IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received December 27, 2019, accepted January 4, 2020, date of publication January 14, 2020, date of current version January 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2966683

Quantum Key Distribution Over Double-Layer Quantum Satellite Networks

DONGHAI HUANG[1], YONGLI ZHAO[1], (Senior Member, IEEE), TIANCHENG YANG[1], SABIDUR RAHMAN[2], XIAOSONG YU[1], XINYI HE[1], AND JIE ZHANG[1]

[1]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Department of Computer Science, University of California at Davis, Davis, CA 95616, USA

Corresponding author: Yongli Zhao (yonglizhao@bupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61601052 and Grant 61822105, in part by the Fundamental Research Funds for Central Universities under Grant 2019XD-A05, and in part by the State Key Laboratory of Information Photonics and Optical Communications of China under Grant IPOC2019ZR01.

ABSTRACT Quantum key distribution (QKD) has attracted much attention on secure communications across global networks. QKD over satellite networks can overcome the limitations of terrestrial optical networks, such as large attenuation over long distance fiber channel and difficulty of intercontinental domain communications. Different QKD networks (around the world) can intercommunicate through quantum satellites, leading to a global quantum network in near future. This raises a new resource allocation and management problem of QKD involving multiple satellite layers and distributed ground stations. Using existing schemes, a single satellite cannot perform QKD for ground stations for the whole day. Moreover, the research problem is more challenging due to limitations of satellite coverage: limited cover time of low earth orbit (LEO) satellite, high channel losses of geostationary earth orbit (GEO) satellite, etc. To overcome these limitations, our study proposes a double-layer quantum satellite network (QSN) implemented quantum key pool (QKP) to relay keys for ground stations. We propose a new architecture of trusted-repeater-based double-layer quantum satellite networks, comprising GEO and LEO satellites. We also address the routing and key allocation (RKA) problem for key-relay services over QSNs. We propose a novel joint GEO-LEO routing and key allocation (JGL-RKA) algorithm to solve the RKA problem. Simulative results show that the proposed scheme can increase success probability of key-relay services significantly. We also present the impact of different route selections mechanisms, number of satellite links, satellite node capability, and service granularity on network performance.

INDEX TERMS Double-layer satellite networks, quantum key distribution, quantum satellite networks, satellite routing, trusted repeaters.

I. INTRODUCTION

Secure communication for the applications across networks is gaining increasing attention from the research community. Traditional security techniques mostly focus on the encryption of communication, where security depends on the mathematical complexity. However, encryption methodologies are becoming less reliable as the eavesdroppers and attackers are gaining powerful computing ability [1]. Quantum cryptography [2] is a new cryptographic technology for generating random secret keys to be used in secure communication. Quantum cryptography can provide communication security based on the laws of quantum physics (e.g., the no-cloning theorem and uncertainty principle). However, the quantum key has to be distributed over the communication network to be used by the senders and receivers.

Reference [3] demonstrated the feasibility of Quantum Key Distribution (QKD) over optical networks. Such a QKD network can be constructed by distributing end to end secret (quantum) keys through trusted repeaters (e.g., based on the point-to-point BB84 protocol). References [4], [5] also reported such optical-fiber-based QKD networks, used to secure metropolitan and backbone networks. Recent studies discussed about integration of QKD and classical networks, such as QKD over WDM networks [6], [7] and QKD enabled software-defined networks (SDN) [8].

While implementing QKD in terrestrial optical networks, distributing secret keys over a long distance (e.g., across the

The associate editor coordinating the review of this manuscript and approving it for publication was Christian Esposito.

globe) is challenging. Single-photon signal transmitted over long-distance optical fiber suffers from high losses and depolarization. Hence, carrying the keys using optical fiber over long distances (e.g., 1000KM) is not an effective solution [9].

To address the limitation of optical fibers, a lot of colleges and aerospace institutes have studies and experimented free-space QKD in recent years. In contrast to optical fibers, the free-space photon will experience negligible loss in vacuum, making it feasible to distribute secret keys over thousands of kilometers. Although the optical beam of a satellite-to-ground link can suffer from atmospheric loss, most of the space is empty, which makes the channel loss less than a long fiber [9], [10]. The quantum satellite *Micius*, launched in 2016 for quantum communication experiments, has successfully demonstrated satellite-to-ground QKD using single-photon source [11]. In 2017, a ground free-space QKD experiment had been carried out using telecom wavelength in daylight and demonstrated the feasibility of inter-satellite QKD in daylight [12], [13]. Therefore, satellite-based QKD is a promising method for distributing quantum keys between two ultra-long-distance parties on the ground.

Since the coverage and flyover time of one satellite is limited, a group of quantum satellites can be used as trusted repeaters to serve the ground stations. Recently, researchers have proposed 'network of quantum satellites' to realize global-scale quantum communications [14], [15]. The authors of [16] proposed a QKD satellite networks architecture based on quantum repeaters. The researchers also proposed the trusted-repeater-based satellite QKD scheme [13]–[17]. Their proposed scheme is based on BB84 protocol since quantum repeaters are still far from implementation. Reference [18] investigated the possible schemes of free-space QKD using inter-satellite links and analyzed the properties of satellite-ground links. These studies motivated our study to contribute towards advancement of the *state-of-the-art* in Satellite based QKD networks.

Prior studies envision that a quantum-capable satellite constellation can be formed to construct global QKD (similar to traditional satellite constellations such as IRIDIUM [19]). In recent proposals, quantum satellites use low earth orbit (LEO) to benefit from its low channel loss. But a LEO satellite can access a particular ground station for a limited time of the day [20]. This limited coverage may lead to a shortage of secret keys between satellite and ground. In contrast, geostationary earth orbit (GEO) satellites can access ground stations continuously, all day. However their signal can suffer from high channel loss and limited key generation rate.

In 2017, German researchers have successfully measured quantum signals that were sent from a GEO to ground station [21]. Italian researchers have also demonstrated the feasibility of quantum communications between high-orbiting global navigation satellites and a ground station [22]. Chinese Academy of Sciences has future projects to launch higher altitudes satellite [11]–[13]. According to the researchers, the future quantum satellite constellation will be comprised of satellites in high and low orbits [23]. Thus, combining both GEO and LEO satellites to build QKD networks is a research direction worth exploring.

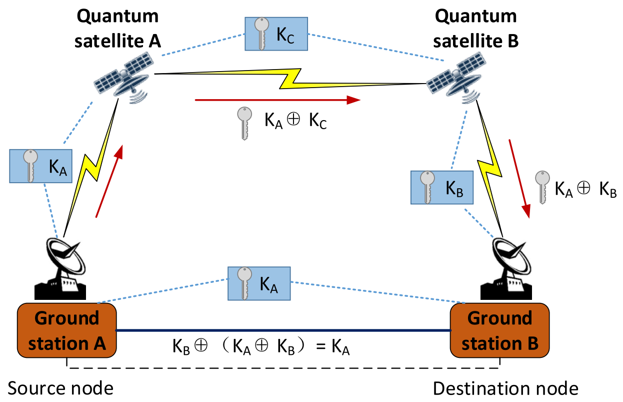


FIGURE 1. Principle of trusted-repeater-based satellite QKD.

To the best of our knowledge, our study is the first to explore this research direction utilizing both GEO and LEO quantum satellite resources to distribute secret keys. Our study proposes a novel solution to the routing and key allocation (RKA) problem for key-relay services, using double-layer (GEO and LEO) satellite networks, which maximizes the number of generated secret keys.

The major contributions of this study are: 1) we propose a new architecture of double-layer quantum satellite networks based on trusted-repeaters. We discuss the topology design and link-set-up strategy; 2) we propose a novel joint GEO-LEO routing and keys allocation (JGL-RKA) algorithm to solve the RKA problem over double-layer quantum satellite networks; 3) we evaluate the performance of our proposed algorithm by simulative results.

The rest of this paper is organized as follows. Section 2 presents the existing and future technologies of satellite-based QKD system. Section 3 proposes a double-layer quantum satellite networks architecture. Section 4 describes the network scenario and problem statement. Section 5 proposes the JGL-RKA algorithm. Section 6 presents the simulation results and analyzes the performance of our proposed scheme. Section 7 concludes the study.

II. SATELLITE-BASED QKD SYSTEM

This section introduces the current and future state of technologies of free-space QKD and quantum satellites, including satellite-to-ground and inter-satellite QKD.

A. FREE-SPACE QKD

Similar to ground QKD, current free-space QKD experiments mostly implement the mechanism of transmitting individual encoded polarized photons to generate secret keys between two communication parties (e.g., Alice and Bob), based on BB84 protocol. The procedure of satellite-to-ground QKD consists of i) quantum communication (quantum signal transmitted in 850nm) and ii) classical communication (classical optical signal transmitted in 1550nm). These two communications are usually located in different working wavelengths over the same laser link. In near future, the quantum satellites will be able to conduct quantum communication and classical communication using single integrated transponder [24]. Typically, the quantum signal is transmitted on downlinks and the classical signal is transmitted on uplinks [11]. The single polarized photons are transmitted in quantum channel. Classical channel can be used for transmitting the measurement-basis signals and key-relay services, as well as data services in the future.

For the inter-satellite quantum channel, the 1550nm wavelength is used due to its higher efficiency in daylight [12]. To be compatible with classical communications, multi-beam system is used in inter-satellite communications. With the on-board multi-beam transponders, quantum signal and data signal can be carried on different laser beams, in the same optical link.

B. TRUSTED-REPEATER-BASED SATELLITE QKD

Quantum satellites can be used as trusted repeaters in generating secret keys for terrestrial nodes. Similar to terrestrial QKD networks, quantum satellites are considered as trusted nodes and even more trusted than ground nodes because the cost of the eavesdropping over satellites is much higher than that of ground networks [17]. With a group of quantum satellites, real-time secret key distribution can be achieved between a pair of ground stations. Fig. 1 illustrates the basic procedure of trusted-repeater-based satellite QKD. The secret key K_A can be transmitted from ground station A to ground station B by successively encrypting and decrypting on intermediate nodes. The XOR operation will be conducted on each link.

Due to the long distance of satellite links, the secret key rate is limited and the round-trip delay is high. To overcome these challenges, quantum key pool (QKP) can be constructed between satellite to ground and between. Each pair of adjacent nodes generate and exchange secret keys continuously and store keys in quantum key pools. Fig. 2 shows the basic structure of QKP enabled satellite QKD system. Each node has its quantum transceiver, laser transceiver, and QKP. The control system calculates the route selection and key assignment and allocates them on each node. The controller can be connected to satellites by radio or optical links (the radio transceiver is omitted in the picture).

III. QUANTUM SATELLITE NETWORKS ARCHITECTURE

Based on the above analysis and technologies of satellite-based QKD, we propose a new architecture of global-scale quantum satellite networks.

A. DOUBLE-LAYER QUANTUM SATELLITE NETWORK ARCHITECTURE

The number of secret keys in quantum key pools depend on the key generation rates and the duration of key generation procedure. However, LEO satellites can only access to a ground station for about 10∼15 minutes in a satellite moving period due to their high-moving speed relative to the earth. Within the short coverage time, the secret keys in QKP between LEO and ground stations may be not enough for key-relay services. On the contrary, GEO satellites stay at rest relative to the earth and cover wider range due to the high orbit, thereby they can perform QKD continuously (at the expense of much larger losses). GEOs can generate and store the keys for all day with lower secret key rates. The technologies of higher link efficiency including larger telescope and better pointing system are being studied to increase the key rates on higher orbit [11].

To eradicate the limitations of single-layer satellite networks, we propose a new architecture of double-layer quantum satellite networks. As shown in Fig. 3, the network consists of at least two orbit layers of satellites. In this paper we consider that the satellite networks comprise of GEO and LEO. The hybrid of LEO and GEO satellite networks can combine the advantages of both satellite layers. In double-layer satellite networks, GEO and LEO can both establish access links to ground stations, while LEO is the priority choice to be access satellite and GEO is alternative. Satellites in the same orbit layer are interconnected by inter-satellite-links (ISL). Also, satellites in different orbit layers could

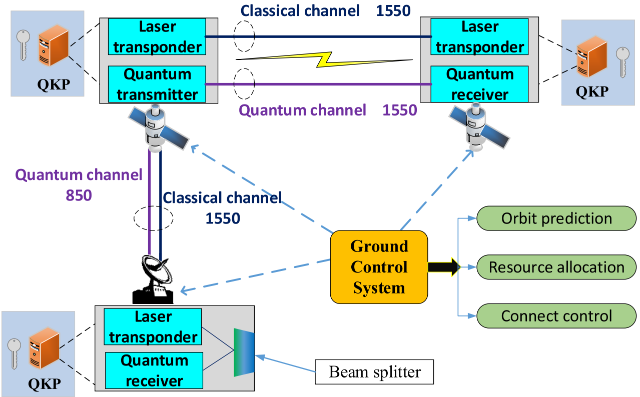


FIGURE 2. Basic structure of QKP enabled satellite QKD system.

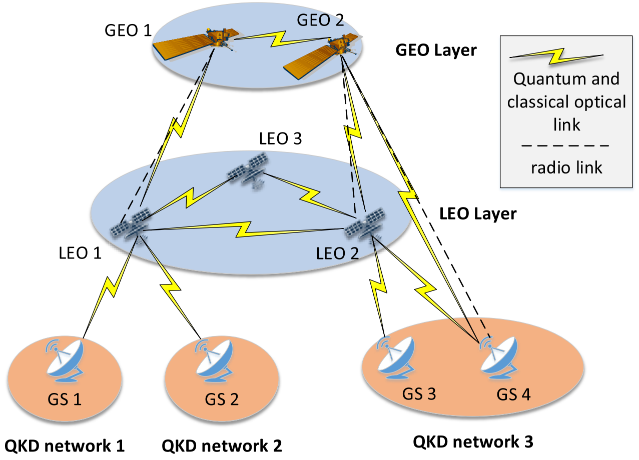


FIGURE 3. Architecture of double-layer quantum satellite networks.

be interconnected by inter-orbit-links (IOL). In the ground segment, QKD networks are distributed all over the world and interconnected by one or more satellites.

B. TOPOLOGY DESIGN AND LINK SETUP STRATEGY

In our proposed scheme, we set 66 LEO and 3 GEO satellites in our satellite constellation. Similar to the IRIDIUM system [25], the LEO layer consists of 6 orbits and satellites locate uniformly in each orbit. The Sun-Synchronous Orbit (SSO) is adopted because it can cover the same area in each satellite period. The GEO layer consists of 3 GEO satellites located uniformly in the equator orbit. Since GEO satellites could provide long QKD performing time and high coverage rate, it stores the generated keys in satellite-ground QKP.

With multiple pairs of transponders on board, a satellite can set up several simultaneous optical links with adjacent nodes and ground stations. However, considering the resource constraint of satellites, the establishment of inter-orbit-layer-links and access links should be scheduled efficiently. We will study the routing problem under the cases with and without GEO-LEO links in the following sections.

With limited transponders on satellite, time-shared scheme can be used in the QKD connection between GEO and ground, which means two or more ground stations can share a transponder on GEO. For example, if one transponder can access to 2 ground stations by turns, GEO with 4 transponder can set up 8 quantum satellite-ground links. In this paper we suppose one transponder can connect to 2 ground stations and each connection lasts for 30 minutes. As for key relaying, GEO can transmit XOR keys to ground stations and LEOs in radio links by broadcasts.

IV. PROBLEM STATEMENT

In the proposed double-layer quantum satellite networks, it is necessary to design a novel routing and key assignment (RKA) algorithm for key-relay services to schedule the end to end key distribution. The algorithm calculates the key-relay path for each key-relay service. Then it allocates bandwidth and quantum keys of each link along the service path.

We assume that key-relay services are originated from two nodes in different QKD networks or two distant nodes in the same QKD network. Each satellite can establish multiple free-space optical links with other satellites. Ground stations (GS) are capable of handling 4 ground-satellite links simultaneously. The optical links can be set up in millisecond (ms) time. The routing and resource allocation problem over quantum satellite networks is stated as follow:

- ***Given***:

1) Terrestrial network topology: the geolocation information of ground stations (GS) in global networks;
2) Node and link property: the capacity of quantum key pool (QKP) between each pair of nodes and secret key rates in different types of links;
3) Satellite network topology: LEO and GEO satellites and respective ISLs, connectivity between satellites and ground stations.

- ***Output:*** The routing, key, and bandwidth assignment results for key services at each instant.
- ***Goal***: Schedule the routing, key, and bandwidth allocation for key-relay services and maximize the number of generated keys in quantum satellite network.
- ***Constraints***: Secret key rates, link durations, numbers of satellite-ground links, existence of GEO-LEO links and numbers of secret keys in QKPs.

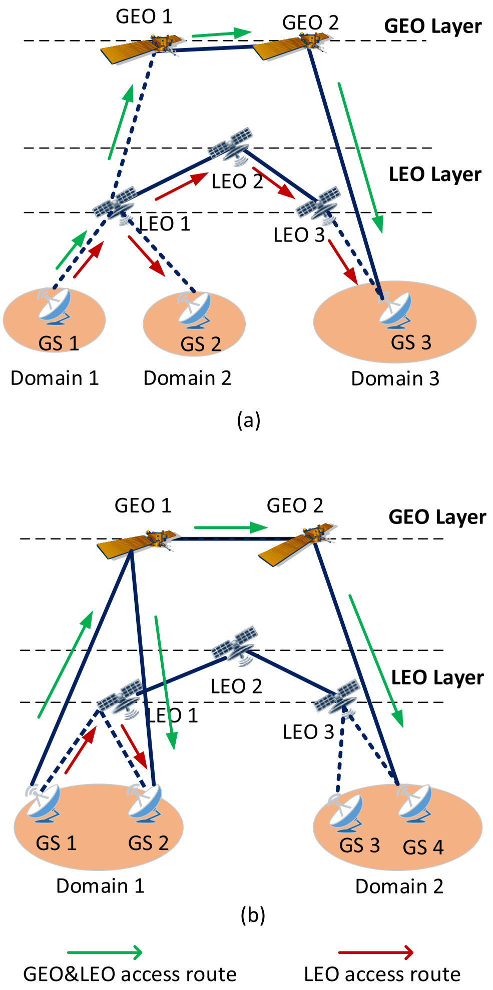


FIGURE 4. Route selection for key-relay services in two scenarios over double-layer quantum satellite network, (a) with and (b) without GEO-LEO links.

Fig. 4 illustrates different route selection schemes in two scenarios of double-layer quantum satellite network. Fig. 4(a) describes the scenario with GEO-LEO links and Fig. 4(b) describes the scenario without GEO-LEO links. The bold lines represent the continuous links and the dotted lines represent the intermittent links. The red arrows identify the routing only using LEO for accessing and the green arrows identify the joint GEO and LEO access routing. The latter scheme

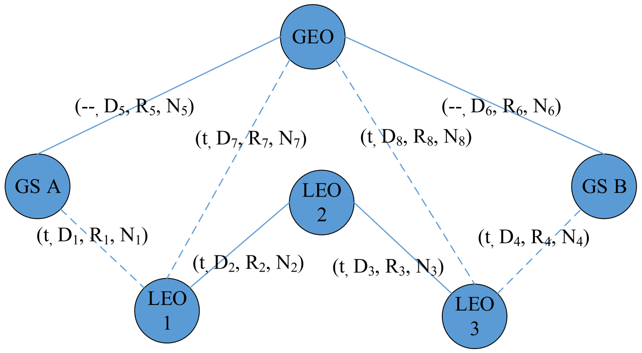


FIGURE 5. **Contact and resource graph of quantum satellite network.**

will be chosen when GS cannot access LEO. In scenario (a), the joint GEO and LEO routing can leverage two types of satellites to relay keys, while in scenario (b) it can only use LEO or GEO with the constraint of no GEO-LEO links.

Given the satellite networks topology is time-variable, the routing and resource allocation scheme should take the variation of link distance and link duration into consideration. In this paper we will handle the satellites routing problem based on the methodology of virtual topology [26]. We partition the satellite period (satellites move periodically) into many time slots, where satellite connectivity remains unchanged. In such time slot, satellite topology can be regarded as static. In short, dynamic topology is divided into a series of static virtual topologies.

V. DESIGNING ROUTING AND RESOURCE ALLOCATION ALGORITHM

Based on the double-layer quantum satellite network architecture, we design a joint GEO-LEO routing and key allocation (JGL-RKA) algorithm to solve the RKA problem.

A. TOPOLOGY AND RESOURCE GRAPH

Since the movement of satellites are predictable and periodic, the connectivity relationship of all nodes can be calculated for a time slot. Thus, we can calculate a series of fixed topology for each timeslot. Although topology graph is more accurate with smaller time slots, too many time slots may decrease the efficiency of route calculation. Thus, we set the time duration of a discrete topology as 1 minute in the 100 minutes of simulation. The period can be divided into n intervals as $\{[t_1, t_2), [t_2, t_3), \ldots, [t_{n-1}, t_n]\}$. The topology matrix is represented by $M = \{M_1, M_2, \ldots, M_n\}$, where each M_k belongs to the interval $[t_{k-1}, t_k]$.

Based on the topology matrixes, the contact and resource graph of quantum satellite network can be created. Fig. 5 shows an example of the contact and resource graph. The solid lines represent continuous links and the dotted lines represent intermittent links. Each link has several parameters (t, D_k, R_k, N_k), including time instant t, link distance D, secret key rate of link R, and available secret keys N in QKP of link between two nodes. This group of parameters identifies the state of link k at instant t. Each R of link is calculated based on link distance and link properties. For fixed links like GEO-ground links, we set their time as "–", as their key rates and link distances remain the same.

As the secret key of each QKP in each node is an important constraint of RKA, the remaining number of secret keys in QKPs should be updated timely in resource graph. The number N_k of secret keys in QKP at next instant is decided by the number of key generation and key consumption of last interval. At the start of each instant, N_k of link k can be calculated according to secret key rate as follow:

$$N_k = N_{Last} + R_k \cdot \Delta t \tag{1}$$

where N_{Last} denotes the remaining number of secret keys of last instant and Δt denotes the duration of a time slot.

According to [11], [12]. the secret key rate of link decreases linearly with the link distance. Therefore, we can describe the relationship between key rate R and link distance D as

$$\begin{aligned} &R = R_{max} \cdot (D - D_{max}) \big/ (D_{min} - D_{max}) \\ &D \in [D_{min}, D_{max}] \end{aligned} \tag{2}$$

D_{min} denotes the distance where key rate reaches the max value and D_{max} denotes the distance where key rate falls to zero.

Since the propagation environment of different type of links are different, the max key rate of different links should be set accordingly. Key rate of inter-satellite links is higher than satellite-ground links as optical signal will not experience atmospheric turbulence. In addition, key rates of LEO-ground links are higher than GEO-ground links due to the shorter transmission distance.

B. PROPOSED ALGORITHM

In order to solve the RKA problem, we design a JGL-RKA algorithm to select the access satellites and QKD route in quantum satellite networks.

In Step 1, Algorithm 1 obtains the time-varying topology matrix and updated resource map. The resource map is updated according to the key consumption and secret key rates of each link. Step 2 performs the access satellite selection to find an access satellite. This selection is executed for both source node and destination node. We propose two access satellite selecting algorithms under the scenarios with GEO-LEO links (Algorithm 2) and without GEO-LEO links (Algorithm 3).

In Algorithm 2, the terrestrial node searches for available LEOs as access satellite and chooses the best one which satisfies wavelength and key requirements. If there is no available LEO, it turns to select GEO as access satellite. While in Algorithm 3, the terrestrial node searches available LEOs as priority selection. If there is no available LEO, the source and destination nodes both turn to search GEO as access node because there are no GEO-LEO links. Third, RKA algorithm is performed for calculating inter-satellite path. If source node and destination node has accessed to the same satellite, inter-satellite route calculation is not required. We have used Dijkstra algorithm to calculate the shortest path between source

Algorithm 1 Joint GEO-LEO Routing and Key Allocation Algorithm

```
Input: $r(s, d, N, B), L$
Output: RKA solution for key services, updated network resource graph
Step 1
1:  for each key-relay service $r(s, d, N, B)$, do
2:      obtain the time-varying topology matrix and updated resource map according to current instant;
3:      if $L == 1$, then
4:          call Algorithm 2;
5:      end if
6:      if L == 0, then
7:          call Algorithm 3;
8:      end if
Step 2
9:      if $S_S == S_D$, then
10:         continue;
11:     else
12:         compute route path $P$ with Dijkstra
12:         algorithm;
13:     end if
14:     search available timeslots $T(P)$ along the
14:     path;
15:     if $T(P) \neq \emptyset$, then
16:         select one timeslot on each link;
17:             search the remaining number $N_k$ of secret
19:         keys in each QKP;
18:         if $N < N_k$, then
19:             select $N$ secret keys from QKPs on each link;
20:         else
21:             inter-satelite key assignment failed;
22:         end if
23:     else
24:         inter-satellite routing failed;
25:     end if
26: end for
```

Algorithm 2 Joint GEO and LEO Access Algorithm

```
1:  for source and destination ground station, do
2:      search all accessible LEOs for ground node;
3:      for each satellite do
4:          choose the best one according to shortest distance;
5:          search the remaining number $N_k$ of secret keys in satellite-ground QKP;
6:          if $N < N_k$ then
7:              select the satellite as access node;
8:              break;
9:          else
10:             continue;
11:         end if
12:     end for
13:     if no LEO satellite has enough keys, then
14:         search all accessible GEOs for ground node;
15:         repeat lines 3-12;
16:         if no GEO satellite has enough keys then
17:             access satellite selecting failed;
18:         end if
19:     end if
20: end for
```

and destination nodes. We also use First-Fit algorithm for timeslot and secret key allocation on each intermediate link for key services.

JGL-RKA algorithm is considered as a two-step process: 1) satellite-to-ground routing and 2) inter-satellite routing. In the scenario where GEO-LEO links exist, joint GEO and LEO access algorithm is executed to select access satellites for the pairs of ground nodes. Whereas in the scenario where GEO-LEO links do not exist, separated GEO and LEO access algorithm is executed to select access satellites for ground nodes.

The time complexity in worst situation of JGL-RKA algorithm is analyzed as follow. The time complexities of Algorithm 2 (lines 3-5) and Algorithm 3 (lines 6-8) in Step 1 are O($|L|+|G|$). The complexity of Step 2 is O($|L+G|^2+|W|\cdot|L+G-1|$). Thus, the total time complexity of JGL-RKA algorithm is O($|L+G|^2$).

Notations:

- $G_t(V_t, E_t)$: substrate topology of double-layer quantum satellite network at instant t, where V_t denotes the set of nodes and E_t denotes the set of optical links
- T: a period of satellite movement
- s: source ground node of key-relay service
- d: destination ground node of key-relay service
- $r(s, d, N, B)$: key-relay service
- S_S: source access satellite
- S_D: destination access satellite
- N: required number of secret keys of key-relay service
- B: required timeslot of key-relay service
- L: integer variable that equals 1if there are GEO-LEO links in double-layer quantum satellite network, and 0 otherwise
- LN: max number of ground stations that can be connected to one GEO
- N_G: maximum threshold of ground-GEO QKP
- N_S : maximum threshold of inter-satellite QKP

VI. SIMULATION RESULTS

To evaluate the performance of JGL-RKA algorithm, the simulation is performed on a satellite topology with 66 LEO, 3 GEO, and terrestrial network with 25 ground stations distributed across the globe (in major population centers). We use AGI STK to obtain the satellite trajectory and calculate satellite topology matrix. Fig. 6 shows the satellite topology. The LEO constellation is similar to the IRIDIUM system, where each LEO establishes 4 ISLs with adjacent

Algorithm 3 Separated GEO and LEO Access Algorithm

```
1:  for source and destination ground station, do
2:      search all accessible LEOs for ground node;
3:      for each satellite do
4:          choose the best one according to shortest distance;
5:          search the remaining number $N_k$ of secret keys in
            satellite-ground QKP;
6:          if $N < N_k$ then
7:              select the satellite as access node;
8:              break;
9:          else
10:             continue;
11:         end if
12:     end for
13: end for
14: if no access LEO for source or destination node then
15:     for source and destination ground station do
16:         search all accessible GEOs for ground node;
17:         repeat lines 3-13;
18:     if no access GEO for source or destination node then
19:         access satellite selecting failed;
20:     end if
21: end if
```

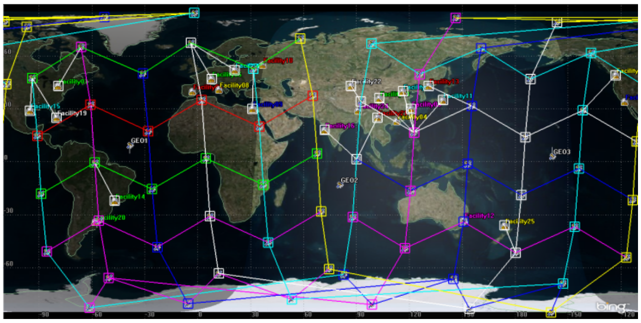


FIGURE 6. Satellite network topology used in simulation. (Picture from STK.) Considered ISL are drawn in the picture.

satellites, including intra-orbit and inter-orbit links. GEO can set up links with LEO in its coverage. Both GEO and LEO can set up links with multiple satellites depending on their optical terminal numbers. We assume that LEO can connect to at-most 4 ground stations simultaneously.

In our simulation, we assume that each pair of nodes generate quantum keys until the number of stored keys exceeds the maximum capacity of QKP, which is related to the storage capacity of satellite nodes. The key relay requests are generated randomly among all terrestrial nodes according to Poisson distribution. We consider 100000 key-relay services in each simulation and the holding time of each service is set as 30s. The proposed algorithm is implemented in C++ with Visual Studio 2017 on a computer with 3.0 GHz Intel Core i5-7200U CPU and 16 GB RAM.

In order to evaluate the performance of our proposed double-layer network and JGL-RKA algorithm, we present success probability (SP) of key-relay services in each scenario of simulation. The SP of access satellite selection and route scheme are reported in subsection A. To study the impact of satellite-ground links and QKP capacity on the key-relay scheme, the performance of different node capabilities is investigated in terms of SP in subsection B. In subsection C the impact of different service granularities is studied in terms of secret key number. In subsection D, we investigate the cost and the coverage rate of quantum satellite network to evaluate the performance of satellite topology. In subsection E and F, the security (described as hop number) and transmission delay of key-relay scheme are analyzed respectively. The simulation parameters are listed in table 1.

TABLE 1. Simulation parameters.

Parameters	Value
Number of time slots on per link	16
Max secret key rate of inter-satellite link	1000 units of keys
Max secret key rate of LEO-ground link	400 units of keys
Max secret key rate of GEO-ground link	40 units of keys
Key-relay service's time slot requirement	1
Hold time of a key-relay service	30 seconds
Interval of a time slot of topology	1 minutes
Processing delay on satellite	20ms

A. SP OF ACCESS SATELLITES AND ROUTE SELECTION

Fig. 7 shows illustrative results of success probability of key-relay services (SP) and access satellite selecting (SP-a) vs. traffic load under different topologies and route selections. We observe that SP decreases as traffic load (in Erlang) increases. We compare the SP under double-layer topology with single-layer topology without GEO. The scenario with and without GEO-LEO links (denotes as GL links) are also compared. The result shows that the SP of key-relay services in double-layer network is higher than the single-layer network.

We can observe similar phenomena on SP-a. The reason is that double-layer quantum satellite networks can provide additional GEO choice for access satellite selection, leading to higher successful probability in satellite-ground routing. On the other hand, the SP and SP-a over topology with GL links is slightly higher than that over topology without GL links.

This is because route selection with GL links can provide more flexibility for access-satellite selection. However, route selecting without GL links only allow ground nodes access to satellites in the same layer.

Fig. 7 c) shows the blocking probability of satellite-ground routing (BP-a), inter-satellite routing (BP-i) and bandwidth allocation (BP-b). Although key resource is the main constraint for key-relay services, bandwidth resource should be considered when traffic load is heavy. The overall trend of BP-i and BP-b is increasing with traffic load increasing, while BP-i fluctuates when traffic load is low. We notice that

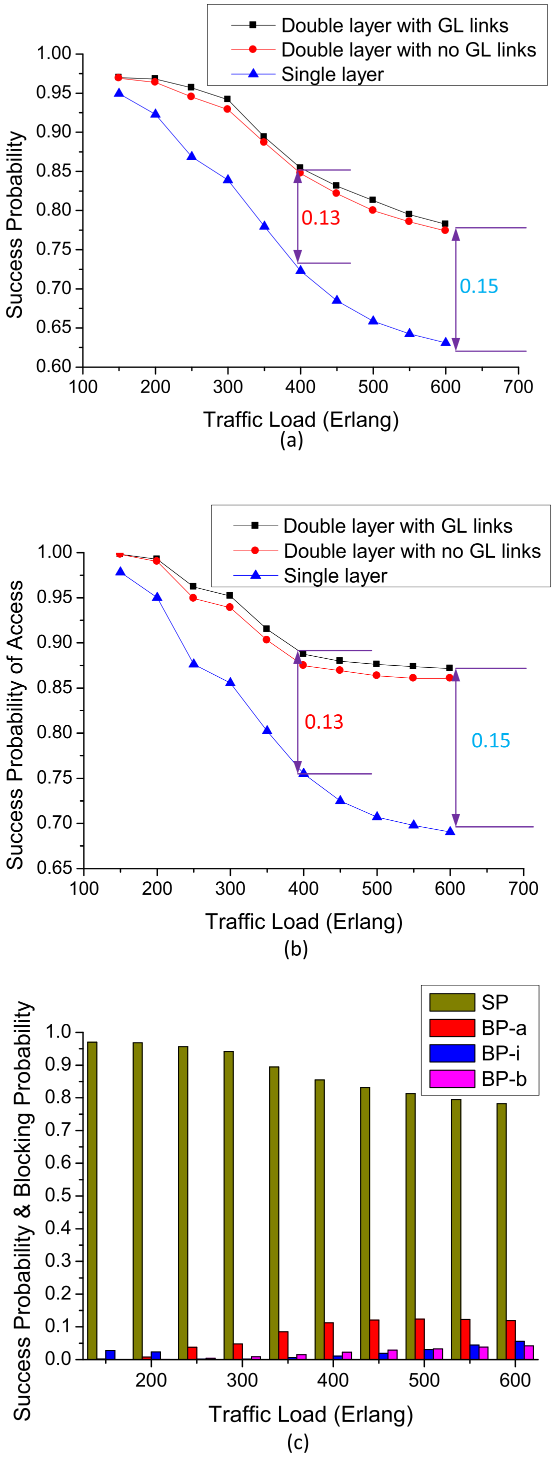


FIGURE 7. SP and SP-a vs. traffic load under different topologies and route selections ($LN = 10$, $N_G = 2000$, $N_S = 20000$, $N = 20$). (a) SP (b) SP-a (c) SP and BP.

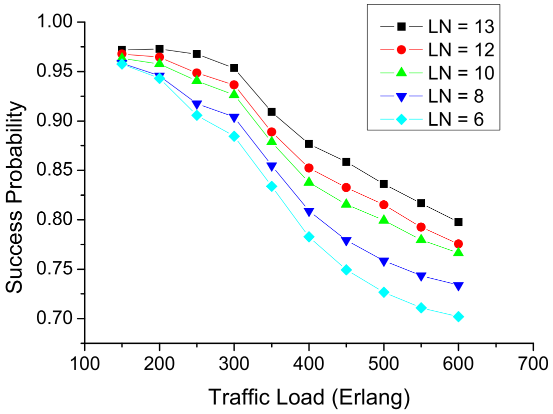


FIGURE 8. SP vs. traffic load with different numbers of GEO-ground links. ($N_G = 2000$, $N_S = 20000$, $N = 20$).

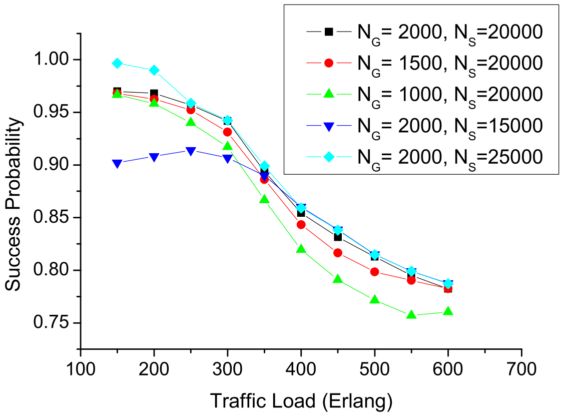


FIGURE 9. SP vs. traffic load with different capacity of QKP. ($LN = 10$, $N = 20$, with GL links).

the blocking probability of satellite-ground routing increases much faster than inter-satellite routing and time slot allocation. It indicates that blocking probability of access satellite selection is the major impact factor of 'total SP'. This is because the secret key rate and duration of inter-satellite links is much larger than satellite-ground links, which results in more secret keys in QKP and larger link capacity on inter-satellite links. As traffic load grows larger, more blocking in satellite-ground routing will lead to a larger share BP-a on total SP. Hence, satellite-ground routing is the major bottleneck for RKA over quantum satellite networks. This also validates the analysis in previous paragraph.

B. PERFORMANCE EVALUATION OF DIFFERENT NODE CAPABILITIES

Satellite nodes may possess different capabilities in terms of transponder number and storage resource. The number of transponders on satellite decides the maximum number of satellite-ground links. The storage capacity decides the maximum number of secret keys stored in QKP. These two factors determine the number of available keys between satellite and ground, which influences the SP of key-relay services.

1) SP VS. THE MAXIMUM NUMBER OF SATELLITE-GROUND LINKS

Fig. 8 presents SP vs. traffic load under different numbers of GEO-ground links. For this results, number of LEO links are fixed. We observe that SP gradually increases as the maximum number of GEO-ground links increases. This is because there are more accessible satellites for ground stations with more satellite-ground links serving. But the increase of GEO-ground links will add up the total links of quantum satellite network. Therefore, there is a trade-off between the SP and the costs of quantum satellite network.

2) SP VS. CAPACITY OF SECRET KEYS IN QKP

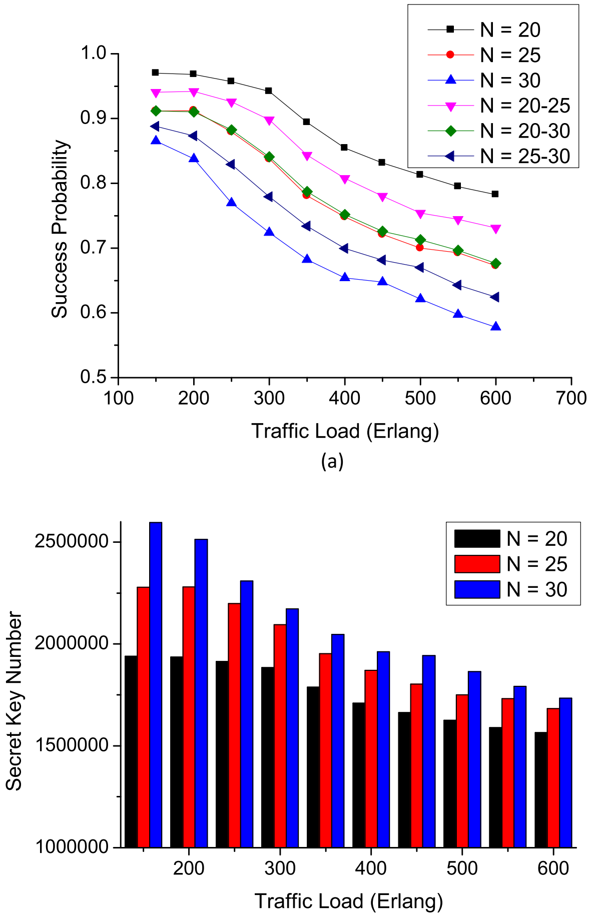
Fig. 9 illustrates the impact of QKP capacity on SP. We observe that SP increases with the increase of GEO-ground QKP (N_G) capacity. However, the capacity of inter-satellite QKP (N_S) remains unchanged. The increase of N_G has little impact when traffic load is low (150-200), while the impact becomes large as traffic load increases. This is because higher capacity of QKPs can enable QKP to store more secret keys in a satellite period and provide more secret keys for ground stations. But when the threshold exceeds 2000, SP will have little change as the threshold is enough for storing secret keys generated in one satellite period.

As for the impact of N_S, we can see that the SP increases with the increase of capacity, when traffic load is low (150-300). When traffic load become larger, the difference of curves will become quite small. The reason is that the SP of access satellite selecting is the major impact factor of SP when traffic load is large (concluded in section A). The increase of N_S can decrease the BP of inter-satellite routing, which have great impact on SP when traffic load is low. Therefore, the SP of different N_S is similar under high traffic load.

C. PERFORMANCE EVALUATION OF DIFFERENT SERVICE GRANULARITIES

The number of transmitted keys can be regarded as granularity of key-relay services. As the service granularity becomes larger, the key requirement on each link also increases. In this work we set uniform and non-uniform key demand for key-relay services. We compare different values for the 'number of required keys' for key-relay services (N) to observe the network performance. Fig. 10(a) illustrates that SP will decrease dramatically when N increases. Higher the secret-key demand increases the consumption of secret keys in QKPs and reduces the SP of key-relay services. We also compare non-uniform key demand [20]–[25], [25]–[30], and [20]–[30], where key demand is varying in a certain range. As a result, the demand of keys varying from 25 to 30 is almost the same with the demand of 20 because the average of [25]–[30] is 20.

Fig. 10 b) shows the number of generated keys vs. traffic load. Note that with the increase of N, the total number of generated keys over quantum satellite network is also increasing, while the SP is decreasing. In this case, the number of keys equals to service number multiplied N. Although more RKA for key-relay services are failed, the number of transmitted keys of one service increases. As a result, the total generated keys of the whole network increases. Therefore, there is a trade-off between SP and the total number of generated keys over quantum satellite network. Larger service granularity may increase the number of keys, at the cost of reducing the SP of key-relay services.



(a)

(b)

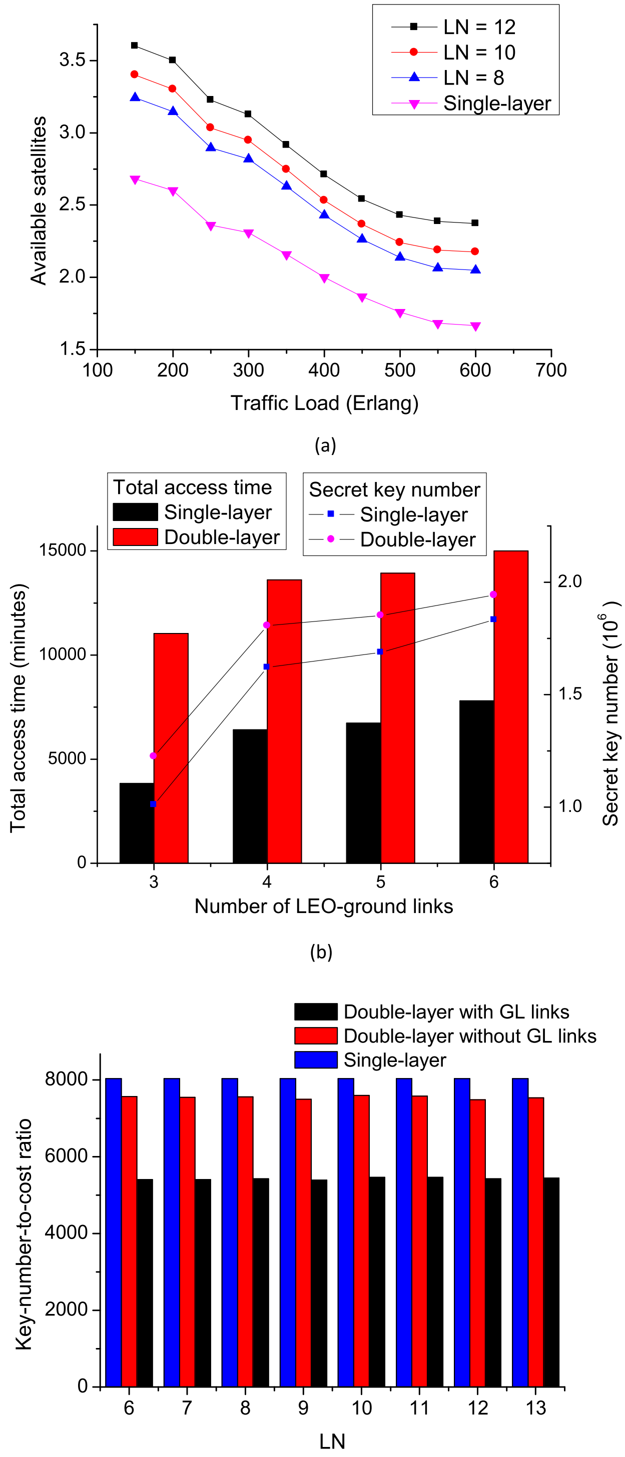
FIGURE 10. SP and secret key number vs. traffic load with different N ($LN = 10$, $N_G = 2000$, $N_S = 20000$). (a) SP (b) secret key number.

D. PERFORMANCE EVALUATION OF SATELLITE TOPOLOGY

The coverage ratio is an important index of satellite network performance. We use the average available satellites to evaluate the coverage ability of quantum satellite network, which is defined as coverage satellite with enough secret keys for a ground station. Fig. 11 (a) shows the average available satellites vs. different topologies. As traffic load increases, the number of average available satellites decreases, which results from the more key consumption of satellite-ground QKP.

Compared with single-layer network, there are more available satellites in double-layer quantum satellite network, and the number of available satellites increases as the number of GEO-ground links (LN) increasing.

Fig. 11(b) shows the total access time and secret key numbers of double layer and single layer networks. It can be observed that the access time becomes larger with more LEO-ground links. Specifically, the increasing rate is highest when there is 4 LEO-ground links. The access time



(a)

(b)

(c)

FIGURE 11. **(a) Average available satellites under different topologies (b) total access time & secret key number under different topologies when traffic load is 300 Erlang (c) key-number-to-cost ratio versus LN under different topologies when traffic load is 300 Erlang. ($N_G = 2000$, $N_S = 20000$, $N = 20$).**

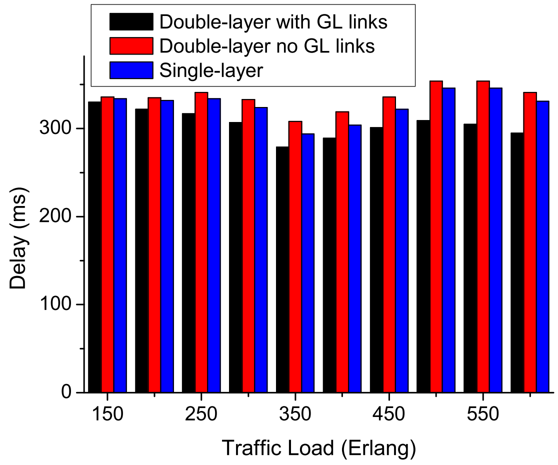


FIGURE 12. **Transmission delay for per key-relay service under different topologies. ($LN = 10$, $N_G = 2000$, $N_S = 20000$, $N = 20$).**

of double-layer network is larger than single-layer network because of the existence of GEO. The same phenomena can be seen in terms of the distributed secret key number over the whole network. The above results indicate that our proposed double-layer satellite topology performs well on the aspects of coverage and key generation.

Although double-layer quantum satellite network can enable network performance and provide larger network capacity, the additional cost of GEO should be considered. We use the total number of optical links to evaluate the cost of double-layer quantum satellite network. Then, we consider the key-number-to-cost ratio as an index of network performance. The key-number-to-cost ratio is defined as the ratio of total transmitted key number to total links number in satellite network.

Fig. 11(c) compares the key-number-to-cost ratio of quantum satellite network vs. the number of GEO-ground links, with different topologies. We observe that the key-number-to-cost ratio stay unchanged as the number of GEO-ground links increases. The key-number-to-cost ratio of double layer topology with GL links is much lower than single layer, while double layer without GL links is slightly lower than single layer. With more satellite links, the efficiency of quantum satellite network decreases. Therefore, there is a trade-off between network capacity and network efficiency.

E. PERFORMANCE EVALUATION OF TRANSMISSION DELAY FOR KEY-RELAY SERVICES

Due to the long distance of transmission in space, transmission delay is a key performance index of satellite services. In quantum satellite network, the transmission delay of key-relay services mainly consists of two parts, i.e., propagation delay of optical link and processing delay of each satellite node. The processing delay is large due to encryption and decryption on each intermediate node along the key-relay path. Fig. 12 presents the transmission delay vs. traffic load under different topologies. It shows that the transmission delay of key-relay services over double-layer satellite network without GL links is the highest. While the transmission delay of double-layer satellite network with GL links is the lowest.

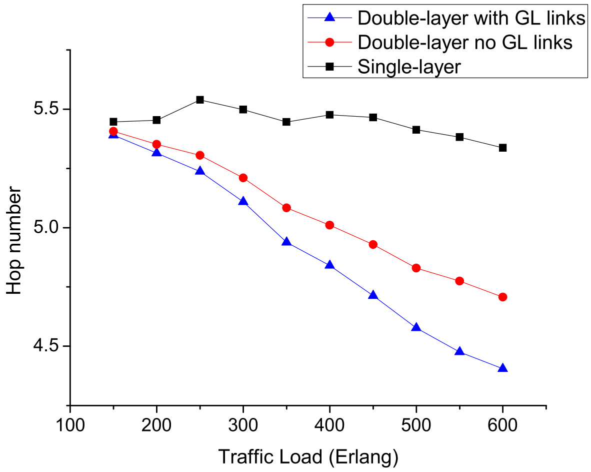


FIGURE 13. Average hop number of route path for key-relay service under different topologies. ($LN = 10$, $N_G = 2000$, $N_S = 20000$, $N = 20$).

This result is caused by several factors. GEO and LEO are used for relaying keys in double-layer network with GL links, while in single-layer network uses only LEO. Although GEO-ground link has high propagation delay, the joint GEO and LEO routing scheme can utilize GEO to decrease the hop of key transmission path, which saves a lot of processing time on intermediate nodes. LEO routing may generate a multi-hop path increasing the total delay. Therefore, transmission delay in inter-orbit-layer links is lower than single-layer network.

We also observe that the transmission delay in double-layer network without GL links is higher than single-layer network. This is because ground stations have to access to GEO or LEO simultaneously in the case without GL links. Ground stations served by GEO can use inter-GEO links to transmit keys, which produces a longer path than those served by LEO. The propagation delay of inter-GEO links is much higher than other links due to the ultra-long distance. Therefore, the total delay in double-layer satellite networks without GL links is larger compared with the case with GL links and single-layer network.

F. PERFORMANCE EVALUATION OF SECURITY FOR KEY-RELAY SERVICES

This subsection discusses the security property of our proposed key-relay scheme. In the trusted-repeater-based QKD scheme, the security of QKD might be weakened by the increase of the hop number of key relaying path because each intermediate node has to be trusted. Therefore, we use the average hop number of key-relay services to characterize the security of route path for key relaying. Fig. 13 illustrates the average hop number of route path for key-relay services under different topologies. It can be observed that the hop number over double-layer satellite network is lower than single-layer network. The hop number becomes smaller over double-layer network with GL links. This is because when the route path is long the secret key can be transmitted by GEO, which is concluded in the former subsection. Therefore, our proposed scheme can lower total hop number of key-relay path and increase the security of key relaying procedure. Also, we can see that hop number decreases with traffic load increasing. The possible reason is that when the consumption of secret key and time slot becomes larger, the long route paths are more likely to fail than short route paths, as their requirements for link resources are larger.

VII. CONCLUSION

In this paper, we investigate the current state of satellite-based QKD networks. Our study proposes a new architecture of double-layer quantum satellite networks. A Joint GEO-LEO Routing and Key Allocation algorithm is designed to resolve the end-to-end key distribution problem. The simulation results demonstrate that our proposed network architecture has better performance than single-layer satellite network. The SP of key-relay services increases with improved abilities of satellites, such as higher number of satellite-ground links and the capacity of secret keys in QKPs, and decreasing the granularity of services. The existence of GEO-LEO links can increase the SP slightly at the cost of setting up more optical links. Future works should study multi-layer quantum satellite network including MEO and more efficient routing scheme for key-relaying which might balance the secret key numbers in QKPs.

ACKNOWLEDGMENT

This work was supported in part by National Natural Science Foundation of China (NSFC) (61601052, 61822105), the Fundamental Research Funds for the Central Universities (2019XD-A05), State Key Laboratory of Information Photonics and Optical Communications of China (IPOC2019ZR01).

REFERENCES

[1] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, no. 7614, pp. 63–66, Aug. 2016.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, Dec. 2014.

[3] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New J. Phys.*, vol. 12, no. 10, Oct. 2010, Art. no. 103042.

[4] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, Feb. 2014, Art. no. 051123.

[5] S. Bahrani, M. Razavi, and J. A. Salehi, "Optimal wavelength allocation," in *Proc. 24th Eur. Signal Process. Conf.*, Budapest, Hungary, Aug./Sep. 2016, pp. 483–487.

[6] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 995–1004, Nov. 2017.

[7] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and A. B. Mukherjee, "Resource allocation in optical networks secured by quantum key distribution," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 130–137, Aug. 2018.

[8] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," *Opt. Express*, vol. 25, no. 22, pp. 26453–26467, Nov. 2017.

[9] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photon.*, vol. 7, no. 5, pp. 382–386, May 2013.

[10] G. Vallone, D. Bacco, and D. Dequal, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, 2015, Art. no. 040502.

[11] S. K. Liao, W. Q. Cai, and W. Y. Liu, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017.

[12] S.-K. Liao *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photon.*, vol. 11, no. 8, pp. 509–513, Aug. 2017.

[13] S.-K. Liao, W.-Q. Cai, and J. Handsteiner, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, 2018, Art. no. 030501.

[14] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 50–55, Aug. 2013.

[15] C. Simon, "Towards a global quantum network," *Nature Photon*, vol. 11, no. 11, pp. 678–680, Nov. 2017.

[16] P. Wang, X. Zhang, and G. Chen, "Quantum key distribution for security guarantees over quantum-repeater-based QoS-driven 3d satellite networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 728–733.

[17] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, no. 1, p. 30, 2017.

[18] M. Pfennigbauer, W. Leeb, and M. Aspelmeyer, "Free-space optical quantum key distribution using intersatellite links," in *Proc. CNES-Intersatellite Link Workshop*, 2003.

[19] S. R. Pratt, R. A. Raines, C. E. Fossa, and M. A. Temple, "An operational and performance overview of the IRIDIUM low earth orbit satellite system," *IEEE Commun. Surveys Tuts.*, vol. 2, no. 2, pp. 2–10, 2nd Quart., 1999.

[20] 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.*, vol. 15, no. 2, Feb. 2013, Art. no. 023006.

[21] K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. R. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, and G. Leuchs, "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, Jun. 2017.

[22] L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Towards quantum communication from global navigation satellite system," *Quantum Sci. Technol.*, vol. 4, no. 1, Dec. 2018, Art. no. 015012.

[23] F. Yu. *ScienceNet.cn, China*. Accessed: Aug. 10, 2017. [Online]. Available: http://news.sciencenet.cn/htmlnews/2017/8/384831.shtm?id=384831

[24] X. M. Liu and L. Zhang, "An on-board integrated system compatible with microwave, laser and quantum communication," CN Patent 103 873 151 A, May 10, 2014.

[25] D. T. S. Kelso. *CelesTrak*. Accessed: 2019. [Online]. Available: http://celestrak.com/satcat/

[26] F. Alagoz, O. Korcak, and A. Jamalipour, "Exploring the routing strategies in next-generation satellite networks," *IEEE Wireless Commun.*, vol. 14, no. 3, pp. 79–88, Jun. 2007.

DONGHAI HUANG received the B.S. degree in optoelectronic information engineering from Sun Yat-sen University, China, in 2017. He is currently pursuing the master's degree in information and communication engineering with the Beijing University of Posts and Telecommunications (BUPT), China. His research interests include quantum key distribution, quantum satellite networks, and satellite network security.

YONGLI ZHAO (Senior Member, IEEE) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), in 2010. From January 2016 to January 2017, he was a Visiting Associate Professor with the University of California at Davis (UC Davis). He is currently a Professor with the BUPT. He has published more than 300 international journal and conference papers. His research interests include software-defined networking, quantum key distribution, elastic optical networks, and optical network security.

TIANCHENG YANG is currently pursuing the bachelor's degree with the Beijing University of Posts and Telecommunications. His research interests include the Internet of Things, computer technology, and software development.

SABIDUR RAHMAN received the B.S. degree from the Bangladesh University of Engineering and Technology, in 2011, and the M.S. degree in computer science from the University of Texas at San Antonio, in 2014. He is currently pursuing the Ph.D. degree in computer science with the University of California at Davis. He has also research and development experience with AT&T Labs and Samsung Research and Development. His research interests include computer network virtualization, the use of machine learning and data analytics to solve network research problems, and cost-efficient networking.

XIAOSONG YU received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), in 2015. From September 2013 to September 2014, he was a Visiting Scholar with the University of California at Davis (UC Davis). He is currently an Assistant Professor with the Information Photonics and Optical Communications Institute, BUPT. He has coauthored more than 50 journal and conference papers. His research interests include elastic optical networks, software-defined optical networks, and optical network security.

XINYI HE is currently pursuing the Ph.D. degree in information and communication engineering with the Beijing University of Posts and Telecommunications (BUPT), China. Her research interests include quantum key distribution, quantum satellite networks, and satellite network security.

JIE ZHANG received the Ph.D. degree in electromagnetic field and microwave technology from the Beijing University of Posts and Telecommunications (BUPT), in 1998. He is currently a Professor and the Dean of the Information Photonics and Optical Communications Institute, BUPT. He has published more than 300 technical articles. He has authored eight books. He has also submitted 17 ITU-T recommendation contributions and six IETF drafts. His research interests include architecture, protocols, and standards for optical transport networks.