Adaptive Quantum Key Distribution for Ultra-Long-Distance Secure Services Based on Satellite Networks

Xinyi He
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
hexinyi@bupt.edu.cn

Lin Li
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
lilinstu@163.com

Yongli Zhao*
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
yonglizhao@bupt.edu.cn

Yuan Cao
Institute of Quantum Information and Technology
Nanjing University of Posts and Telecommunications
Nanjing, China
yuancao@njupt.edu.cn

Xiaosong Yu
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
xiaosongyu@bupt.edu.cn

Jie Zhang
State Key Laboratory of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
lgr24@bupt.edu.cn

***Abstract*—Targeting the secret-key provision mismatch with the security requirements of ultra-long-distance services, this paper designs an adaptive quantum key distribution scheme based on satellite networks, improving more than 23% of service success probability compared to the benchmark.**

***Keywords*—quantum key distribution, satellite networks, ultra-long-distance, success probability**

I. Introduction

With the development of global economic integration, ultra-long-distance (ULD) services are urgently demanding high security. Affected by quantum computers, for ULD services that require secure encryption, more advanced data encryption technologies and more secure key distribution schemes are required to ensure service security. The AES algorithm can be used for data encryption, which is capable of resisting the attack of quantum computing by increasing the length of secret keys. Quantum key distribution (QKD) is a promising key distribution method, which has been proved to be unconditionally secure in theory. Integrating AES with QKD for high-bit-rate data encryption is verified to be an effective way to resist quantum attacks [1, 2]. However, the transmission distance for QKD is limited by transmission losses. It is difficult to provide secure keys for ultra-long-distance (typically a few thousand kilometers) services with security requirements through fiber-based QKD networks. Compared to fiber-based communications, the loss of light transmission in free space is smaller, the transmission distance is longer, and the coverage is wider, hence a large number of scholars have also studied free-space QKD [3]. With the success of the QKD experiment between the Micius and the ground station, the 7,600 km intercontinental QKD between China and Austria was completed by using the Micius as a trusted relay [4]. Meanwhile, with the success of the free-space QKD experiment in daytime [5], using multiple quantum satellites as trusted relays for networking [6], it is expected to achieve QKD over a ultra-long distance at any time period on the ground. However, due to the high-speed relative motion of Low Earth Orbit (LEO) satellite to earth, time windows for secret key negotiation are limited. Furthermore, the secret key rate on the Inter-Satellite Link (ISL) is low owing to the long distance between satellites. The total number of secret keys generated through quantum satellite-based relays is limited. Therefore, how to adaptively provide on-demand secret keys for ULD secure services has become an urgent problem. In this work, we formulate the quantum satellite network model, determine the calculation method of secret key resources on dynamic topology, and propose a service-oriented adaptive maximum flow path (SA-MFP) algorithm. Furthermore, we adopt the quantum satellite constellation based on 72 LEO satellites, and analyze the influence of different parameters on network performance by using the success probability of ULD secure service requests as a performance indicator. Simulation results show that the success probability of ULD secure service requests for the SA-MFP algorithm is 23% larger than that for the benchmark algorithm.

II. Problem Statement

A. Quantum Satellite Network Architecture

Different from fiber-based QKD networks, quantum satellite networks consider both the satellite constellation and the network architecture. Fig. 1 shows the quantum satellite network based on constellation design. Quantum nodes (e.g., LEO satellites and ground stations) are connected by laser links. Satellites are connected through the ISLs. Satellites and ground stations are connected through the Satellite-Ground Links (SGLs). Both the ISL and SGL consist of quantum channels and classical channels [7]. Under the existing technical conditions, it is better to choose the LEO as the quantum satellite [8]. The SGL uses a downlink channel to transmit quantum signals of 850 nm wavelength on the laser link and classical signals on the microwave link [9, 10]. Because of the higher efficiency of 1550 nm wavelength in daylight, both quantum channels and classical channels can also choose 1550 nm as they working wavelength [5].

In order to simplify the problem, the spatial part of the quantum satellite network adopts the Walker constellation with uniform distribution. Limited by the number of laser ports, each satellite is continuously connected to four adjacent

satellites, two of which are in the same orbital plane and the other two are in different orbital planes [11]. The ground station is connected to four satellites at most. The duration of connection varies with the position of the satellite. When a service is issued from the ground source node, the secret key pairs used for relaying between quantum nodes are consumed. Meanwhile, secret key pairs are constantly generated between neighboring quantum nodes with direct laser links. If the number of keys generated exceeds the number of keys consumed, the remaining keys are stored in a Quantum Key Pool (QKP) [12].

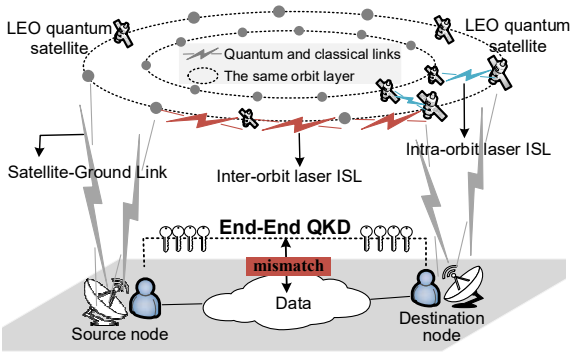

Fig. 1. An architecture of the quantum satellite network.

B. Secret Key Resource Model

In order to solve the mismatch problem between the number of consumed keys and the number of generated keys, we first model the secret key resources. Fig. 2 shows the QKD process for ULD secure services based on the quantum satellite networks, aiming to distribute the random key K from gs1 to gs2 through quantum satellites (qs1 and qs2). All nodes connected with direct laser links can continuously perform QKD, and the generated secret key (e.g., Ka) is stored in QKP (e.g., QKP_gs1&qs1).

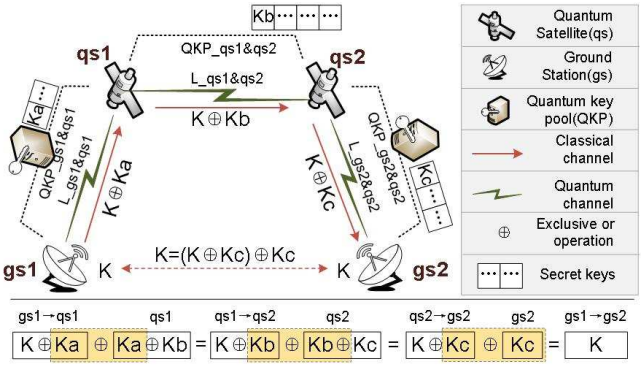

Fig. 2. The process of QKD.

Due to the high dynamic nature of satellites, it is difficult and unnecessary to update the topology in real time during the study of satellite networks. In most of the works, researchers preferred to use the snapshot to extract topology [13, 14]. Some of them used the topology snapshot at a fixed time interval, while others extracted the topology snapshot based on the satellite-ground link connectivity. This paper assumes that $\Delta t = t_1 - t_0$ to be the time interval of a topology snapshot. At t_1 moment, the calculation of the secret key resources in the QKP is as follows:

$$|P(t_1)| = |P(t_0)| + \Delta G(t) - \Delta K(t) \tag{1}$$

where $|P(t_1)|$ is the number of secret keys in the QKP at t_1, $|P(t_0)|$ is the number of secret keys in the QKP at the initial time, $\Delta G(t)$ is the number of secret keys generated within $[t_0, t_1]$, $\Delta K(t)$ is the number of secret keys consumed within $[t_0, t_1]$.

Secret key generation is the process of uninterrupted secret key negotiation and secret key generation between adjacent nodes with connection relations. The generated secret keys are eventually stored in the QKP of the transceiver node. In this case, the number of secret keys in the QKP is expressed as follows:

$$\Delta G(t) = \int_{t_0}^{t_1} r(t)\,\mathrm{d}t \tag{2}$$

$$r(t) = r_{ref} \times f(|E(t)|) \tag{3}$$

where $r(t)$ is the secret key rate when the link length is $|E(t)|$. r_{ref} is the secret key rate only related to the device in vacuum state. $f(|E(t)|)$ has different expressions in different environments, which are functions of distances.

When the transceiver devices are determined, the secret key rate of the decoy-state BB84 protocol is related to losses, and the key-generation rate decreases with the increase of losses [7]. Substituting the link loss into formulas in [15], the secret key rate of the ISL link can be calculated. For the SGL, the real-time secret key rate can be obtained by the data of the satellite-ground QKD experiment of Micius [16].

Secret key consumption is the process of key negotiation and key consumption between ground stations through trusted relays. As shown in Fig. 1, when the ULD secure services are triggered at the ground stations, the secret key between the source and destination nodes will be obtained through a series of encryption and decryption processes. During the topology period, the number of secret keys consumed is expressed as follows:

$$\Delta K(t) = \sum_{t_0}^{t_1} k_r \tag{4}$$

where k_r is the number of secret keys required for each service.

C. Objective Function

According to Fig. 2, there are two necessary conditions for accomplishing end-to-end QKD: ① the routing paths between source and destination nodes can be found; ② the number of secret keys in the QKP between relay node pairs on the path is no less than the secret key requirements of end-to-end services. Since LEO satellites are in constant motion, the SGL is not continuously connected. This also means that when dynamic services arrive randomly, there may exist no routing paths between the source and destination nodes. Based on the experience of fiber-based QKD networks, the construction of end-to-end QKP is a feasible method, which has been described in detail in other results. This paper will focus on the routing and key resource allocation problem, that is, when the number of satellites is sufficient, how to provide sufficient secret keys for ULD secure services?

In this paper, the services with security requirements are abstracted into static services and dynamic services. Static services are characterized by simultaneous arrival and departure times. The characteristics of dynamic services are that the arrival time and departure time of services obey certain rules (such as Poisson Distribution). Both static and dynamic service requests are represented by

$r(V_j, V_{j'}, t_{arr}, t_{lea}, k_r)$, where V_j and $V_{j'}$ represent two different ground stations, t_{arr} and t_{lea} indicate the arrival time and the departure time of the secure service request, respectively. When the security requirement arrives, the Eq. (1) is extended to

$$|P(t_{lea})| = |P(t_{arr})| + (t_{arr} - t_0) \times r_{arr} - k_r \quad (5)$$

where r_{arr} is the secret key rate at the arrival time. Based on Eq. (5), when services continue to arrive, the secret keys in the QKP are constantly consumed. Finally, the key resources in the relay node are insufficient to complete end-to-end QKD, resulting in the failure of the service request.

The success probability of ULD secure service requests may not remain at 100% as the number of services increases. The optimization of the algorithm is beneficial to avoid the use of relay nodes with insufficient secret keys and improve the success probability of secure service requests. More specifically, in the static scenario, a better algorithm means an increase in network capacity, which is a network planning problem. In the dynamic scenario, a better algorithm means lower blocking rate, which is a routing problem. This work targets at the network planning problem.

III. SA-MFP Algorithm

In a static scenario, all services with security requirements are known, such as V_j, $V_{j'}$, and k_r. To simplify the expression, we set the basic unit of the secret key as $128k$ bits, with k as a positive integer. When $|P(t_0)| = 10$, the number of secret keys in a QKP is $1280k$ bits. Meanwhile, the static service does not consider the duration, hence the secret key generation is no longer calculated, that is, $\Delta G(t) = 0$. Then, we design the SA-MFP algorithm. By finding the maximum flow path in the current network topology, services are adaptively matched with the maximum flow path, and the secret key resources of links are fully utilized to improve the success probability of ULD secure service requests. The detailed process of SA-MFP algorithm is divided into the following seven steps and exemplified in Fig. 3.

① When the ULD secure service request is triggered at t_0 and the network topology is shown in State1, the controller calculates the current network resources (e.g., the number of secret keys and connectivity status).

② Through the Maximum Flow(MF) algorithm, find the maximum flow path. Two paths of V_a-V_c are found: V_a-V_2-V_4-V_c (up to 5 units of secret keys are generated) and V_a-V_2-V_1-V_3-V_5-V_6-V_c (up to 4 units of secret keys are generated).

③ When the service request1 between V_a and V_c is 3 units of secret keys, path1 will be selected with fewer hops. The service request1 succeed and the resources will be updated as shown in State2.

④ Continue to find the maximum flow path, two paths of V_a-V_d are found: V_a-V_2-V_1-V_3-V_5-V_d (up to 3 units of secret keys are generated) and V_a-V_2-V_1-V_3-V_5-V_d (up to 2 units of secret keys are generated).

⑤ When the service request2 between V_a and V_d is 5 units of secret keys, the service request is split into 2+3 units of secret keys, route according to path3 and path4. The key resources will be updated as shown in State3.

⑥ Continue to find the maximum flow path, two paths of V_b-V_c are found: V_b-V_4-V_d (up to 4 units of secret keys are generated) and V_b-V_4-V_6-V_d (up to 2 units of secret keys are generated).

⑦ When the service request3 between V_b and V_c is 7 units of secret keys, the total number of secret key resources on path5 and path6 is 6 units. Therefore, insufficient secret keys are provided, the service request3 is failure.

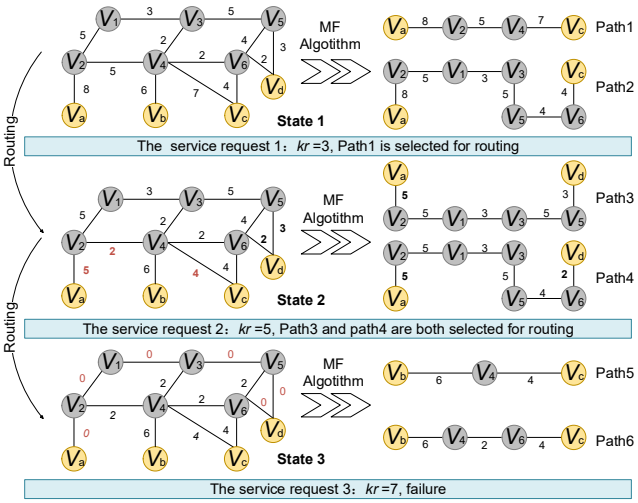

Fig. 3. The process of SA-MFP algorithm.

IV. Simulation Results

As shown in Fig. 4, to evaluate the performance of the SA-MFP algorithm, we construct a Walker constellation containing six orbital planes, each of which has 12 LEO satellites. In each orbit, all the satellites are evenly distributed. In the simulation, the source and destination nodes are randomly selected from Beijing, New York, Colorado, London, Melbourne, Moscow. It is assumed that any two quantum nodes execute QKD as long as there is a link between them. The LEO satellite has an orbit altitude of 500 km, an inclination of 87°, and an orbital period of 6027s. AGI STK software is employed to obtain satellite constellation information and calculate the satellite topology matrix. Considering the dynamic changes of satellite topology, we set the establishment or dismantling of SGL as a sign to update the topology. When we add the topology at time 0, we get a total of 88 topologies. The parameters are shown in Table I.

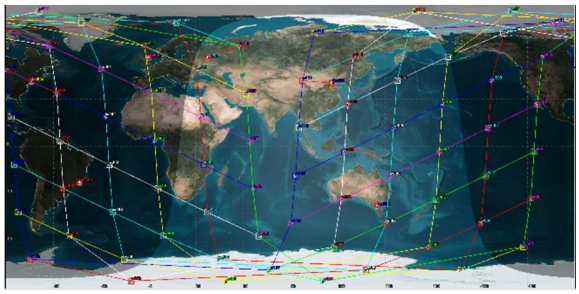

Fig. 4. Network topology with 72 satellite nodes and 6 ground stations.

In order to simplify the model, this paper defaults to traffic balance at each moment and defaults to a static scenario where the traffic is balanced at all times, that is, the volume of traffic within each sampling period is same. Then, in the static scenario, within 6027s of the entire satellite operation period,

the total number of services is 88 times of the number of services in each sampling period.

TABLE I. SIMULATION PARAMETERS

The quantum network parameters	**Values**
Constellation type	Walker
Number of satellites	72 (6 Orbits)
Orbit altitude	1000 km
Source/Destination node	Beijing, New York, Colorado, London, Melbourne, Moscow
Orbital period	6027 s
Number of discrete topologies	88
Simulation parameters	**Values**
The number of secret keys in QKP at the initial time ($\|P(t_0)\|$)	1000
The number of secret keys required by a single service (k_r)	4~6
The number of static services	100~2100
Topology update condition	The SGL changes

The relationship between the number of ULD secure service requests and success probability is shown in Fig. 5. With the increasing number of secure service requests, the success probability decreases. However, under the same network topology, the SA-MFP algorithm still guarantee the success probability of 100% when the number of secure service requests reaches 700. In other words, the quantum satellite network carries more ULD secure services by using SA-MFP algorithm. In addition, with the increasing number of secure service requests, the success probability of ULD secure service request declines more slowly by using the SA-MFP algorithm. When the number of secure service requests reaches 2100, the success probability improvement of using the SA-MFP algorithm versus the benchmark algorithm is up to 23%. The reason is that SA-MFP algorithm can adaptively match the services to the secret key resources, where the secret key resources are fully utilized.

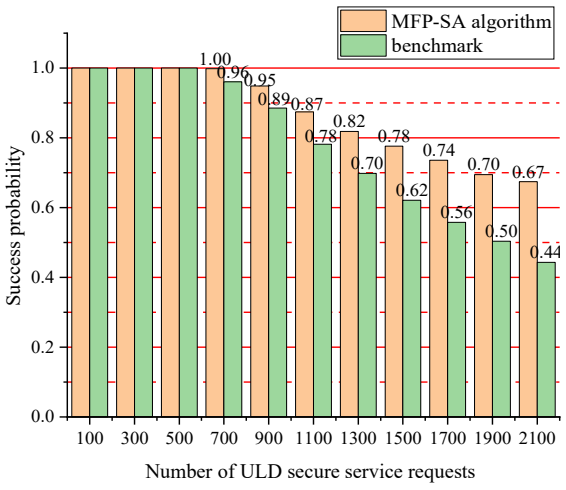

Fig. 5. Success probability of ULD secure service requests for different algorithms.

When the number of secret keys required by each service changes, the relationship between the success probability and the number of ULD secure service requests is shown in Fig. 6. The simulation sets the initial amount of QKPs as 1000. The ULD services are secure as long as their number is less than 700. The success probability of secure service requests will decrease with the increase in K_r. This is because the larger the K_r, the greater the demand for secret key resources.

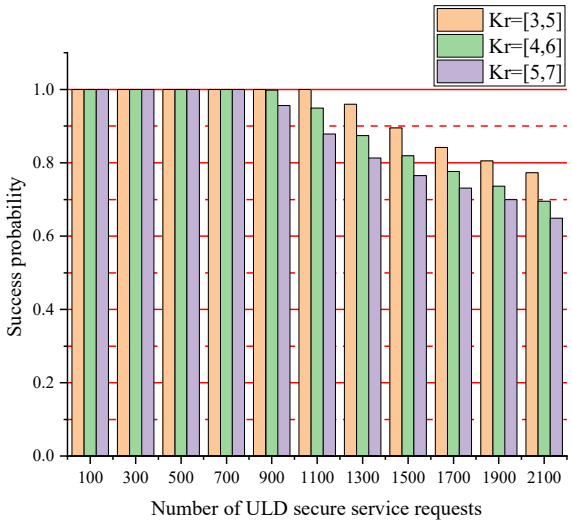

Fig. 6. The impact of different $|k_r|$ on success probability of ULD secure service requests.

V. CONCLUSION

This paper modelled the secret key resources based on quantum satellite networks, and presented an SA-MFP algorithm to efficiently match the demand of secret keys with the generated secret keys relying on QKD. Simulation results demonstrated that the proposed SA-MFP algorithm outperforms the benchmark algorithm in terms of service success probability.

ACKNOWLEDGMENT

This work is supported by National Key Research and Development Program of China (2020YFE0200600), NSFC project (62150032, 62201276，61971068，62101063).

REFERENCES

[1] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, “Quantum key distribution and 1 Gbit/s data encryption over a single fibre,” New J. Phys., 12, 063027, 2010.

[2] G. Sharma, S. Kalra, “A novel scheme for data security in cloud computing using quantum cryptography,” in Proceedings of Advances in Information Communication Technology and Computing (AICTC), Bikaner, India, August 2016.

[3] A. Kumar, D. Augusto de Jesus Pacheco, K. Kaushik, J. Rodrigues, “Futuristic view of the Internet of Quantum Drones: Review, challenges and research agenda,” Vehicular Communications, 36, 2022.

[4] S. K. Liao, W. Q. Cai, et al., “Satellite-relayed intercontinental quantum network,” Physical Review Letters, 120(3): 030501, 2018.

[5] S. K. Liao, H. L. Yong, et al., “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication,” Nature Photonics, 11(8): 509, 2017.

[6] V. Tom, L. Sergio, B. Robert, K. Hans, L. Alexander, “Modelling of satellite constellations for trusted node QKD networks,” Acta Astronautica, 173: 164-171, 2020.

[7] C. Bennett, G. Brassard, “An update on quantum cryptography,” in Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984.

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

[9] R. Radhakrishnan, E. William W., A. Fatemeh, R. Ramon Martinez, P. Frank, B. Scott C., “Survey of inter-satellite communication for small satellite systems: physical layer to network layer view,” IEEE Commun. Surv. Tutorials, 18(4), 2442–2473, 2017.

[10] H. Takenaka, “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite,” Nat. Photonics, 11(8), 502–508, 2017.

[11] D. Huang, Y . Zhao, T . Yang, S. Rahman, X. Yu, X. He, and J. Zhang, “Quantum key distribution over double-layer quantum satellite networks,” IEEE Access 8, 16087–16098 (2020).

[12] Y. Cao, Y. Zhao, Y. Wu, X. Yu, J. Zhang, “Time-scheduled quantum key distribution (QKD) over WDM networks,” J. Lightwave T echnol. 36(16), 3382–3395, 2018.

[13] H. Chang, B. Kim, C. Lee, S. Min, Y. Choi, H. Yang, D. Kim, C. Kim, “FSA-based link assignment and routing in low-earth orbit satellite networks,” IEEE Transactions on Vehicular Technology, 47(3), 1037-1048 (1998).

[14] J. Huang, Y. Su, L. Huang, W. Liu, F. Wang, “An optimized snapshot division strategy for satellite network in GNSS,” IEEE Communications Letters, 20(12), 2406-2409 (2016).

[15] H. Lo, X. Ma, K. Chen, “Decoy state quantum key distribution,” Physical Review Letters. 94, 2005.

[16] S. K. Liao, W. Q. Cai, W. Y. Liu, et al. “Satellite-to-ground quantum key distribution,” Nature, 549(7670): 43-47, 2017.