Journal of Computers Vol. 29 No. 2, 2018, pp. 276-285
doi:10.3966/199115992018042902027

Quantum Network Routing Algorithm Based on Trusted Center

Shao-sheng Jiang[1*], Xiao-jun Wen[1], Xin-can Fan[1]

[1] School of Computer Engineering, ShenZhen POLYTECHNIC, Shenzhen 518055, China
{jss, wxjun, horsefxc}@szpt.edu.cn

Received 24 July 2017; Revised 19 September 2017; Accepted 19 October 2017

Abstract. Quantum network routing algorithm is important for large-scale quantum network, especially when long-distance quantum communication system is established. In this paper, a quantum grid network model based on Trusted Center is proposed. With two-way quantum communication, the original information does not need to be transmitted through the quantum relay node, but instead a quantum entanglement channel established by two remote users using quantum teleportation. Using this model, the security of quantum relay nodes and quantum information transmission channels can be effectively guaranteed. Upon this, a quantum network routing algorithm is proposed to further improve the performance. When users need to set up an m-path quantum communication in the quantum grid network, this algorithm can greatly improve the efficiency of quantum communication, accompanied with self-correcting ability. Security analysis proves that the proposed m-path routing algorithm can greatly improve the security probability of quantum communication in quantum network.

Keywords: entanglement swapping, quantum routing, quantum teleportation, trusted relay

1 Introduction

Recently, research and experiments on quantum communication and quantum secure communication networks are developing rapidly. In 2004, the United States Department of Defense Advanced Research Projects Agency built the world's first DARPA Quantum Network [1]. In 2008, a joint European team in Vienna established secure communication based on Quantum Cryptography [2]. Then, in 2010, Japan's Toshiba European Research Center and the Swiss ID Quantique, Austria All Vienna research group established the Tokyo QKD Network [3]. In China, the research team led by Pan Jianwei accomplished a 13-km free space quantum communication experiment in 2005 for the first time in the world [4]. In 2008, they built a fiber-based quantum telephone network [20]. In 2012, they built the world's largest 46-node quantum communication test network in Hefei [5]. Currently, China has started the construction of the longest fiber-based quantum communication link in the world to connect Beijing and Shanghai. In 2016, the first quantum science experimental satellite was successfully implemented, and it was the first time to realize the quantum communication between the satellite and the ground. All these practical experiments and deployments indicate that secure inter-connections between the quantum nodes will be demanded and the establishment of large-scale quantum networks will be put on the agenda [6].

However, in the long-distance quantum communication systems or quantum network mentioned above, two remote nodes may require relay nodes to help establish secure quantum communication instead of a single section of quantum channel due to the limitation of quantum transmission distance [7]. Therefore, most of the quantum communication solutions use classical channel to transmit encrypted information, while the quantum channel is mainly used for quantum key distribution [8], such as the European SECOQC network and QKD network in Tokyo. In 2016, we proposed a quantum key relay transmission scheme [9], which is based on the characteristics of quantum entanglement transfer and quantum entanglement swapping. Studies show that the performance of quantum information transmission is promoted with an increase in the probability that the quantum entanglement is successfully established. But with the expansion of the communication network, the node number increases, and the security of

* Corresponding Author

network instability increases gradually along with network maintenance costs, and the throughput of the network is severely restricted. So, with the rapid development of quantum backbone networks in the future, the research of quantum network routing algorithms and performance analysis based on security is imperative.

In this paper, a quantum communication network model based on a trusted center and the establishment of a quantum communication network m-path grid based on the principle of quantum teleportation and entanglement switch are introduced. Based on the model and network architecture, an m-path routing algorithm of grid quantum communication network is proposed. Finally, the security and the efficiency of the proposed algorithm are analyzed.

2 The Grid Quantum Communication Network Based on Trusted Center

At present, there are mainly two quantum relay communication models, one is quantum communication relay model tree network structure based on quantum control centers [10] and the other one is bus network topology [11]. However, both of them need to solve the problems in the security and the efficiency of quantum information transmission [12]. In this paper, based on the above models, a grid quantum relay transmission system model under the control of trusted center is proposed. This model can not only ensure the security of the key nodes of quantum information transmission channel, but also enhance the security and efficiency of information transmission of quantum network as the transmission mode of grid m-path is more effective. The grid quantum relay transmission system model is shown in Fig. 1.

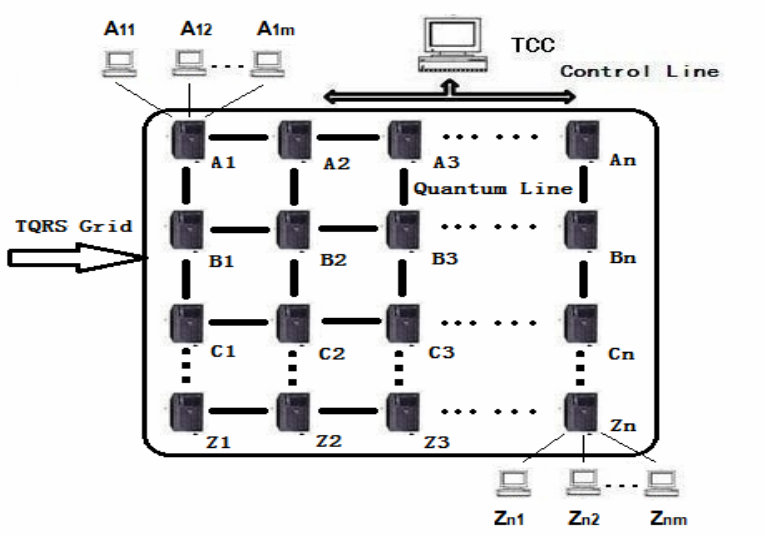

Fig. 1. The grid quantum relay transmission model under the TCC

In the figure, TCC is trusted control center, and ⟸ (arrow line) represents the channel in classic network. Control Line is connected to each relay node, so TCC ensures the legitimacy and security of all the relay nodes and transfers some auxiliary information to the node [14]. ——— (solid line, means directly connected), - - - (dotted line, means indirectly connected) represents quantum channel. It is mainly used to produce the remote quantum entanglement channel, and ultimately achieve quantum information relay transmission function.

All the relay nodes in the model are the quantum relay server (QRS). The quantum channel is established directly between each QRS and its user group and the adjacent QRS, so that the QRS can realize the quantum information relay function. Quantum communication between users in the same relay QRS group can be directly achieved through this QRS transmission, such as the QRS_{A1} user group contains A_{11}, A_{12}, A_{1m} and other users. If the two-user security communication cannot share the same QRS in a quantum communication network, then they can use several QRS through the grid quantum communication network based on TCC, as shown in Fig. 1, to complete quantum information transmission functions. In the network, TCC guarantees that every relay switching center node is legitimate and secure [13], and all the QRS are built as trusted quantum relay server modes, referred to as

TQRS [14]. Through the TQRS, this model can guarantee that any two users are indirect. For example, when two users belonging to $TQRS_{A1}$ group and $TQRS_{Zn}$ group need to communicate securely, they can build a quantum entanglement channel between the two users, and then complete quantum information transfer.

3 Establishment of Remote Quantum Entanglement Channel

In Fig. 1, the process of establishing a quantum entanglement channel between user A11 and user Znm can be described as Fig. 2.

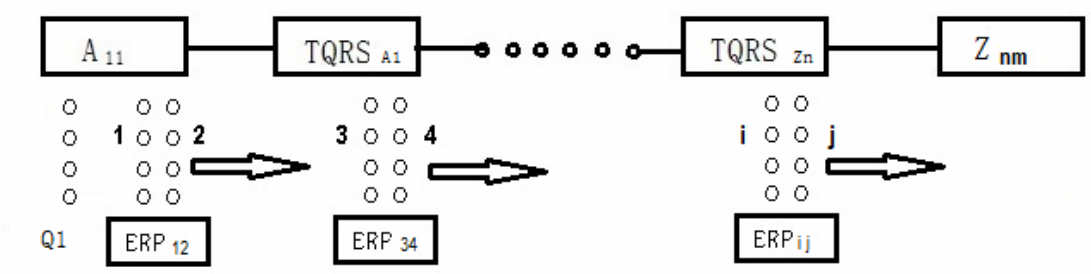

Fig. 2. The process of establishing quantum entanglement channel

In the absence of security communication tasks, each user (including all TQRS) should establish a lot of entangled pairs for their own. For example, in Fig. 2, the user A_{11} establishes a series of entangled pairs ERP_{12}, $TQRS_{A1}$ establishes a series of entangled pairs ERP_{34}, $TQRS_{Zn}$ establishes a series of entangled pairs ERP_{ij} (assuming that entangled pairs at the N relay node, i=2N+1, j=2N+2), etc. Each user (including all TQRS) should split their own entangled pairs into two quantum sequences. So, the user A11 split entangled pairs ERP_{12} into the quantum sequence 1 and 2. Similarly, $TQRS_{A1}$ have the quantum sequence 3 and 4, and $TQRS_{Zn}$ have the quantum sequence i and j, etc.

Before the transfer of quantum relay, there is no entanglement between each user (including all TQRS). In Fig. 2, the user A_{11} belong to the $TQRS_{A1}$ group, and the user Z_{nm} belongs to the $TQRS_{Zn}$ group. If these two users want to secure quantum communication, it is required to gradually establish a quantum entanglement channel between $TQRS_{A1}$ and $TQRS_{Zn}$, and may go through a lot of TQRS. If the quantum transfer initiator is A_{11}, it needs to build a quantum entanglement channel between user A_{11} and Z_{nm} by following steps below:

Step 1. The user A_{11} application to the server $TQRS_{A1}$ for the establishment of a quantum entanglement channel with Z_{nm}.

Step 2. The server $TQRS_{A1}$ application to TCC for the establishment of a quantum entanglement channel with Z_{nm}.

Step 3. TCC proposed quantum channel routing based on trusted relay networks, and notifies each TQRS that sends the front quantum of its first quantum entanglement sequence to its next relay node (or goal) in this quantum channel. At this time, all quantum entanglement pairs consist of system states as follows:

$$|\phi>_{1234...ij}=|\phi>_{12}\otimes\phi>_{34}\otimes\cdots\otimes|\phi>_{ij} \quad (1)$$

Step 4. As shown in Fig. 2, the $TQRS_{A1}$ will have 2 and 3 quantum at a time, which $TQRS_{A1}$ can measure 2 and 3 quantum using BELL measurement. The base measurement that it selects is:

$$|\phi>_{23}>\frac{1}{\sqrt{2}}(|H>_2|V>_2|H>_3) \quad (2)$$

After measuring, system state is:

$$|\phi>_{14...ij}=<\phi|_{23}[\phi>_{12}\otimes\phi>_{34}\otimes\cdots\otimes|\phi>_{ij}]=|\phi>_{14}\otimes\cdots\otimes|\phi>_{ij} \quad (3)$$

Step 5. With Step 4, each communication node in the quantum channel routing in turn will measure 2 quanta in the hands using Bell measurement. At last, system state is:

$$|\phi>_{1j}=\frac{1}{\sqrt{2}}(|H>_1|V>_j+|V>_j|H>_1) \tag{4}$$

The formula 4 shows, although quantum 1 and *j* are initially independent of each other, after repeated BELL measurements they established a new entangled relationship and formed new entangled pairs $|\varphi>_{1j}$. According to Fig. 2, at this time, quantum 1 is stored in user A_{11}, and quantum *j* is stored in user Z_{nm}. User A_{11} and user Z_{nm} complete the establishment of the quantum entanglement channel between them.

4 Quantum Information Transmission Using Quantum Teleportation

Secure transmission of quantum information can be realized based on the proposed model in section 2, the quantum entanglement channel construction scheme in section 3 and quantum teleportation. Firstly, quantum teleportation requires both sides to share an EPR pair. Second, the sender measure the shared 1/2 EPR pair and the quantum information transmitted using BELL measurements. Then, the receiver's shared 1/2 EPR pair will collapse on the moment when measuring and form another state. As long as the sender transmits the measurement results to the receiver, the receiver can do the corresponding unitary transformation on the state of his own 1/2 EPR pair according to the measurement results, then he get the sent quantum information [15].

For example, if the user Alice needs to send quantum 1 in an unknown quantum state to the user Bob, the quantum state can be described as:

$$|\phi>_1=a|0>+b|1> \tag{5}$$

Alice prepared a quantum EPR pair and quanta were 2 and 3 respectively. Assuming the entangled state of this ERP pair is:

$$|\phi>_{23}=\frac{1}{\sqrt{2}}(|H>_2|V>_3-|V>_2|H>_3) \tag{6}$$

If Alice left quantum 2, quantum 3 is transmitted to Bob through the quantum channel, then the mixed state of these quanta can be expressed as:

$$\begin{aligned}|\phi>_{123}=\frac{1}{2}[&(\varphi^+>_{12}(-a|0>b|1)_3+|\varphi^->_{12}(-a|0>b|1)_3+|\psi^->_{12}(b|0)+a|1>)_3+\\&|\psi^+>_{12}(-b|0)+a|1>)_3]\end{aligned} \tag{7}$$

According to the above formula, when Alice combines quantum 1 and 2 to do BELL measurements, quantum 3 for Bob will instantly collapse to another quantum state, as shown in Table 1. As long as Alice will transmit the measurement results to Bob，Bob can complete the corresponding unitary transformation on quantum 3 and recover its state into the initial state $|\varphi>_1$ of quantum 1. The corresponding unitary transformation is shown in Table 1.

Table 1. The operation table of the recovery quantum state corresponding to quantum teleportation

Alice measurement results	Quantum 3 state for Bob	Corresponding unitary transformation
$\|\varphi>_{12}$	$-a\|0-b\|1>$	$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$
$\|\varphi^->_{12}$	$-a\|0+b\|1>$	$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$
$\|\psi^->_{12}$	$b\|0>+a\|1>$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
$\|\psi^+>_{12}$	$-b\|0>+a\|1>$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$

In the section 3, there is a request to secure quantum communication between user A_{11} and user Z_{nm}. According to steps 2-5, a quantum entanglement channel has been established between user A_{11} and user Z_{nm}, and then the following steps to quantum communication are:

Step 1. User A_{11} mix quantum information sequence A which need to be transmitted and their check code sequence S using Hamming code rules, and mix into quantum sequence P:

$$P=\{ S1,S2,A1,S3,A2,A3,\cdots,A_i,\cdots,S_j,\cdots,S_r,\cdots A_k\}\ A_i\in\{0,1\}\ S_j\in\{0,1\} \quad \textbf{(8)}$$

According to the Hamming code check rule, if K is quantum information digits which need to be transmitted and r is the check code digits which need to be added, they should meet the following relationship:

$$N = K + r \leq 2r - 1 \quad \textbf{(9)}$$

According to the formula (8), the relationship between quantum information digits and the check code digits is shown in Table 2.

Table 2. The relationship table between quantum information digits and the check code digits

Quantum information digits	1	2~4	5~11	12~26	27~57	58~120	121~247	……
Check code digits	2	3	4	5	6	7	8	……
Quantum information digits	1	2~4	5~11	12~26	27~57	58~120	121~247	……

Step 2. According to the process of quantum teleportation, when user A_{11} combines the first quantum S_1 in quantum sequence P and quantum 1 in the quantum entanglement channel to do BELL measurement, the quantum entanglement channel will instantly collapse. The state of quantum S_1 will be teleported to the user Z_{nm} according to Table 1. After a successful recovery, the user Z_{nm} inform the user A_{11} that quantum information transfer has been successful.

Step 3. Following the steps in Section 3, the user A_{11} and user Z_{nm} need reestablished the quantum entanglement channel and they will repeat Step 2 above. In this process, user A_{11} will continuously send all states of the quantum sequence P to user Z_{nm} using quantum teleportation. Finally, user A_{11} and user Z_{nm} shared quantum sequence P.

Step 4. User A_{11} announced the all quantum information regarding Hamming code. Ideally, the results of users A_{11} and Z_{nm} measuring these quanta should be consistent with the relationships in Table 1. If there is noise or other attacks in the channel, the user A_{11} and Z_{nm} can detect the error rate of quantum information sequences during the transfer process. If the error rate exceeds a certain threshold, the quantum communication results will be given up, but otherwise can be regarded as a successful quantum information sequence A transfer.

$$A=\{A_1, A_2, \cdots, A_i, \cdots, A_K\}\ A_i\in\{0, 1\} \quad \textbf{(10)}$$

Step 5. The user Z_{nm} further purifies the quantum information sequence A using automatic error correction technology or information enhancement technology, such as Hamming code error correction technology.

In accordance with the above steps, users A_{11} and Z_{nm} transfer quantum information A via a quantum entanglement channel. In the transmission process, a trusted relay network model is established under the control of the TCC so that every quantum relay exchange center node is legitimate and secure. By using quantum entanglement swapping, quantum relay nodes are only used to build quantum entanglement channels. Quantum information A is only transferred directly by both the user using the method of quantum teleportation, and they cannot be obtained by quantum relay nodes and the quantum channel. Therefore, the common “intercept/resend,” “middle man” and other attacks are unable to succeed [16-17].

5 Quantum Network Routing Algorithm Based on TCC

As shown in Fig. 1, there may be multiple quantum communication paths between two remote nodes in the quantum grid network. In order to ensure the security of communication and improve the communication efficiency, all communication routing between users should be designed. In all the designed routes, the priority path should be the number of relay nodes is smaller and there are no overlap

parts with other paths. If one path has an overlap with another path and the number of its relay nodes is relatively more, it can be set to the standby path. The optimal design path is the path of fewest relay nodes, and the second path is the path of second fewest relay nodes, etc., with remaining paths determined by priority in this same manner. When a channel of the selected path is busy, a user can use the next priority path as an alternate quantum communication route. This design can strengthen quantum communication smoothly, and improve the switch rate. Finally, this design can increase the reliability of quantum network and improve the service quality of quantum network.

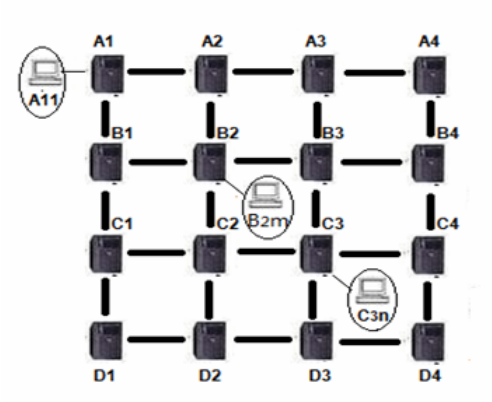

Fig. 3. A 4x4 grid quantum communication network

In Fig. 3, if users A11 and B2m need quantum communication, there are two paths for A1-A2-B2 and A1-B1-B2 between them. As the numbers of relay nodes of both paths are the same, they can randomly select the path A1-A2-B2 as the best path, and A1-B1-B2 path as the second best path. Similarly, if the user C3n and B2m need quantum communication, there are four independent paths between them, B2-A2-A3-A4-B4-C4-C3, B2-B1-C1-D1-D2-D3-C3, B2-B3-C3, and B2-C2-C3. Among them, path B2-B3-C3 and path B2-C2-C3 which the numbers of relay nodes are 3 can be selected for priority 1 (the highest) and 2 path. The remaining two paths which the number of relay nodes are 7 can be used as a low priority path. More quantum channels may exist between any two TQRS in a quantum network, and this can improve the transmission rate of quantum information and further ensure the communication's security.

Assuming that users A_{11} and C_{3n} need quantum communication in a quantum network as shown in Fig. 3, there are two non-overlapping paths between them, which are P_1 and P_2. Path P_1 is A1-A2-A3-B3-C3, and the priority of path P_1 is 1. Path P_2 is A1-B1-C1-C2-C3, and the priority of path P_2 is 2. When path P_1 or P_2 is busy, the chosen alternate path is A1-A2-B2-B3-C3 or A1-B1-B2-C2-C3. In this example, the quantum network routing algorithm can be designed as follows:

Step 1. Communication from user A_{11} to the server $TQRS_{A1}$ requires the establishment of a quantum entanglement channel with C_{3n}.

Step 2. Communication from server $TQRS_{A1}$ to TCC requires the establishment of a quantum entanglement channel with C_{3n}.

Step 3. TCC proposed several quantum channel routings based on a trusted relay network, and notifies each TQRS that sends the front quantum of its first quantum entanglement sequence to the next level of its relay node (or goal) in these quantum channels.

Step 4. First, it must determine that the priority 1 path is busy or not. (All relay nodes with received quantum must submit a confirmation message to the $TQRS_{A1}$. If any relay node in a path does not return a confirmation message within a specified time, it means this path is busy.) If the priority 1 path is busy, this path is set to the lowest priority, and the priorities of other paths are increased by 1. Then again select the priority 1 path and repeat Step 4.

Step 5. If the priority 1 path is not busy, $TQRS_{A1}$ send the confirmation message to user A_{11}that a quantum entanglement channel can be established between user A_{11} and Z_{nm} according to the steps described in Section 3. At this time, the number of idle quantum channel routings will be reduced by 1 and the priority of other paths will be increased by 1. Until the quantum entanglement channel is created and the quantum information is transferred between users in accordance with the steps of Section 4, the channel occupancy is released, and the priority of this path is set to 1 (the highest), and the priority of other paths are reduced by 1, and the number of free quantum channel routings is increased by 1.

Step 6. According to the priority, it is determined that the next path is busy or not. If the path is idle,

$TQRS_{A1}$ send the confirmation message to user A_{11} again, the second quantum entanglement channel can be established between user A_{11} and Z_{nm} according to the steps described in Section 3 and the users can transfer the rest of the quantum information through this channel. All the processed are the same as Step 4 until all free quantum channels were chosen and the number of free quantum channels routings is 0.

Step 7. The transfer of quantum information is completed, and all occupied channels are freed.

This quantum network routing algorithm makes full use of the grid characteristics of quantum network and enhances the flow rate of the quantum communication between users and quantum communication flow.

6 Security Analysis of Communication in Quantum Grid Network

In the quantum network relay transmission system, with the increasement of the communication distance, the number of relays required by quantum communication will increase, which will affect the security of quantum communication [18-19]. Particularly when users use only a single channel to complete the transfer of quantum information and as long as there is a partial path that was attacked in this quantum channel, the quantum entanglement channel will probably not be built and quantum information cannot transfer. If the quantum routing algorithm of the previous section is adopted, the quantum information will be transmitted using the multipath dispersion method. The attacker must destroy all possible paths to succeed, and thus the risks of failure are effectively reduced and the security of quantum communication is effectively increased.

In Fig. 3, if users C_{3n} and B_{2m} need quantum communication, there are four independent paths between them. If it is assumed that the path P_1 is B_2-B_3-C_3, path P_2 is B_2-C_2-C_3, path P_3 is B_2-A_2-A_3-A_4-B_4-C_4-C_3, and path P_4 is B_2-B_1-C_1-D_1-D_2-D_3-C_3, and if users C_{3n} and B_{2m} are safe, their TQRS and all TQRS in the way are safe because TCC ensures their safety according to the grid quantum relay transmission system model in Section 2. If it is assumed that the safety probability of the path between all the adjacent TQRS is p and independent, the safety probability of multipath quantum communication will be greatly improved.

When the communication path is only P_1, the safety probability of the quantum communication is $1-(1-p^2)=p^2$;

When the communication paths are P_1 and P_2, the safety probability of the quantum communication is $1-(1-p^2)(1-p^2)=2p^2-p^4$;

When the communication paths include P_1, P_2 and P_3, the safety probability of the quantum communication is $1-(1-p^2)(1-p^2)(1-p^6)=2p^2-p^4+p^6-2p^8+p^{10}$;

When the number of communication paths is 4, the safety probability of the quantum communication is $1-(1-p^2)(1-p^2)(1-p^6)(1-p^6)=2p^2-p^4+2p^6-4p^8+2p^{10}-p^{12}+2p^{14}-p^{16}$.

From the above, with the number of communication paths increasing, the security probability of quantum communication networks is also increasing. If the number of paths is n when the two users are communicating, each path is marked as (1, 2…, *m*…, *n*), and n_m is the number of links between TQRS in the m path. Then, for the m path through nm link, the safety probability of this path can be calculated as:

$$P(m)=1-(1-p^{n_m})=p^{n_m} \tag{11}$$

If all *n* paths can be quantum communication and it is assumed that a common link number of the *i* and *j* pathways is (n_i, n_j), then the joint security communication probability of all n paths is:

$$P(1,2,\cdots,n)=1-\prod_{i=1}^{n}(1-p^{n_j})=\sum_{1\le i\le n}p^{n_i}-\sum_{1\le i,j\le n,i\ne j}p^{|n_i+n_j-(n_i,n_j)|}+\sum_{1\le i,j,k\le n,i\ne j,j\ne k,k\ne i}p^{|n_i+n_j+n_k-(n_i,n_j)-(n_j,n_k)-(n_k,n_i)+(n_i,n_j,n_k)|}-\cdots \tag{12}$$

If quantum communication uses random routing methods and the experimental data can be calculated using formula 12, when it is considered that the safety probability of each link is respectively 0.8 and 0.9 in two cases, the relation of security probability versus link number is respectively shown in Fig. 4 and Fig. 5.

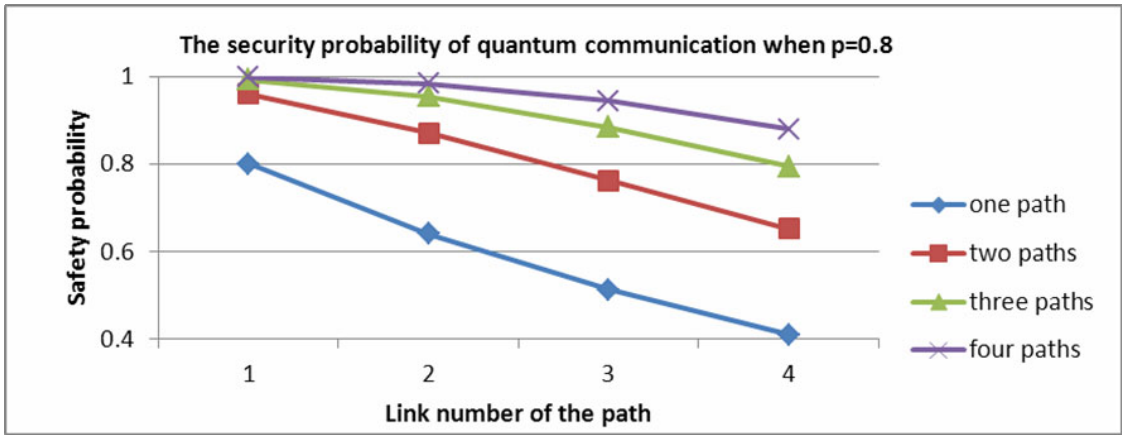

Fig. 4. The security probability of quantum communication when p=0.8

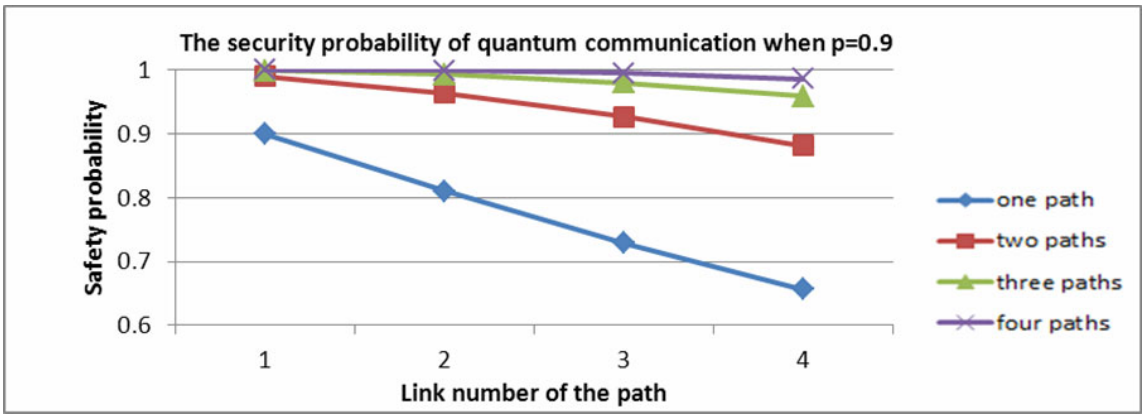

Fig. 5. The security probability of quantum communication when p=0.9

As shown in Fig. 4 and Fig. 5, the experimental results indicate that when the safety probability of the link is fixed, the optional path between the two users will increase the probability of safe communication. If the safety probability of the link is increased, the security probability of quantum communication will significantly increase. If the communication path of both users can have two or more pathways, the security probability of quantum communication will improve much more than with only one path. Although there can be higher security with more than one path, it can be concluded that when path numbers increase to a certain extent, the increase in security will become insignificant while requiring more traffic to confirm data forwarding. This may lead to network congestion and reduction in the efficiency of the quantum communication.

7 Conclusions

In this paper, a quantum communication network model based on a trusted center and the establishment of a quantum communication network m-path grid based on the principle of quantum teleportation and entanglement switch are introduced. The scheme can guarantee the security and legitimacy of the relay nodes in the quantum key transmission channel by using the trusted control central network model. The establishment of a remote quantum entanglement channel is adopted, which ensures the security of the original key, and that the original key will not be transmitted directly in the quantum relay node and quantum relay channel. The characteristics of quantum teleportation are used, so that the users remote quantum entanglement channel that are established can directly carry out the quantum key agreement and determine the final shared quantum key. Using this model, a grid m-path routing algorithm of quantum communication is proposed to improve the efficiency of quantum communication with a certain ability of self-correction. In the quantum grid network model based on trusted centers, TCC ensures the safety of each TQRS and quantum entanglement channel using quantum teleportation and entanglement swapping

to ensure the security of the quantum communication path. Security analysis of the routing algorithm shows that even if the attackers destroy one of all quantum communication paths between both users, users can still ensure secure quantum communication using the quantum grid network routing algorithm.

Acknowledgements

The work was partially supported by Guangdong Provincial Natural Science Foundation, China (No. 2016A030313023), Shenzhen Basic Research Project (No. JCYJ20160322114027138).

References

[1] D. Pearson, High-speed QKD Reconciliation using Forward Error Correction, AIP Conference Proceedings 734(2004) 299-302.

[2] M. Peev, SECOQC: Major results, the QKD-Network Prototype in Vienna, AIP Conference Proceedings 1110(2009) 323-326.

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger, Field test of quantum key distribution in the Tokyo QKD Network, Optics Express 19(2011) 10387-10409.

[4] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M.D. Shaw, J.A. Stern, S.W. Nam, D. Oblak, Q. Zhou, J.A. Slater, W. Tittel, Measurement-device-independent quantum key distribution: from idea towards application, Journal of Modern Optics 62(14)(2015) 1141-1150.

[5] T. Lian, M. Nie, Model and simulation of entanglement signaling repeater NetWork based on entanglement dwapping, Optics Express 41(2012) 1251-1255.

[6] Y.-B. Li, S.-W. Xu, Q.-L. Wang, F. Liu, Z.-J. Wan, Quantum key distribution based on interferometry and interaction-free measurement, International Journal of Theoretical Physics 55(1)(2016) 98-106.

[7] X. Wen, An E-payment system based on quantum group signature, Physica Scripta 82(2010) 065403-065407.

[8] X. Wen, Y. Tian, X. Niu, A group signature scheme based on quantum teleportation, Physica Scripta 81(2010) 055001-055005.

[9] S. Jiang, X. Wen, Quantum key relay transmission model based on entanglement switch and teleportation, Journal of Computers 28(3)(2017) 1-10.

[10] G. Xu, X.-B. Chen, Z. Dou, Y.X. Yang, Z. Li, A novel protocol for multiparty quantum key management, Quantum Information Processing 14(8)(2015) 2959-2980.

[11] X. Wen, Y. Liu, N. Zhou, Realizable quantum broadcasting multi-signature scheme, Int. J. Mod. Phys. B. 22(24)(2008) 4251-4259.

[12] X. Wen, Y. Liu, N. Zhou, Secure quantum telephone, Optics Communications 75(1)(2007) 278-282.

[13] Y.S. Yu, Extended research on trusted network connection under Web environment, Journal of East China Normal University(Natural Science) 4(2009) 137-140.

[14] S. Jiang, R. Chi, X. Wen Quantum key relay scheme based on trusted control center, Telecommunication Science 30(2014)

102-107

[15] X. Wen, Y. Liu, Y. Sun, Quantum MultiSignature potocol based on teleportation, Z. Naturforschung A 62(2007) 147-151.

[16] X. Wen, X. Niu, L. Ji, Y. Tian, A weak blind signature scheme based on quantum cryptography, Optics Communications 282(4)(2008) 666-669.

[17] X. Wen, Y. Chen, J. Fang, An inter-bank E-payment protocol based on quantum proxy blind signature, Quantum Information Processing 12(1)(2013) 549-558.

[18] X. Wen, Y. Liu, Secure authentic digital signature scheme using quantum fingerprinting, Chinese Journal of Electronics 17(2)(2008) 340-344.

[19] D. Wu, W. Yu, B. Zhao, C. Wu, Quantum key distribution in large scale quantum network assisted by classical routing information, International Journal of Theoretical Physics 53(10)(2014) 3503-3511.

[20] K. Cui, Research on real time processing of quantum key distribution, [dissertation] Taipei: University of Science and Technology of China, 2014.