Exploiting Potentialities of Dynamic Satellites for Future Space-based Quantum Network: Downlink Scheduling and Orbital Deployment

Xingyu Wang
National University of Defense Technology

Chen Dong (✉ dongchengfkd@163.com)
National University of Defense Technology https://orcid.org/0000-0003-2745-0258

Tianyi Wu
National University of Defense Technology

Lei Shi
Air Force Engineering University

Boyu Deng
Tsinghua University

Haonan Zhu
Air Force Engineering University

Shanghong Zhao
Air Force Engineering University

Article

Keywords: quantum network, SatQKD, low-Earth orbit (LEO), high-orbit satellite.

Posted Date: October 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-963458/v1

Exploiting potentialities of dynamic satellites for future space-based quantum network: downlink scheduling and orbital deployment

Xingyu Wang [1,2] Chen Dong [1] ✉, Tianyi Wu [1], Lei Shi [2], Boyu Deng [3], Haonan Zhu [2], Shanghong Zhao [2] ✉

With the goal of a space-based quantum network is to have satellites distribute keys between any nodes on the ground, we consider an evolved quantum network from a near-term form, in which a space-based relay, Micius, executes a sequence of Satellite QKD (SatQKD) missions, allowing any two cities to have a shared key. Accordingly, we develop a comprehensive framework integrated with precise orbital modelling and a cloud statistics model to enable a preassessment of SatQKD. Using this framework, we consider three different scheduling strategies and estimate the keys that can be delivered to cities. By the assistance of using different optimizations on scheduling problem formulations, it is possible to allows for the possibility to consider strategies for different missions such as extending connection for distant nodes, prioritized delivery to nodes with higher privileges, and promoting keys utilization. We also provide a comparison of the total number of keys delivered using different-altitude satellites. It is demonstrated that the plan for constructing a low-Earth orbit (LEO) satellite constellation is more efficient than that for employing an expensive high-orbit satellite to an execution of scheduling SatQKD.

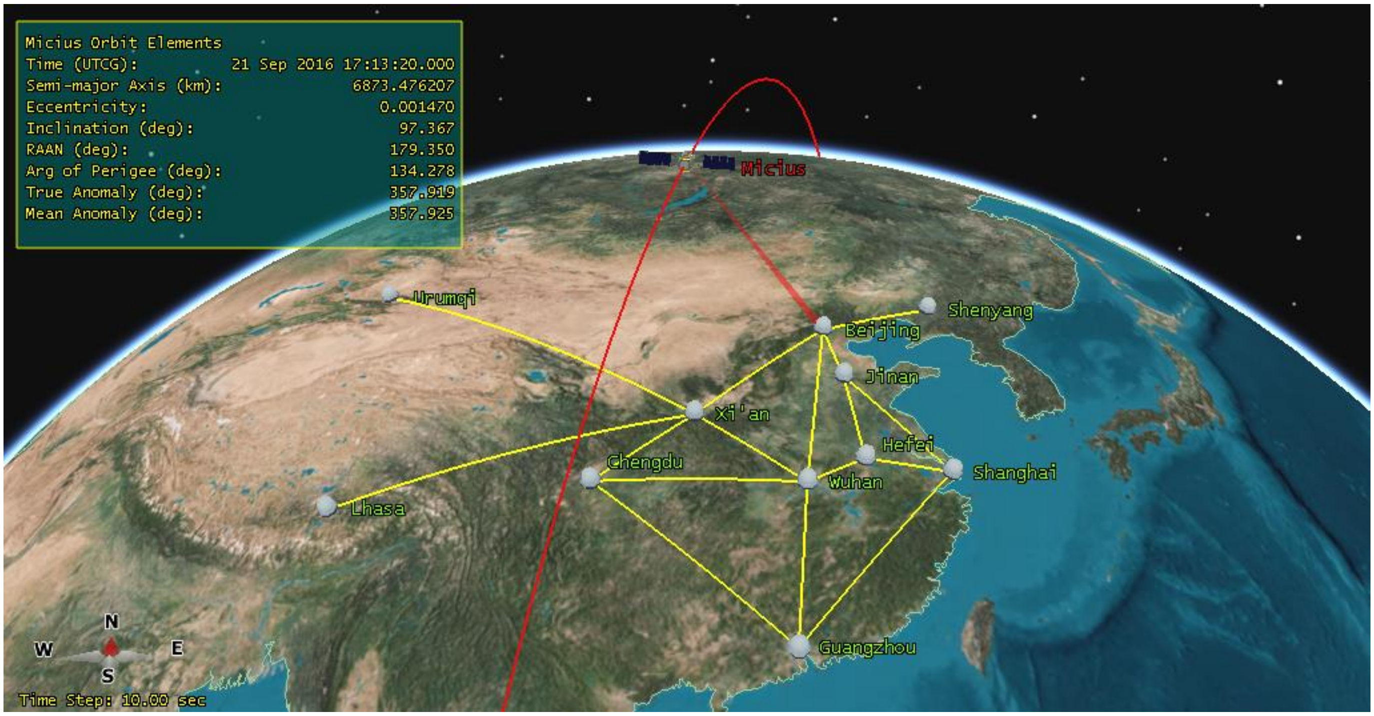
INTRODUCTION

Quantum key distribution (QKD) is a family of protocols that can provide information-theoretic security to share keys between two distant parties[1–3]. In addition to mature fibre-based QKD approaches, free-space QKD has progressed out of laboratories into real-world scenarios[4–7]. Several pioneering experiments[8-11], such as the Chinese Quantum Experiments at Space Scale (QUESS) missions contributing to full in-orbit demonstrations of satellite-based QKD approaches, provide the most feasible option for achieving an ultralong-distance QKD with current technology. Very recently, by integrating fibre and free-space QKD links, a space-to-ground QKD network has been successfully extended to a distant optical ground station (OGS) site, up to a total distance of 4,600 kilometres, which sparked worldwide interest in the design of future global quantum networks[12].

In such an integrated space-to-ground network, fibre-based trusted nodes have been built to extend these limited point-to-point QKD distances from one backbone node to another but are in fixed locations that could be subject to constant surveillance and probes[13]. To remove these fibre-channel risks, one could consider a hypothetical but possible network (illustrated in Fig. 1) adapted from the paradigm, consisting of a space-based mobile platform (i.e., Micius) and selected cities with OGSs (i.e., the built and planned backbone nodes for the future national network). Here, Micius, operates as either a 'trusted node' or an 'untrusted node' and directly mediates the distribution of secure encryption keys pairwise between these cities. The remarkable fact that an 'untrusted node' configuration, such as the implemented entanglement-based QKD[11] or a future space-based measurement device-independent (MDI)[14] QKD, is more secure but feasible only when both OGSs are within the satellite coverage simultaneously. Moreover, although a constellation of satellites that provides a continuous, on-demand entanglement distribution service to cities appears to be viable in the future, the limitation of orbit resources and the costs of construction should be considered before wide deployment[15,16]. Instead, in the current 'trusted node' configuration, Micius carries out QKD operations with distinct OGSs to establish independent keys with each of them and subsequently broadcasts the XOR hash[17] of both delivered keys over a public channel, thus allowing any two cities to have a shared key. Therefore, encrypted communication in such a possible network could be implemented without the need for fibre-based relays.

However, one major challenging bottleneck in putting the network into extensive use is that satellite-based QKD has not been efficient enough to support one-time-pad encryption. In seeking a higher key rate, there have been proposals for free-space continuous-variable (CV) QKD[18] and asymmetric MDI-QKD[19], whereas directly applying these modifications to the space environment is difficult and yet to be achieved. Additionally, the loss of uplink is more severe than that of downlink due to atmospheric properties[20,21]; for example, turbulence may cause the optical beam to wander, which results in a more complicated situation in the two arms of MDI-QKD. Another way to improve the key rate is to raise the technical realization level of space-based QKD systems. It is suggested that a state-of-the-art transmission system installed in a geosynchronous orbit (GEO) satellite could be employed to run 24-hour QKD[22]. Unfortunately, the yields of long-term satellite-based QKD in the daytime are unclear due to cyclical changes in solar radiation[23]. Moreover, improving the experimental settings (e.g., employing a larger lens or a more efficient detector)

[1]Information and Communication College, National University of Defense Technology, Xi'an, 710006, China. [2]School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China. [3]Department of Electronic Engineering, Tsinghua University, Beijing 100084, China. ✉Email: dongchengfkd@163.com; zhaoshangh@aliyun.com



Micius Orbit Elements	
Time (UTCG):	21 Sep 2016 17:13:20.000
Semi-major Axis (km):	6873.476207
Eccentricity:	0.001470
Inclination (deg):	97.367
RAAN (deg):	179.350
Arg of Perigee (deg):	134.278
True Anomaly (deg):	357.919
Mean Anomaly (deg):	357.925

Fig. 1 An illustration of a hypothetical but possible network adapted from the integrated space-to-ground network reported in ref. [12]. The network consists of a space-based mobile platform (i.e., Micius) and 11 selected cities of China with OGSs: Urumqi, Lhasa, Xi'an, Chengdu, Shenyang, Beijing, Jinan, Hefei, Wuhan, Shanghai, and Guangzhou. Considering that the simulation results can help in future in-orbit operations, the actual longitude-latitude-altitude (LLA) data of cities are considered in the scenario, as well as Micius orbit elements (see the embedded table) updated by two-line element (TLE) datasets. Here, the encrypted communication in such a network is assisted by several backbone fibre links (yellow lines), using the satellite as the only trusted relay. In particular, the satellite carries out QKD operations with distinct OGSs to establish independent keys with each of them, and it subsequently broadcasts the XOR hash of both keys over a public channel, allowing any two nodes to have a shared key. Since no fibre-based QKD exists in such a large-scale encrypted communication network, there is an urgent need to address the design of the scheduling strategy of satellite-based QKD for these cities.

is regarded as beneficial for a higher performance, while from a system engineering perspective, a trade-off in determining the space-qualified parameters exists[24].

The other approach is to consider a delay in the delivery of final keys in practice. It was shown in ref. [12] that raw keys downloaded from a satellite can first be stored in a buffer of the OGS and then used for postprocessing after enough have been collected. At present, symmetric key encryption methods such as the Advanced Encryption Standard (AES) are thought to provide 'quantum security' in the foreseeable future. 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. Like the previous works [12,25], we there considered the AES-256 protocol that refreshes the 256-bit final keys every second to share private randomness. Thus, this approach provides an efficient method to achieve encryption and has been adopted in existing QKD networks[26-28]. However, the aforementioned works have been confined to the in-orbit analysis of protocols involving a satellite and one or two OGSs, lacking consideration of the promotion of key generation through satellite applications. Recently, the authors of ref. [29] elegantly extended the idea of scheduling radio downlinks in Earth observation missions to the scenario of satellite-to-ground QKD. By modelling several realistic constraints of space environments, they proposed a formulation to schedule an optical downlink from one satellite to the cities, allocating suitable time to download the number of final keys. Nevertheless, for the given example of a small-scale network scenario, this shows neither the advantage of employing space-based QKD in a long-distance transmission nor a comparative study with different schedule strategies. In addition, note that the view periods of OGSs have variable durations that depend on the geometry of the orbit relative to the OGS. Therefore, modelling incorporating simple circular orbital propagation needs to be modified to close the gap between theory and practice.

In this work, we follow the method of delaying key delivery to address the problem of encryption needs in future large-scale QKD networks. The critical ingredient of the implementation is an improvement in the final key rates by considering a sequence of key delivery missions that the satellite should execute, i.e., a schedule that could be designed by a prior comparison of the results of all possible satellite operations. For this purpose, we develop a comprehensive framework integrated with our designed orbital modelling[21] and a cloud statistics model based on Himawari-8 data statistics[30]. Using this framework, we consider three different scheduling strategies and estimate the keys that it is possible to deliver to cities. Assigning weights to the cities to quantify the individual needs, we modify the genetic algorithm (GA) [31] to perform the optimizations. With Kullback–Leibler (KL) divergence[32], which progressively tightens the match between the resulting key distribution and the expectations, we find that the strategy of pursuing a distribution of final keys delivered that is coincident with that of the data traffic guarantees the individual needs, further promoting the utilization of the delivered keys. We also provide a comparison of the total number of keys delivered by satellites with different-altitude orbits, which could support decisions involving the orbital selection of future quantum satellites.

RESULTS

Integrating precise orbit modelling and a cloud statistics model to provide a preassessment framework for satellite-based QKD applications.

Scheduling the QKD downlink from a satellite to the cities requires a prior comparison of the expected results of all possible satellite operations to design a sequence of missions that a satellite should execute, ultimately achieving the best performance of the network, measured in terms of keys delivered. What makes satellite applications unique are the time-varying properties of the satellite-to-ground transmission channel, which are critical for the formulation of the optimization problem of scheduling a downlink with the constraints. Thus, a comprehensive modelling framework considering optical beam propagation and

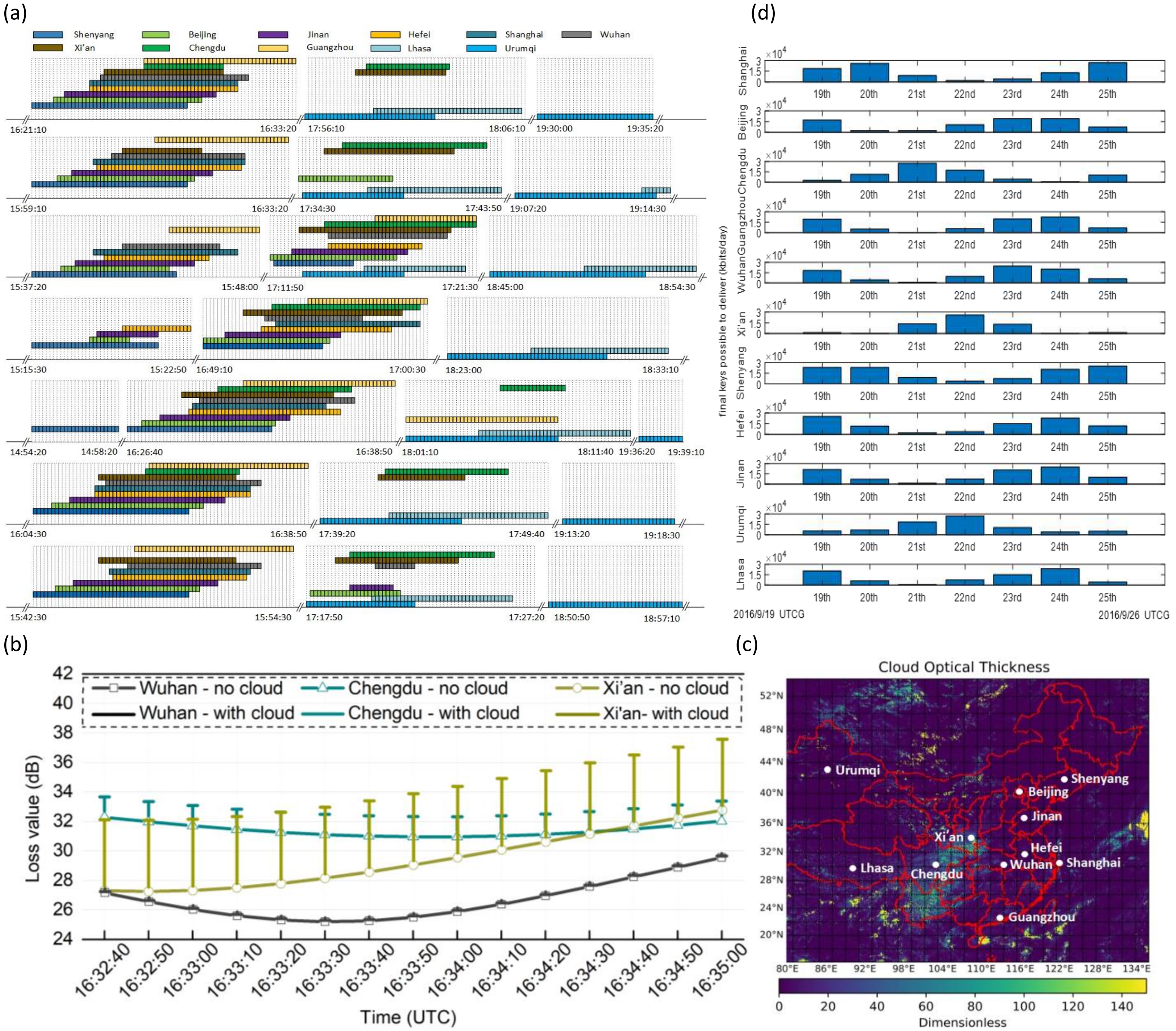


Fig. 2 Results of the framework in the modelling of satellite-to-ground QKD operations during the week of the 19th September, 2016. a. Illustration of the timeline, where the cities that can access Micius in each interval (10 seconds) are labelled with different colours. **b** Variations in the total loss budget during a common-visible interval of the cities Wuhan, Chengdu, and Xi'an. **c** The map of the cloud distribution over China on Sep 23 2016, 16:32:40 UTC**,** which was obtained from the Himawari-8 datasets. The cloud cover statistics for each city were encoded as integer values ranging from 0 to 150. Specifically, the values 0 and 150 correspond to sunny and heavy clouds, respectively. For more details, see the Methods. **d** The expected results of the final keys delivered to the cities on different days of the week**.** For comparison, the sending intensities are the same as those reported in ref. [12], where μ = 0.5, ν = 0.08 and ω = 0, respectively. The source repetition rate M_s is assumed to be 200 MHz, and the other parameters are listed in Table 2.

the satellite orbit will be necessary to minimize gaps in reality. For this, our proposed framework is integrated with the AGI System Toolkit's modelling capabilities, which is achieved by our secondary development of the tool using the code involved. Here, one of the advantages is that the orbital elements of a given satellite could be periodically updated at each time step to cover the orbital drift. As such, the reports of a specific scenario regarding visibility, relative elevation angles and the distance from a satellite to a city are more precise than those obtained from naive circular orbit modelling.

In this work, the week of 19th September, 2016, in Universal Time Coordinated (UTC) format is taken as an example time period to demonstrate a course of Micius flying across cities in China. We simulated the satellite operations under the specific scenario associated with the TLE dataset (see Data Availability) and the experimental settings and estimated the intervals available for access. As depicted in Fig. 2a, the available intervals are separated into two or three durations in the umbra of the sun due to the sun-synchronous orbit cycle. Consistently, within the total of 30 mins available for performing satellite-to-ground QKD per day, cities dispersed in western China, such as Lhasa and Urumqi, could immediately access Micius since they seldom shared their visible windows with other cities. For cities densely distributed in eastern China, preadoption of an appropriate schedule could achieve a reduction the time spent on the handoff resulting from random access.

Although the available intervals are predictable with orbital dynamics, days with severe transmission disturbance resulting from cloudy weather are often excluded from the design of QKD missions. Given that predictions of the link budget, such as the proposals of Pirandola[33] or Villoresi[34], are based on the generalized modelling of various effects, including geometric loss, turbulent disturbance, and atmospheric loss, we modified the modelling calculation by incorporating cloud statistical information and estimated the weather-induced attenuation. Quantitative images of the cloud cover and resulting link budget are illustrated in Fig. 2b and 2c. Notably, the cities of Xi'an and Chengdu on the 23rd suffered from a serious obstruction, and the total budgets in the worst case reached 37.6 dB and 33.8 dB, where the effect of clouds accounted for approximately 4.7 dB and 2.1 dB, respectively. This extra loss will be detrimental to the efficiency in receiving the photons.

To address this issue, by using the results to estimate the key generation rate per time step, we can obtain the possible final keys delivered during an arbitrary interval. For simplicity, the estimation of key rate with Gottesman–Lo–Lütkenhaus–Preskill (GLLP) security[35] is calculated in the asymptotic case. The expected number of keys delivered to the cities on different days of the week is shown in Fig. 2d. As a demonstration, the cities of Xi'an and Chengdu on the 24th have no keys generated, whereas thin clouds over the city of Wuhan promote more final keys to be delivered within the same visible window, which indicates that the situation in which clouds prevent the delivery of raw keys could be mitigated through a flexible schedule. See the "Methods" section for a full description of our framework. In conclusion, not only could our framework be used as a function to further formulate optimization problems but also these assessments related to satellite-to-ground transmissions could be used to obtain a universal design in a future quantum space-based network.

Targeted delivery guarantees the individual needs, further promoting the utilization of delivered keys. The previous section implies that employing a schedule in the network improves the performance in terms of the number of keys delivered, but the question still remains whether performing scheduling from one satellite to cities in the network can meet their different encryption needs. To answer this question, we considered that cities are assigned normalized weights whose values are proportional to a possible network traffic distribution (i.e., data traffic between a city and all other cities relative to the sum of that in the network). After the key downloaded throughout last week is used, each party would remove the delivered key from its trusted key store due to the security requirement that a key cannot be reused. Aiming to maximize the total number of final keys while preserving individual needs, we then adopted different scheduling strategies to deliver keys, including (1) general delivery to the cities without considering the weights (S-GD), pursing only the maximization of the total final keys; (2) prioritized delivery to cities with higher weights (S-PD), ensuring that high-priority tasks are completed first; (3) targeted delivery to cities with distinct weights (S-TD), making the proportions coincident with the network traffic distribution. All these strategies are achieved by using our modified algorithms, which will be introduced later.

Fig. 3a shows the resulting final keys delivered under each strategy for the different cities. The observations made from the results are as follows:

(1) Employing S-GD unsurprisingly improved the total number of final keys beyond that achieved with S-PD or S-TD. Moreover, as a demonstration of the 7,468 kbits delivered to the city of Urumqi, it even embodied the same final keys as that of the fibre-based QKD that relayed at least 5 ideal nodes to the city of Xi'an (see Fig. 3b). However, as shown in Fig. 3d, there is a great difference between the delivered proportion distribution and the expected distribution according to the weights. In fact, the communication between two cities is encrypted by the shared key, which is from the XOR hash of the final keys of a specific city and any destination cities. In other words, the utilization of the delivered final keys is the proportion of the resulting number of shared keys determined by a network traffic distribution to that of the final keys. Consider that their one-week availability, though more final keys were delivered to the Urumqi city or the Lhasa city, delivering final keys that exceeds the individual needs has no substantial improvement on the utilization of keys.

(2) Employing S-PD promoted more final keys being delivered to higher-weighted cities, while the keys could not be promised to be delivered to lower-priority cities. For instance, for the city of Shanghai, the number of final keys delivered by S-PD was 8,332 kbits, achieving a 2,551 kbit gain against S-GD, while no keys were delivered to the cities of Hefei and Jinan. This is due to the iteration

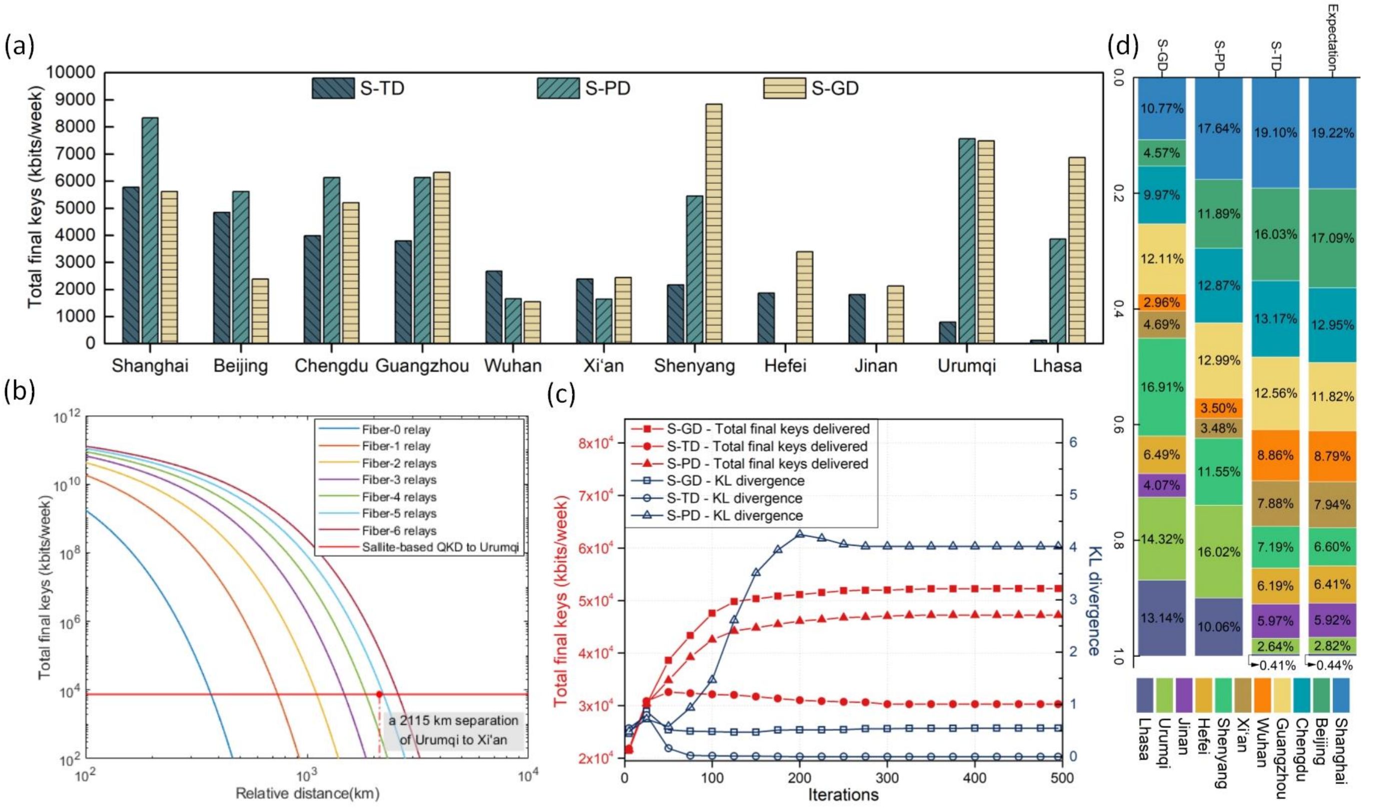


Fig. 3 Comparison of the delivery of the final keys under different scheduling strategies. a. The number of final keys delivered to the cities under different strategies: pursuing a distribution of final keys delivered that is consistent with that of the data traffic (dark green); prioritized delivery to higher-weighted cities (light green); pursuing only the maximization of the total number of final keys (yellow). **b**. A comparison between the total final-key bits in the week and the bits of the fibre-based quantum repeater schemes, where the key rate by fibre-based QKD with G_{rep} ideal relay nodes is given by the PLOB bound $R_{\text{fib}}^{\text{rep}} = -\log_2(1-\sqrt[G_{rep}+1]{\eta_{\text{fib}}})$ [36]. **c**. Comparison of the KL divergence and total final keys for the three different strategies in the iteration procedure. **d**. Comparison of the delivered proportion distributions. For convenience, the values of the assigned weights are temporarily proportional to the population in each city. These values could also be modified by a practical network traffic statistic.

of finding an optimal solution. Specifically, cities with a lower priority, such as Hefei and Jinan, are rarely chosen in cases where a higher-priority city can communicate at the same time. On the other hand, the total number of final keys delivered under S-PD is lower than that under S-GD since a city under the chosen priority level is usually suboptimal in terms of the link loss budget. Therefore, S-PD may be more suitable for different levels of encryption missions.

(3) In contrast, adoption of S-TD not only achieves a flexible schedule to improve the number of final keys delivered but also makes the delivery distribution coincident with the expectation to guarantee individual needs. In Fig. 3d, we further verify the superiority of S-TD by conducting a comparison of the iteration procedure. In the iterative optimization based on the idea of the genetic algorithm, we introduce KL divergence to characterize the degree of matching between the distribution of the delivered final keys and the traffic distribution, which can be represented by[32]

$$D_{KL} = \sum_{n=1}^{N} p(x_n) \log\left[\frac{p(x_n)}{q(x_n)}\right] \quad (1)$$

Here, N is the number of cities, $p(x_n)$ is the proportion of the number of final keys delivered to city i to all that of all cities. $q(x_n)$ is the value of the normalized weight assigned to city i. That is, if two distributions match perfectly, $D_{KL}=0$; otherwise, this variable takes values between 0 and $\inf$. The lower the KL divergence value is, the better matched the distribution of the delivered keys is to the traffic distribution.

When pursuing a higher number of final keys, the KL divergence inevitably increases under S-GD and S-PD, which causes a distribution mismatch, resulting in a lower utilization in practice. Clearly, although the promotion of the total number of final keys delivered under S-TD is lower than the others, the lowest KL divergence indicates the best performance in preserving individual needs. Specifically, the KL divergence under S-TD finally reached 9.7x10-2. Note that a higher degree of matching could be achieved with a finer time step in the time discretization model. From the perspective of practical design, this is also feasible scheduling to avoid inefficient work by a spacecraft with limited coverage time. Moreover, by introducing KL divergence in such iterations, the idea of adopting general divergence-based deep learning algorithms[37] is used to efficiently solve the optimization problems of a network of many ground nodes. The above results validate that scheduling under S-TD has great potential to guarantee individual needs, further promoting the utilization of the delivered final keys.

Table 1. Variations on link budget over the visible duration of the cities for satellites at different orbit types and diffraction angles of satellite-based transmitting telescope.

Orbit type	Total visible duration (s)	Diffraction angle (urad)	Variations on link budget (dB)										
			Shanghai	Beijing	Chengdu	Guangzhou	Wuhan	Xi'an	Shenyang	Hefei	Jinan	Urumqi	Lhasa
LEO (~500km)	12240	1	9.32-14.28	9.65-15.53	9.27-14.51	9.42-14.09	9.36-14.02	9.48-19.9	9.4-15.19	9.46-14.25	9.36-14.32	9.3-17.71	9.35-17.11
		3	11.52-22.28	12.58-23.52	11.47-22.45	12.08-22.07	11.8-22.02	11.65-27.9	11.77-23.22	11.74-22.24	11.79-22.33	11.5-25.71	11.92-25.03
		5	14.79-26.61	15.93-27.84	14.75-26.77	15.53-26.39	15.17-26.35	14.92-32.22	15.09-27.55	15.05-26.56	15.15-26.65	14.78-30.03	15.34-29.34
		10	20.29-32.58	21.45-33.81	20.25-32.74	21.11-32.36	20.71-32.32	20.41-38.19	20.62-33.52	20.56-32.53	20.69-32.62	20.28-36.01	20.91-35.31
MEO1 (~2500km)	45370	1	15.22-Inf	15.33-25.98	14.94-23.07	15-22.51	15.04-23.11	15.12-42.37	15.12-26.79	15.12-22.84	15.15-26.29	15.11-Inf	14.95-Inf
		3	24.04-Inf	24.17-35.34	23.74-32.43	23.8-31.87	23.84-32.47	23.93-51.73	23.93-36.15	23.92-32.2	23.95-35.65	23.92-Inf	23.75-Inf
		5	28.42-Inf	28.56-39.77	28.12-36.86	28.18-36.29	28.23-36.9	28.31-56.16	28.31-40.57	28.3-36.63	28.34-40.08	28.31-Inf	28.14-Inf
		10	34.42-Inf	34.56-45.78	34.12-42.87	34.18-42.31	34.23-42.91	34.31-62.17	34.31-46.59	34.3-42.64	34.34-46.09	34.31-Inf	34.14-Inf
MEO2 (~5000km)	81910	1	21.24-Inf	21.51-30.39	21.25-27.21	21.27-27.24	21.24-28.92	21.62-Inf	21.28-Inf	21.32-27.68	21.21-27.64	21.24-Inf	21.15-Inf
		3	30.62-Inf	30.89-39.87	30.63-36.69	30.65-36.72	30.62-38.4	31-Inf	30.66-Inf	30.71-37.16	30.59-37.12	30.62-Inf	30.54-Inf
		5	>35	>35	>35	34.98-41.15	34.05-42.83	34.42-Inf	34.79-Inf	34.14-41.59	34.81-41.55	>35	34.96-Inf
		10	>40	>40	>40	>40	>40	>40	>40	>40	>40	>40	>40
GEO (~35863km) (RAAN=50.059°)	358700	1	>35	>35	>35	>35	>35	>35	>35	>35	>35	>35	>35
		3	>45	>45	>45	>45	>45	>45	>45	>45	>45	>45	>45
		5	>50	>50	>50	>50	>50	>50	>50	>50	>50	>50	>50
		10	>55	>55	>55	>55	>55	>55	>55	>55	>55	>55	>55

Apart from geometric attenuation and atmospheric attenuation, single photon detection efficiency (3 dB), pointing efficiency (2 dB) and coupling efficiency (3 dB) are included in the total link budget. Moreover, consider the situantion where the transmission is completely obstructed by cloud cover so that the vaule of budget could be set as 'Inf'.

The scenario in which low-Earth orbit (LEO) satellites are deployed is more suitable for performing scheduling. Despite the promising results of the proposed scheduling under the current experimental settings of Micius satellite, we also seek to explore the possibility of using a satellite with different orbits to perform the proposed schedule in a future network. However, it has been reported that space-based QKD by medium-Earth orbit (MEO) or GEO satellites is difficult to achieve, at least under the current parameter settings in ref. 12. To show the benefits of scheduling under S-TD more intuitively, we adopt the suggested parameters, in which the divergence angle of the satellite-based transmitting telescope is assumed to be a set of fixed values of 1, 3, 5 and 10 μrad and the diameter of the ground-based receiving telescope is assumed to be 2 m. For comparison, the other parameters remain unchanged. We include the following orbit types for Micius in the simulation: (1) the initial orbit of Micius, i.e., an altitude of approximately 500 km, denoted as LEO; (2) orbit altitudes of approximately 2,500 km and 5,000 km, denoted as MEO1 and MEO2, respectively; and (3) orbit altitudes of approximately 35,863 km, denoted as GEO, where the Right Ascension of Ascending Node (RAAN) of the GEO satellite is chosen as 50.0591 degrees for full coverage of all the cities. Similarly, for all orbit types, the other orbital parameters are consistent with those of Micius. Here, the length of the duration available and the variations in the link budget in the implementations of space-based QKD are first investigated, where the results for the week are exhibited in Table 1. We can see that for a GEO satellite, the minutes of satellite availability during local night time is increased to approximately 358,700 s (99 h 25 mins), which is longer than that at LEO (204 mins), MEO1 (12 h 36 mins), and MEO2 (22 h 45 mins). However, for all the divergence angles we consider, the link budgets from the GEO satellite to all these cities exceeded the maximal tolerable budget (approximately 35 dB in a recent experiment[12]) that can generate a secure key. This implies that scheduling appears to be difficult when the transmissions from the GEO satellite to these cities face severe geometric losses, since there are few feasible alternatives even within a long duration. Fortunately, as the orbit altitude decreases, the link budget from MEO2 to the cities at a loss of less than 35 dB is possible for a divergence angle lower than 5 μrad.

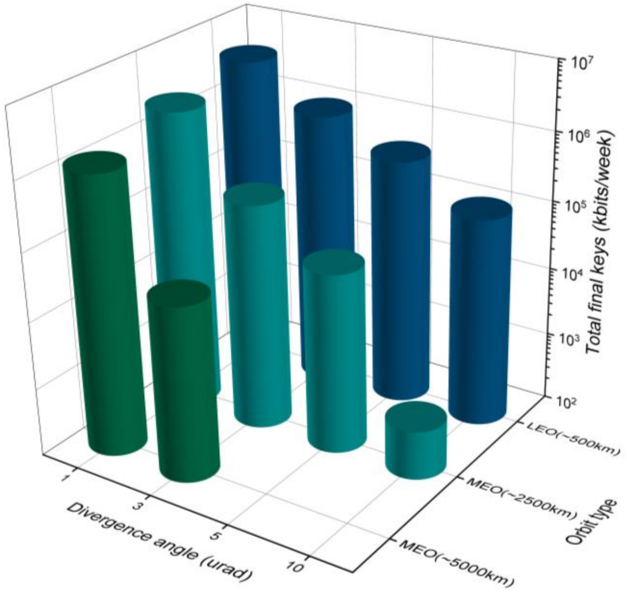


Fig. 4 Comparison of the total number of final keys delivered under different satellite altitudes and divergence angles. The final keys for Micius satellite with an orbit altitude of 500 km (blue), 2,500 km (cyan) and 5,000 km (green) and different values of the divergence angle, 1, 3, 5 and 10 μrad, are shown. For comparison, the resulting keys are obtained under the S-TD strategy, where the KL divergences of the delivery distributions are lower than 0.01.

We now predict the total final keys delivered separately under the same S-TD scheduling strategy. By setting the threshold of KL divergence to the same value of 0.01, we can further compare the

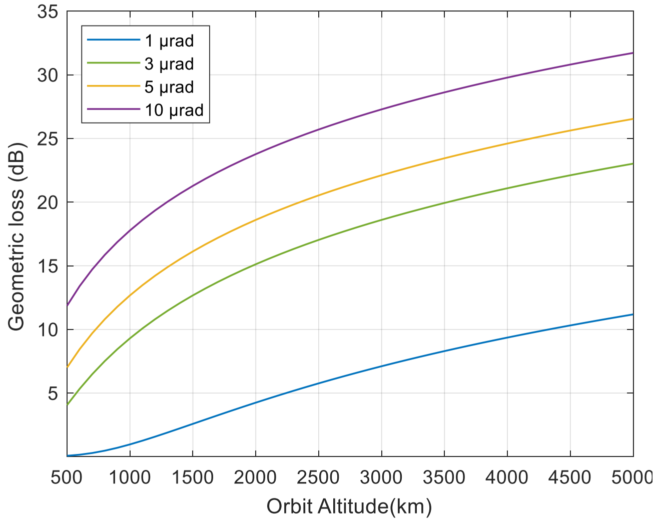


Fig. 5 Geometric loss vs. satellite altitude. Trend of the geometric loss as a function of the satellite altitude for several values of the divergence angle.

results for the satellite at different orbits and divergence angles. Considering that no secure key could be generated in the case where the channel from the satellite at GEO to the ground suffers serious attenuation, we show only the resulting keys for the satellites at LEO, MEO1 and MEO2 in Fig. 4. For the satellite with a divergence angle of 10 μrad, the final keys delivered from MEO1 are significantly fewer than those delivered from LEO1. This is because the delivery distribution must be lower than the threshold of KL divergence, even in the case where some cities have high budgets. For the satellite at MEO2, there is similar performance, which restricts the yields.

Another observation obtained from the results is that with the increase of the orbit altitude, the total number of delivered keys decreases. Indeed, choosing a satellite at a higher orbit altitude can effectively increase the duration but can also introduce a greater budget because of the increase in the received beam width. Specifically, for divergence angles of 3, 5, and 10 μrad, the link budget of the satellite at MEO2 is generally lower by more than one and two orders of magnitude than those of the satellite at MEO1 and at LEO, respectively. Therefore, the key generation rates calculated by the GLLP are also decreased by the corresponding orders of magnitude. The duration available for access to the satellite at MEO2 increased by only 4 and 8 compared to those at MEO1 and LEO. Therefore, in terms of the total number of keys delivered, the negative effect of the increased link loss is greater than the positive effect of the extended duration. Remarkably, by increasing the aperture of the transmitting telescope to decrease the diffraction-limited induced divergence angle to 1 μrad, a slight increase in the geometric loss (see Fig. 5) can mitigate the total link budget when the satellite orbit altitudes increase, whereas the current manufacturing technologies, along with the in-orbit load limits, make implementation of this strategy challenging in practice. Contrary to expectations of an improvement in the total number of keys delivered by an increase in orbit altitude to increase the available duration, these results verify that the plans for constructing a LEO satellite constellation[38] are more efficient than those for employing an expensive high-orbit satellite even with a payload allowing for larger optics.

DISCUSSION

In this paper, we explored the possibility of scheduling a satellite for QKD in an integrated space-to-ground network without fibre-based relays. Adapted from an existing paradigm, the hypothetical but possible network consists of Micius satellite and the 11 main cities of China. To design a sequence of missions that the satellite needs to execute, a comprehensive framework integrated with precise orbital modelling and a cloud model based on Himawari-8 data statistics was proposed to enable an accurate preassessment of satellite-based QKD applications. By formulating a problem that considers both the individual needs of cities and a target of maximizing the number of final keys delivered, we designed three different optimization methods to find the optimal solution for different scheduling strategies. With a set of defined weights for the cities based on an assumed traffic distribution, along with a scheduling strategy, i.e., S-PD, to prioritize delivery to cities with higher weight, more keys are significantly promoted for delivery with a high priority. Additionally, with a general scheduling strategy (S-GD) to maximize the total number of final keys, it is possible to obtain 7,468 kbits delivered to the city of Urumqi in a week, which represents the same final key rate as that of the fibre-based QKD relayed by at least 5 ideal nodes to a separation of 2,115 km from Xi'an.

However, satellite-based QKD operating under these two scheduling strategies can in certain cases outperform fibre-based QKD with relays, with the drawbacks that a difference between the delivered distribution and the expected distribution emerges and that the mismatch limits the XOR hash operations and thus reduces the utilization of the delivered final keys. To address this, we considered the S-TD strategy and introduced KL divergence to the algorithm to make the delivery distribution coincident with the expectation. As a result, we found that the benefits of the S-TD strategy are apparent in terms of ensuring individual needs and even promoting the utilization of the delivered keys in practical use. Finally, we explored the possibility of using satellites with different orbits to perform the proposed schedule. Contrary to expectations of an improvement in the total number of keys delivered by an increase in orbit altitude to increase the available duration, the results demonstrated that mitigating the geometric loss is the first consideration in future selection of the satellite orbit. In summary, constructing a LEO quantum satellite constellation to exploit the potential of applications is the best strategy that can be expected.

There is no denying that a satellite operating as the 'trusted node' to distribute keys will be replaced as an 'untrusted node' in the near future, especially with the decreasing loss budget of uplink [22] and the improving fidelity of entanglement sources. Nonetheless, once the schedules are employed, the current configuration could show higher flexibility than the entanglement-based QKD scheme because the latter requires that the two downlinks are feasible at the same time. Moreover, a network traffic graph is also needed to distribute the pairwise keys when employing entanglement-based

QKD. Notably, these two schemes, in fact, are not in conflict and should be integrated together for different encryption tasks. This allows us to make full use of the limited time to distribute more keys. Given the increasingly complex situation, satellite applications such as schedule design are urgently needed. Conveniently, our proposed framework may be used to explore this issue in future work. In summary, our work not only provides a practical solution to achieve network encryption without the need for fibre-based relays but can also be used as a pathfinder to support decisions involved in the selection of future quantum communication.

METHODS

In this section, we first introduce the framework given in the main text; then, we discuss how to formulate the satellite-based QKD scheduling problem. More specifically, scenario modelling and link budget modelling are key components in the framework, which lays the groundwork for scheduling optimization by providing the key rate estimation.

Space-based QKD modelling framework

We now discuss the components in the space-based QKD modelling framework, including scenario modelling, link budget modelling and the estimation of the transferred final keys. Figure 6 illustrates the individual components and how the components interact. The details of each component are given below.

Scenario modelling. The time-varying scenario constraints due to satellite movement can be predicted with orbital dynamics. Specifically, by using the involved ephemeris data of the simulation time ranging from a start date to an end date, the orbital elements of the satellite are periodically updated in modelling, thus covering orbital drift cases. With the latitude-longitude-altitude (LLA) of the specific cities, we directly obtain the report of a specific scenario

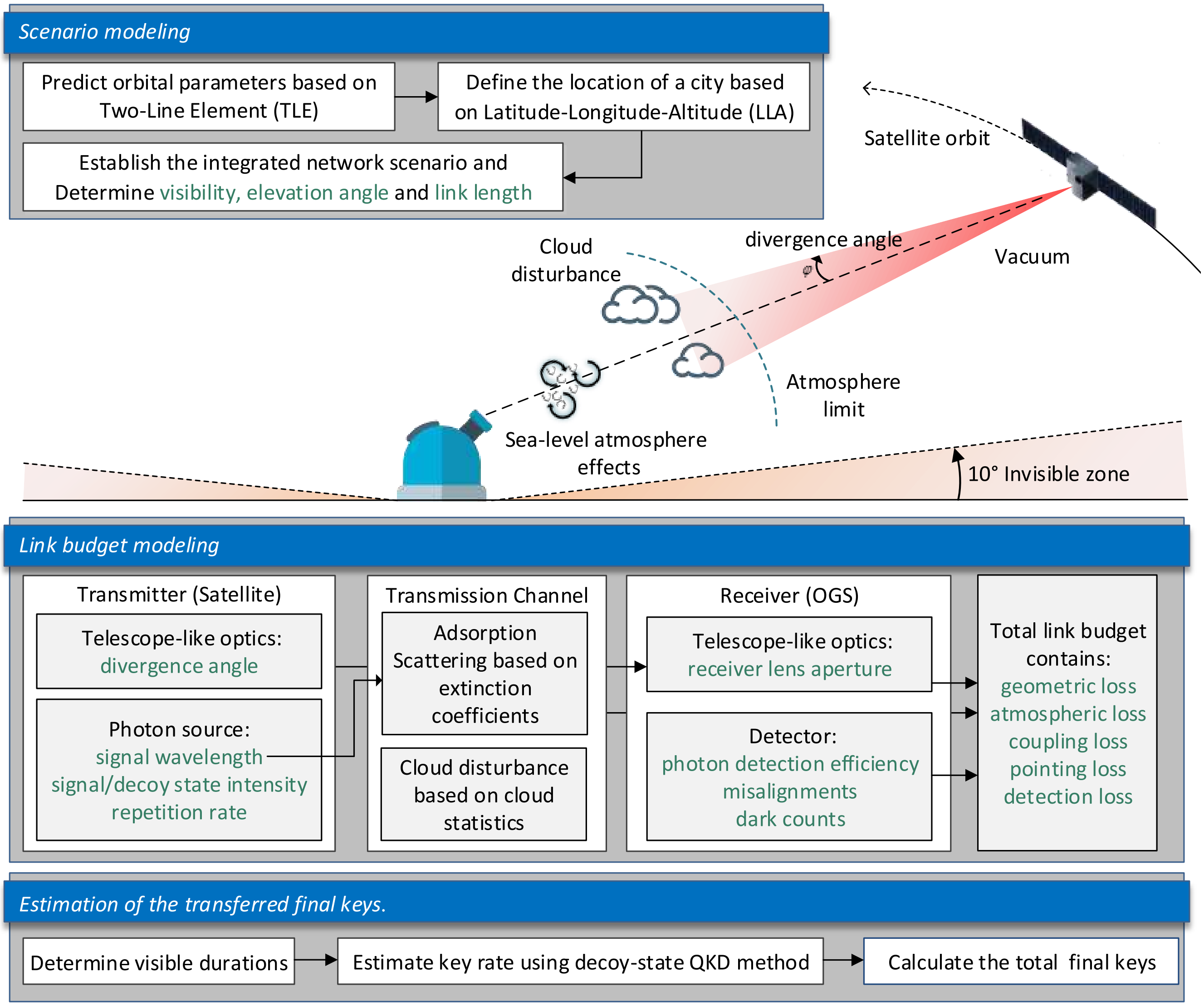

Scenario modeling
Predict orbital parameters based on Two-Line Element (TLE)
Define the location of a city based on Latitude-Longitude-Altitude (LLA)
Establish the integrated network scenario and Determine visibility, elevation angle and link length
Satellite orbit
divergence angle
φ
Vacuum
Cloud disturbance
Atmosphere limit
Sea-level atmosphere effects
10° Invisible zone
Link budget modeling
Transmitter (Satellite)
Telescope-like optics: divergence angle
Photon source: signal wavelength signal/decoy state intensity repetition rate
Transmission Channel
Adsorption Scattering based on extinction coefficients
Cloud disturbance based on cloud statistics
Receiver (OGS)
Telescope-like optics: receiver lens aperture
Detector: photon detection efficiency misalignments dark counts
Total link budget contains: geometric loss atmospheric loss coupling loss pointing loss detection loss
Estimation of the transferred final keys.
Determine visible durations
Estimate key rate using decoy-state QKD method
Calculate the total final keys

Fig. 6. The framework for modelling space-based QKD. First, based on the data file format referred to as TLE sets, an exact orbital element of a specific satellite together with practical geographic locations of a given city can be used as inputs to determine the visibility, elevation angle and relative distance. Then, the link budget is estimated by combining the QKD experimental transceiver parameters and cloud cover statistics involving three procedures relevant for optical signal attenuation: sending, transmission, and receiving in the satellite-based QKD system. Using a general decoy-state QKD method to estimate the key generation rate per second, the total final keys in a determined interval can be calculated as their sum.

concerning visibility, relative elevation angle and distance from a satellite to the destination. Subsequently, the available intervals can be defined as the times at which the satellite is in the darkness of night time and the elevation angle between the satellite and a city is greater than or equal to 10 degrees. Last, the elevation angle together with the relative distance from the satellite to a given city will be passed to be used as an input for the subsequent link budget modelling.

***Loss budget modelling*.** For the satellite-based QKD experimental configuration shown in Fig. 6, the optical power launched from the transmitter is affected by various factors until it is finally detected at the receiver. The prediction of the geometric loss owing to the beam takes the divergence angle, the link distance, and the receiver lens aperture size as inputs, and it scales as the inverse square of the propagation distance, with the final beam width typically being several times larger than the diameter of the receiving telescope. Consequently, the geometric loss Λ_G can be expressed as

$$\Lambda_G = 1 - \exp\left(-\frac{{D_r}^2}{2{\omega_r}^2}\right)$$
$$\omega_r = \sqrt{\left(\frac{\lambda}{\pi\varphi}\right)^2 + (\varphi L)^2} \tag{2}$$

where ω_r is the final beam width, D_r is the receiver lens aperture, φ is the divergence angle, λ is the wavelength and L denotes the link length. On the other hand, because the optical beam propagates through the atmosphere in downlinks, beam spreading leads to a less significant pointing loss Λ_p compared to the uplink. However, aerosols that absorb or scatter light are present throughout the atmosphere, particularly in clouds. As a consequence, days with heavy cloud cover are often excluded from the design of QKD missions. We focused our analysis on cloud disturbance in the presence of cloud thickness. To evaluate the contribution of this factor, the historical cloud statistics were obtained from Himawari-8, where the cloud cover for each city was encoded as an integer value ranging from 0 to 150. Note that the cloud cover used can be updated every ten minutes, and thus, the atmospheric transmittance model can be modified by $\Lambda_A = \Lambda_{A,0} \csc\beta \frac{150-\alpha}{150}, 0 \le \alpha \le 150$, where β is the elevation and $\Lambda_{A,0}$ is the sea-level extinction coefficient, which are typically 0.5 and 0.22 for 808 nm and 1550 nm, respectively[39]. The system loss resulting from coupling operation inefficiencies Λ_c and nonideal detection efficiency Λ_d depends greatly on the design specifications and is specified by the manufacturers. For convenience of analysis, we replicate the specific experimental values (see Table 2) reported in [12]. To summarize, we calculate the link budget within the available intervals separately for each step and export these values for key rate estimation.

***Estimation of the transferred final keys*.** Here, we present a general procedure for estimating the final keys transferred over an available interval. The polarization-encoded decoy-state BB84 protocol for the implementation of space-based QKD is used. The standard channel model[40] using a known transmittance is employed to estimate the gain Q_μ and quantum bit error rate (QBER) E_μ for all the photon number components. Using the GLLP security analysis, the key generation rate in the asymptotic case is given by[41]

$$R_{\mathrm{GLLP}} = q\left\{-f_e(E_\mu)Q_\mu h_2(E_\mu) + Q_1\left[1-h_2(e_1)\right]\right\} \tag{3}$$

where q depends on the implementation (1/2 for the BB84 protocol because half of the time, Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol, $q \approx 1$), f_e is the error correction inefficiency function, μ is the intensity of the signal state and h_2 is the binary entropy function. Q_1 and e_1 are the gain and error rate of the single photon states estimated using decoy-state theory, respectively. Therefore, the total final keys over the interval from a start time a to an end time b can be calculated as the sum of the rates per second,

$$K_{a,b} = \sum_{i=a}^{b} R_{GLLP}[\eta(t_i)] \tag{4}$$

where $\eta(t_i)$ is the link budget at time t_i.

Table 2. Parameters summary.

Parameter	Symbol	Reference value
Divergence angle	φ	10 μrad
Signal wavelength	λ	1550 nm
Fixed signal state intensity	μ	0.5
Fixed decoy state intensity	v	0.08
Repetition rate of the source	M_s	200 MHz
Sea-level extinction coefficient	β	0.22
Fixed pointing efficiency	Λ_p	2 dB
Fixed coupling efficency	Λ_c	3 dB
Detection efficiency	Λ_d	3 dB
Receiver lens aperture	D_r	1.2 m
Error probability of dark counts	e_d	0.5
Error probability of optical misalignment	e_0	0.015
Error-correction efficiency	f_e	1.16
Fixed background rate	Y_0	3x10^{-6}

Summary of the main simulation parameters used in our model, together with their reference values. Note that the background rate have been chosen as a fixed value while may up to 10^4 counts per second at a low elevation. Therefore, further study will be needed to obtain more practical performances for the channels.

Scheduling optimization

Problem formulation. The scheduling problem formulation allocates the time for delivering final keys to a given ground station. Before formally introducing the problem, we repeat some fundamental definitions that will be used. For simplicity, let the simulation period T be divided into intervals as in Fig. 2a, where the intervals have the same length of 10 s. Here, we denote the number of intervals as M. Without loss of generality, M could be a variable value based on the length of the simulation period. Thus, K_m^n represents the number of final keys that could be sent to cities $n \in [1, ..., N]$ during an arbitrary interval $m \in [1, ..., M]$. Note that all physical constraints are handled in the definition of K_m^n. For instance, in the interval m when the OGS located in each city n is in the darkness of night time or the elevation angle between the satellite and the OGS is smaller than 10 degrees, K_m^n will return 0. Moreover, considering the time spent switching between consecutive deliveries from one city to another, we add an interval to represent the switch before the next access, which can be expressed as:

$$\begin{cases} \sum_{n\in N}\sum_{m\in M} x_m^n \le 1 \\ x_{m+1}^n \le x_m^n + x_m^0 \end{cases}, \forall n \in [1, ..., N], \forall m \in [1, ..., M] \tag{5}$$

where the binary variable x_m^n describes whether interval m is assigned to city n. In constraint (5), the first inequality implies that at every time in the simulation period, at most one city can be assigned. The second inequality ensures that the required switching period x_m^0 before a handoff to other cities is considered. That is, if interval $m+1$ is assigned to a city, then either the preceding interval m should be scheduled for the same transmission or the requested switch x_m^0 should be performed at interval m.

With the above constraints, we formally define the optimization problem. Our goal in optimization is to find the optimal schedule that maximizes the total number of final keys under the different strategies involving (1) S-GD; (2) S-PD; and (3) S-TD. For this purpose, the general problem for these strategies can be formulated as:

$$\begin{aligned} &\text{Max} && \sum_{n=1}^{N} E_n^T \\ &\text{Subject to} && E_n^T = \sum_{m=1}^{M} K_m^n x_m^n \\ &&& \sum_{n=1}^{N}\sum_{m=1}^{M} x_m^n \le 1 \\ &&& x_{m+1}^n \le x_m^n + x_m^0 \qquad \forall n \in [1,...,N], \forall m \in [1,...,M] \end{aligned} \tag{6}$$

where E_n^T is the number of final keys delivered to city n over the simulation period T, which is the product of the number of final keys and the resulting binary variable x_m^n.

Algorithm statement. To obtain optimal solutions in the different strategies, we performed optimization based on the logical rule of the GA. In general, exploration of the search space is assured by the crossover- and mutation-driven recombination of solutions, whereas the fitness-based selection ensures the property of convergence. In this case, we start with a population of randomly generated individuals. For S-GD, we consider the cost function to be only sum of the final keys, which is calculated as $\text{Fitness}(I)=\sum_{n=1}^{N} E_n^T$. Thus, we solve the problem by finding the maxima (i.e., the maximum fitness levels). For S-PD, the cost function is modified to $\text{Fitness}(I)=\sum_{n=1}^{N} E_n^T w_n$, where w_n is the weight assigned to city n. Similarly, this allows the iterative process to tend towards higher-priority cities when searching for higher fitness. For S-TD, in addition to finding higher-fitness individuals by the same cost function used in S-GD, we compare the KL divergence of these individuals after every fitness-based selection, which is calculated by Formula (1), in which the relatively lower-value solutions are more likely to be chosen as a subset of the new population. Hence, with different modifications of the GA, solving the problems of maximizing the total number of final keys under different strategies can be achieved. Code snippets of the above methods are illustrated in Algorithms 1–3.

DATA AVAILABILITY

TLE database of Micius acknowledges support from the Celestrak (http://celestrak.com/satcat/search.php).

CODE AVAILABILITY

The code that contributed to the results of this study is available on request from the corresponding authors.

Box 1 Three algorithms used in optimization

```
Initialize: $t=1$, cross ratio $R_{cross}$, mutate ratio $R_{mutate}$,
population number $P_{num}$, stopping criterion $t_{\max}$, parent population
$X$.
Repeat
   1. Select, Crossover and Mutate to generate the new population
 $X_{new}$;
   2. for each individual $I$ do
Algorithm 1 for S-GD
     Calculate the cost function  $Fitness(I)=\sum_{n=1}^{N} E_n^T$
       end for
   3. Sort $X_{new}$ by their fitness values and choose the top $j$
individuals;
Algorithm 2 for S-PD
     Calculate the cost function  $Fitness(I)=\sum_{n=1}^{N} E_n^T w_n$
       end for
   3. Sort $X_{new}$ by their fitness values and choose the top $j$
individuals;
Algorithm 3 for S-TD
     Calculate the cost function  $Fitness(I)=\sum_{n=1}^{N} E_n^T$
     Compute the KL divergence $D_{KL}(I)=\sum_{n=1}^{N} p(x_n)\log\left[\frac{p(x_n)}{q(x_n)}\right]$
       end for
   3. Sort $X_{new}$ by their fitness values and choose the top $j\times 2$
   individuals; Sort the $j\times 2$ individuals by their KL divergences and
   choose the last $j$ individuals;
   4. Sort $X$ by their fitness values and choose the last $j$
individuals;
   5. Update the parent population $X$ by replacing the $j$
individuals with those in the new population $X_{new}$
  $t=t+1$
Until $t=t_{\max}$
```

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
2. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557-559 (1992).
3. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48**, 351-406 (2001).
4. Buttler, W. T. et al. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* **81**, 3283 (1998).
5. Peng, C. Z. et al. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.* **94**, 150501 (2005).
6. Yin, J. et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* **488**, 185 (2012).
7. Schmitt-Manderbach T. et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
8. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 –47 (2017).
9. Ren, J. G. et al. Ground-to-satellite quantum teleportation. *Nature* **549**, 70–73 (2017).
10. Yin, J. et al. Space-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
11. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometers. *Nature* **582**, 501-505 (2020).

12. Chen, YA. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
13. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 16025 (2016).
14. Cao, Y. et al. Long-distance free-space measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **125**, 260503 (2020).
15. Wang, J., Chen, H. & Zhu, Z. Modeling research of satellite-to-ground quantum key distribution constellations. *Acta Astronaut*. **173**, 164–171 (2020).
16. Khatri, S., Brady, J. A., Desporte, A. R., Bart, P. M., Dowling, P. J. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Inf.* **7**, 4 (2021).
17. Liao, S. K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
18. Dequal, D. et al Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Inf.* **7**, 3 (2021).
19. Wang, W., Xu F. & Lo, H.-K. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Phys. Rev. X* **9**, 041012 (2019).
20. Khaligh, M.-A. & Uysal, M. Survey on free space optical communication: a communication theory perspective, *IEEE Commun. Surv. Tut.*, **16**, 2231-2258 (2014).
21. Wang, X.-Y., Dong C., Zhao S.-H., Liu Y., Liu X.-W. & Zhu H.-N. Feasibility of space-based measurement-device-independent quantum key distribution. *New J. Phys.* **23**, 045001 (2021).
22. Vallone, G. et al. Satellite quantum communication towards GEO distances. *Proc. SPIE* **9900**, 99000J (2016).
23. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nature Photonics, **11**, 509-513 (2017).
24. Bedington, R, Arrazola, J. M. & Ling A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).
25. Sheng-Kai Liao, et al. Satellite-relayed intercontinental quantum network, *Phys. Rev. Lett*., **120**, 030501, 2018.
26. Peev, M. et al. The SECOQC quantum key distribution network in Vienna, *New J. Phys*. **11**, 075001 (2009).
27. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment, *New J. Phys*. **13**, 123001 (2011).
28. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
29. Polnik, M., Mazzarella, L., Di Carlo, M., KL Oi D. Annalisa R. & Ashwin A. Scheduling of space to ground quantum key distribution. *EPJ Quantum Technol.* **7**, 3 (2020).
30. JAXA Himawari Monitor: Service Homepage. Last accessed 15/3/2021. https://www.eorc.jaxa.jp/ptree/.
31. Holland, H.-J. et al. *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence* (MIT press, 1992).
32. Barz, B., Rodner, E., Garcia Y.-G. & Denzler, J. Detecting Regions of Maximal Divergence for Spatio-Temporal Anomaly Detection. *IEEE T. Pattern. Anal.*, **41**, 1088-1101 (2019).
33. Pirandola, S. Satellite Quantum Communications: Fundamental Bounds and Practical Security. *Phys. Rev. Research* **3**, 023130 (2021).
34. Bonato, C. et al. Feasibility of satellite quantum key distribution. *New J. Phys.* **11**, 045017 (2009).
35. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325 (2004).
36. Pirandola, S. Limits and security of free-space quantum communications. *Phys. Rev. Research* **3**, 013279 (2021).
37. Salakhutdinov, R. & Hinton, G. An efficient learning procedure for deep boltzmann machines. *Neural Computation* **24**, 1967-2006 (2012).
38. Vergoossen, T., Loarte, S., Bedington, R., Kuiper, H. & Ling, A. Modelling of satellite constellations for trusted node QKD networks. *Acta Astronautica,* **173,** 1 (2020).
39. Kerstel, E., Gardelein, A., Barthelemy, M., Fink, M., Joshi, S.-K. & Ursin, R. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration, *EPJ Quantum Technol.* **5**, 6 (2018).
40. Lo, H.-K., Ma, X. & Chen, K. Decoy-state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
41. Ma, X., Qi, K., & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. Lett.* **72**, 012326 (2005).

ACKNOWLEDGEMENTS

This work has been supported by the National Natural Science Foundation of China (Grants No. 61971436); the National University of Defense Technology (19-QNCXJ-009); the Innovative Talents Promotion Plan in Shaanxi Province (Grant No.2020KJXX-011) Key Research and Development Program of Shaanxi (Program No. 2019ZDLGY09-01. We gratefully thank Stefano Pirandola, Xuan Han for helpful discussions.

AUTHOR CONTRIBUTIONS

Xingyu Wang performed the bulk of this work at National University of Defense Technology during an exchange stay. Major of Satellite-based QKD modeling framework was worked by Xingyu Wang in this study. Chen Dong designed the optimization methods. Boyu Deng modified the manuscript. With thanks to Lei Shi, Haonan Zhu and Tianyi Wu from a research group who mooted the concept of the space-based QKD network with us. Shanghong Zhao supervised Wang at School of Information and Navigation.

COMPETING INTERESTS

The authors declare that there are no conflicts of interest related to this paper.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to Z. S. H or D. C.