://doi.org/10.15129/53077534-9b4e-4c6a-b46b-6518e046c198>. Last accessed 13/11/2019.
60. Grover LK. A fast quantum mechanical algorithm for database search. 1996. [arXiv:quant-ph/9605043](https://arxiv.org/abs/quant-ph/9605043).
61. Lo H-K, Ma X, Chen K. Decoy state quantum key distribution. *Physical Review Letters*. 2005;94(23). <https://doi.org/10.1103/physrevlett.94.230504>.
62. Ma X, Qi B, Zhao Y, Lo H-K. Practical decoy state for quantum key distribution. *Physical Review A*. 2005;72(1). <https://doi.org/10.1103/physreva.72.012326>.
63. Mendoza GJ, Santagati R, Munns J, Hemsley E, Piekarek M, Martín-López E, Marshall GD, Bonneau D, Thompson MG, O'Brien JL. Active temporal and spatial multiplexing of photons. *Optica*. 2016;3(2):127–32. <https://doi.org/10.1364/OPTICA.3.000127>.
64. Mazzarella L, Ticozzi F, Sergienko AV, Vallone G, Villoresi P. Asymmetric architecture for heralded single-photon sources. *Phys Rev A*. 2013;88:023848. <https://doi.org/10.1103/PhysRevA.88.023848>.
65. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. *Phys Rev Lett*. 2000;85:1330–3. <https://doi.org/10.1103/PhysRevLett.85.1330>.
66. Gottesman D, Lo H-K, Lütkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. *Quantum Inf Comput*. 2004;4(5):325–60.

67. Uysal M, Capsoni C, Ghassemlooy Z, Boucouvalas A, Udvary E. Optical wireless communications—an emerging technology. 2017. <https://doi.org/10.1007/978-3-319-30201-0>.
68. Bourgoin J-P, Meyer-Scott E, Higgins B, Helou B, Erven C, Hübel H, Kumar B, Hudson D, D'Souza I, Girard R, Laflamme R, Jennewein T. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J Phys*. 2013;15:1. <https://doi.org/10.1088/1367-2630/15/2/023006>.
69. Berk A, Conforti P, Kennett R, Perkins T, Hawes F, van den Bosch J. MODTRAN6: a major upgrade of the MODTRAN radiative transfer code. In: Velez-Reyes M, Kruse FA, editors. Algorithms and technologies for multispectral, hyperspectral, and ultraspectral imagery XX. SPIE, vol. 9088. Baltimore: International Society for Optics and Photonics; 2014. p. 113–9. <https://doi.org/10.1117/12.2050433>.
70. Vallado DA. Fundamentals of astrodynamics and applications. Hawthorne: Microcosm Press; 2013.
71. Warner D. SGP4 Library—Simplified Perturbations Models. Last accessed 11/3/2019. <https://github.com/dnwrnr/sgp4>.
72. Jia X, Xu M, Pan X, Mao X. Eclipse prediction algorithms for low-earth-orbiting satellites. *IEEE Trans Aerosp Electron Syst*. 2017;53(6):2963–75. <https://doi.org/10.1109/TAES.2017.2722518>.
73. Open Weather Map: Service Homepage. Last accessed 25/1/2019. <https://openweathermap.org>.
74. Met Office, Department for Business, Energy and Industrial Strategy, United Kingdom: How We Measure Cloud. Last accessed 4/3/2019. <https://www.metoffice.gov.uk/guide/weather/observations-guide/how-we-measure-cloud>.
75. Morf H. Sunshine and cloud cover prediction based on Markov processes. *Sol Energy*. 2014;110:615–26. <https://doi.org/10.1016/j.solener.2014.09.044>.
76. Gurobi Optimization L. Gurobi optimizer reference manual. <http://www.gurobi.com>.
77. Polnik M, Di Carlo M. Scheduling of Space to Ground Data Transfers—Source Code Repository. Last accessed 9/3/2019. <https://github.com/pmateusz/quake>.
78. Bos JW, Halderman JA, Heninger N, Moore J, Naehrig M, Wustrow E. Elliptic curve cryptography in practice. In: Christin N, Safavi-Naini R, editors. Financial cryptography and data security. Berlin: Springer; 2014. p. 157–75.
79. Ekert AK. Quantum cryptography based on bell's theorem. *Phys Rev Lett*. 1991;67:661–3. <https://doi.org/10.1103/PhysRevLett.67.661>.
80. Franson JD. Bell inequality for position and time. *Phys Rev Lett*. 1989;62:2205–8. <https://doi.org/10.1103/PhysRevLett.62.2205>.

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► [springeropen.com](https://www.springeropen.com)
