Journal of Computers Vol. 28, No. 3, 2017, pp. 1-10
doi:10.3966/199115592017062803001

Quantum Key Relay Transmission Model Based on Entanglement Switch and Teleportation

Shaosheng Jiang*, and Xiaojun Wen

School of Computer Engineering, SHENZHEN POLYTECHNIC, Shenzhen 518055, China
szwxjun@sina.com

Received 01 July 2015; Revised 27 July 2015; Accepted 10 August 2015

Abstract. A quantum key transmission model based on an entanglement switch and teleportation is proposed. When the user needs to share a quantum key, the original quantum key does not need to go through quantum relay nodes. However, it goes through the user for the establishment of the quantum entanglement channel and uses quantum teleportation to determine the quantum key. Using this model of quantum key relay transmission, the proposed model can effectively guarantee the security of the quantum relay node and the quantum information transmission channel. Research shows that, the quantum information transmission performance of this model increases along with an increase in the probability of success of the original quantum entanglement. The original quantum key also has high efficiency.

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

1 Introduction

In long-distance quantum communication systems, two sides need secure communication that is generally not directly connected to the quantum channel and the relay mode must be used to transfer quantum information in a quantum communication network. Because current large-scale quantum networks have not yet been completed, research directions are mostly dependent on transmitting encrypted information from a classical network channel, and the quantum channel is mainly used for only quantum key distribution. There are two main classes of quantum key distribution schemes. One is based on the "non-orthogonal" quantum state [1-2], while the other is based on the entanglement state [3-4].

The quantum entangled state is an important research direction for next generation secure communications, and it is widely used in quantum teleportation, quantum key distribution, quantum computing, and etc. The main function of the entanglement switch is that it allows two quantum entanglements without any interaction. Thus, the entangled state is not influenced by the distance between the two quanta. At present, many researchers have established the quantum relay system for channel security using the special properties of the entangled state [5-6]. But, quantum entanglement swapping can only solve the security problem of the quantum channel, but the security and the legitimacy of the quantum relay nodes cannot be confirmed. Furthermore, the key agreement of the users cannot be carried out in the quantum channel.

In regards to security, quantum teleportation performs well for secure delivery. But quantum teleportation must rely on a quantum entanglement channel that is directly established between the users who need to transmit the quantum information. If not, the shared quantum key can only reach the target user through each relay point in the path. Therefore users that are not directly connected to the quantum channel want security sharing for the quantum key. Furthermore, to ensure the legitimacy of safety relay nodes, it usually requires that a comparison is made of the quantum information in the quantum channel between each pair of relay nodes referring to BB84 protocol to ensure the security of the quantum channel [7-8]. This ensures that not only that the efficiency of quantum key can be reduced, but also that both the user and each relay node in the transmission process needs to be constant for classical

* Corresponding Author

information exchange, whereby there is a reduction in both the transmission efficiency of quantum key relay transmission and the utilization of initial quantum key.

In this paper, a quantum key relay transmission scheme is proposed, which is based on the characteristics of quantum entanglement transfer and quantum entanglement swapping. 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. Studies show that the two users without a directly connected quantum channel can still use this model to carry out the quantum key security transmission, and that the performance of quantum information transmission is promoted with an increase in the probability that the quantum entanglement is successfully established.

2 Quantum Relay Transmission Model Based on Quantum Entanglement Swapping

2.1 Quantum Entanglement Swapping

The quantum entanglement swapping is an exchanging process where two or more pairs of quantum entanglement which is not entangled in a super space remote transmitting manner. An EPR pair is a double quantum system which is currently used in the maximum entangled state. The state may be expressed in any of the following four states.

$$|\varphi^+>=\frac{1}{\sqrt{2}}(|00>+|11>) \tag{1}$$

$$|\varphi^->=\frac{1}{\sqrt{2}}(|00>+|11>) \tag{2}$$

$$|\psi^+>=\frac{1}{\sqrt{2}}(|01>+|10>) \tag{3}$$

$$|\psi^->=\frac{1}{\sqrt{2}}(|01>-|10>) \tag{4}$$

These four states are entangled states (Bell state). Clearly, the four states $\{\{|\varphi^+>,|\varphi^->,|\psi^+>,|\psi^->\}\}$ constitute a complete orthogonal basis of the double quits system, which can be used to measure the state of the double quits system, i.e. Bell measurement. If $|H>_i$ and $|V>_j$ represent the two entangled particles' state in horizontal and vertical polarization, the entanglement can be expressed in the following formula:

$$|\phi>_{ij}=\frac{1}{\sqrt{2}}(|H>_i|V>_j+|V>_i|H>_j) \tag{5}$$

Assume that Alice and Bob share two Bell States $|\phi>_{12}$ and $|\phi>_{34}$, where Alice has quantum 1 and 4, and Bob has quantum 2 and 3. The tensor product state of $|\phi>_{12}$ and $|\phi>_{34}$ can be expressed as $|\phi>_{12}\otimes|\phi>_{34}$. If Alice performs the Bell measurements on quantum 1 and 4, then she obtains one result with equal probability among $|\varphi^+>14,|\varphi^->,|\psi^+>14,|\psi^->14$. If Bob performs Bell measurements on quantum 2 and 3, he will obtain the same results as Alice. Thus, the original quantum of non - entanglement (1, 4) and (3, 2) is the generated entanglement, respectively. That is:

$$|\phi>_{1234}=\frac{1}{2}[|H>_1|V>_2+|V>_2+|V>_1|H>_2]\otimes[|H>_3|V>_4+|V>_3|H>_4] \tag{6}$$

After Alice performed the Bell measurements on quantum 1 and 4, the entanglement pair produced the corresponding decomposition and the collapse of the entanglement. Four kinds of Bell states can be used to re-do the equivalence decomposition for the entangled states of these 4 quanta, and are stated as the following:

$$|\phi>_{1234}=\frac{1}{2}[|\varphi^{+}>_{14}|\varphi^{+}>_{23}+|\varphi^{-}>_{14}|\varphi^{-}>_{23}+|\psi^{+}>_{14}|\psi^{+}>_{23}+|\psi^{-}>_{14}|\psi^{-}>_{23}] \quad (7)$$

After Alice performed Bell measurements, the entanglement will collapse to formula (7) and any one of the four sub items on the right. For example, the result of Alice in a measurement is $+|\psi^{-}>_{14}$, and then she informs Bob of this result. So Bob knows that his quantum 2 and 3 not only have been entangled through the association of the collapses, but have also been in the $+|\psi^{+}>_{23}$ state.

The two quantum which are not together and have no entanglement can be entangled using the quantum entanglement swapping property, resulting in and entanglement channel between these quantum. Thus, if two users in which there is no quantum channel directly connected, need to share a quantum key for secure communications, they can build the quantum entanglement channel between the users before the quantum key is share, and then they are able to transfer the quantum key with quantum teleportation. This method is not guarantees high security, but also according to the efficiency calculation method of the QKD scheme [9], the utilization efficiency of the quantum key has nothing to do with the number of relay nodes which will be analyzed later.

2.2 Quantum Relay Transmission Model

For the typical long-distance quantum relay communication system, the proposed method is shown in Fig. 1 [10]. It uses two sets of quantum sequences as communication resources that both the user and the quantum relay server generate respectively. The encrypted information is transmitted in the classical channel, and the encryption key is transmitted in the quantum channel.

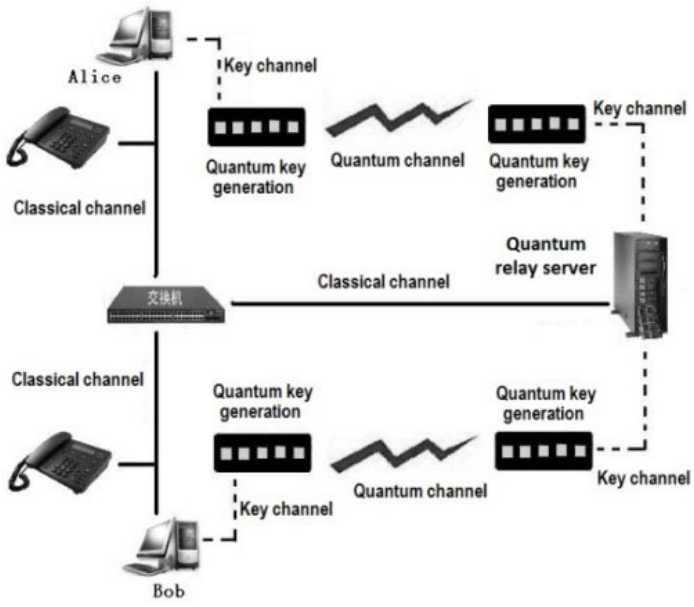

Fig. 1. The typical long-distance quanta relay communication system

At present, many scholars study this type of quantum relay communication model. Some view it through the formation of quantum communication relay model tree network structure based on quantum control centers [11] and some through the formation of bus network topology and quantum relay transmission [6]. However, they all need to solve the two problems of the safe and efficient transmission of quantum information. In this paper, a quantum relay transmission model based on the trusted control center is proposed, which guarantees the security of the key nodes in the transmission channel of the quantum information relay. The trusted relay network model is shown in Fig. 2.

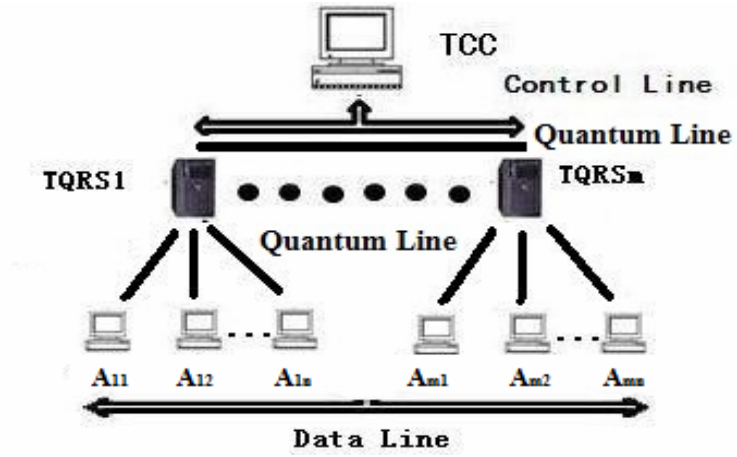

Fig. 2. A quantum key relay transmission model under TCC control

In the figure, TCC is the trusted control center, and the ⟺ Control Line represents the classic network. Among them, the Data Line is the transmission line used to transfer encrypted data between the user, and the Control Line is a classical channel for the trusted control center to ensure the legitimacy and security of all the relay nodes. The quantum channel is represented by ——, which is responsible for the generation of the quantum entanglement channel and the relay transmission of the key.

In the proposed model, all relay nodes are quantum relay servers, and the following is a description of QRS process. The relay node is used to connect with its neighboring users and other QRS's, establishes a quantum channel, and realizes the corresponding quantum key relay transmission function. The user in the same relay QRS group can accomplish the quantum key sharing between the two users by using the quantum relay communication system as shown in Fig. 1. If two users which need to secure communication are unable to realize the sharing of a quantum relay server in the network, the relay transmission function will be accomplished by the network based on the trusted control center (TCC) as shown in Fig. 1. TCC guarantees the legitimacy and security of each relay exchange center node [10], that is, all QRS's will be built as a trusted quantum relay server (TQRS) mode. Through TQRS, the model can achieve the indirect of any two users, such as when two users belong to $TQRS_1$ group and $TQRS_m$ group. When these two users secure communication, the quantum entanglement channel can be built first, and then the security sharing of the quantum key can be carried out.

2.3 Establishment Scheme of Quantum Remote Entanglement Channel

Assume that in Fig. 2, the user A_{11} wants to share the quantum key with the user A_{mn}. The process of establishing a quantum entanglement channel between them can be described in Fig. 3.

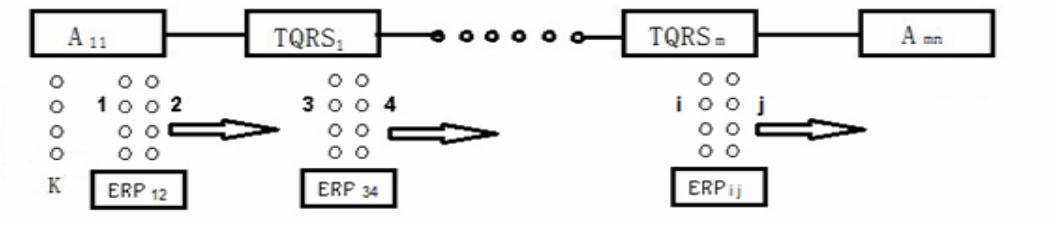

Fig. 3. The process of establishing the quantum entanglement

In the absence of security communication tasks, each user (including all TQRS) should be established for their own series of entangled pairs. For example, in Fig. 3, the user A_{11} establishes a series of entangled pairs ERP_{12}, $TQRS_1$ establishes a series of entangled pairs ERP_{34}, $TQRS_m$ establishes a series of entangled pairs ERP_{ij} (assuming that the entangled pairs at the N relay node are 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 splits the entangled pairs ERP_{12} into the quantum sequence 1 and 2. Similarly, $TQRS_1$ has the quantum sequence 3 and 4, and $TQRS_m$ has the quantum sequence i and j, etc.

Before the transfer of the quantum relay, there is no entanglement between each user (including all TQRS). In Fig. 2, the user A_{11} belong to the $TQRS_1$ group, and the user A_{mn} belongs to the $TQRS_m$ group. If these two users want to share quantum key K for secure communication, it is required for $TQRS_1$ to $TQRS_m$ to gradually establish a quantum entanglement channel, and it may go through many TQRS. If the quantum key transfer initiator is A_{11}, it needs to realize quantum key shared between user A_{11} and A_{mn}, and build a quantum entanglement channel by following the steps outlined below:

Step 1. The user A_{11} to the server $TQRS_1$ application requires the establishment of a quantum entanglement channel with A_{mn}.

Step 2. The server $TQRS_1$ to the TCC application requires the establishment of a quantum entanglement channel with A_{mn}.

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

$$|\phi>_{1234...ij}=|\phi>_{12}\otimes|\phi>_{34}\otimes\cdots\otimes|\phi>_{ij} \tag{8}$$

Step 4. As shown in Fig. 3, the $TQRS_1$ will have 2 and 3 quantum at a time, in which $TQRS_1$ can be 2 and 3 quantum with BELL measurements. The base measurement that it selects is:

$$|\phi>_{23}>=\frac{1}{2}(|H>_2|V>_3+|V>_2|H>_3) \tag{9}$$

After measuring, the system state is:

$$|\phi>_{14...ij}=<|\phi_{23}[|\phi>_{12}\otimes|\phi>_{34}\otimes\cdots\otimes|\phi>_{ij}]=|\phi>_{14}\otimes\cdots\otimes|\phi>_{ij} \tag{10}$$

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

$$|\phi>_{1j}=\frac{1}{\sqrt{2}}(|H>_1|V>_j+|V>_j|H>_1) \tag{11}$$

Formula 11 shows that although quantum 1 and j are initially independent of each other, after repeated BELL measurements they establish a new entangled relationship and form new entangled pairs $|\varphi>_{1j}$. According to Fig. 3, at this time, quantum 1 is stored in user A_{11}, and quantum j is stored in user A_{mn}. User A_{11} and user A_{mn} complete the establishment of the quantum entanglement channel between the two.

Step 6. The user A_{11} and user A_{mn} realize the transfer of the quantum key based on quantum teleportation, and is described in more detail in the next section.

Step 7. After the quantum information is transmitted, user A_{mn} sends the information to the user A_{11} to confirm the receipt of quantum 1 and begin applying for the next quantum delivery.

Step 8. Repeat step 2-7 until the original quantum key is successfully shared.

3 Quantum Key Distribution Scheme Based on the Model

Quantum information security transmission can be realized based on the model in section 2.2, the channel construction scheme in section 2.3 and quantum teleportation. First, quantum teleportation requires that both sides secure communication sharing an EPR pair. Second, the sending user uses the shared 1/2 EPR pair and the quantum information transmitting to conduct the Bell measurements. Then, the receiving user's shared 1/2 EPR pair will collapse at the moment of measurement and form another state. As long as the sending user transmits the measurement results to the receiving user, the receiving user can complete the corresponding unitary transformation on his own 1/2 EPR pair of the state according to the measurement results, namely restoring the quantum information needing to be sent.

If the user Alice needs to send information 1 in an unknown quantum state to the user Bob, the quantum state can be described as:

$$|\phi>_1=a|0>+b|1) \tag{12}$$

If Alice prepared a quantum EPR pair, and the quantum information is 2 and 3, then the assumption of the entangled state of this ERP pair is:

$$|\phi>_{23}=\frac{1}{\sqrt{2}}(|H>_2|V>_3-|V>_2|H>_3) \tag{13}$$

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

$$\begin{aligned}|\phi>_{123}=\frac{1}{2}[&|\varphi^+>_{12}(-a|0>-b|>1)_3+|\varphi^->_{12}(-a|0>+b|1>)_3+|\psi^->_{12}(-b|0>+a|1>)_3\\&+|\psi^+>_{12}(-b|0>+a|1>)_3]\end{aligned} \tag{14}$$

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 transmits the measurement results to Bob, then Bob can complete the corresponding unitary transformation on quantum 3 and recover its state into quantum 1 of the initial state $|\varphi>_1$. 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 2.3, there is a request to share quantum key between user A_{11} and user A_{mn}. According to steps 2-5 between user A_{11} and user A_{mn}, a quantum entanglement channel has been established, then the following steps to the quantum key distribution are outlined as follows:

Step 1. The quantum sequence of the original key K prepared by the user A_{11}.

$$K=\{K_1, K_2, \ldots, K_i, \ldots, K_N\} \qquad Ki \in \{0, 1\} \tag{15}$$

Step 2. Secure detection preparation for the quantum entanglement channel. After the establishment of the quantum entanglement channel, user A_{11} randomly selects S quantum (S=N-M) in the original quantum key as the channel detection particle, and records the number of them in the sequence. N is the quantum number of the total quantum sequence, and M is the quantum number that is ultimately used as the quantum key to share.

Step 3. According to the process of quantum teleportation, when user A_{11} combines the first quantum K1 in the quantum sequence K and quantum 1 in the quantum entanglement channel to conduct Bell measurements, the quantum entanglement channel will instantly collapse and the quantum state of K_1 will teleport to the user A_{mn}. The user A_{mn} only needs to restore the quantum states of K_1 according to Table 1, and after a successful recovery, inform user A_{11} that the quantum information transfer has been successful.

Step 4. Following the steps in Section 2.3, user A_{11} reestablished the quantum entanglement channel and user A_{mn} will repeat step 3 above. In this process, user A_{11} will continue to teleport all quantum states of the quantum sequence K to user A_{mn}. Finally, user A_{11} and user A_{mn} have shared quantum sequence K.

Step 5. User A_{11} announces the quantum information regarding the channel detection particle. Ideally, the results of users A_{11} and A_{mn} measuring these quanta should be consistent with the relationships in Table 1. If there is noise or other attacks in the channel, user A_{11} and A_{mn} can detect the error rate of the

quantum information sequences during the transfer process. If the error rate exceeds a certain threshold, the quantum communication results will be given up. Otherwise, it can be regarded as a successful quantum information sequence K transfer. The remaining M quantum of the original shared key can become shared key K' as in accordance with the user agreement.

$$K'=\{ K'_1, K'_2, \ldots, K'_I, \ldots, K'_M\} \qquad K'_{i\in}\{0, 1\} \tag{16}$$

Step 6. The user A_{11} and A_{mn} can adopt the information reconciliation and privacy enhancement technology for the agreed K', which can finally get the security private key shared by the two parties.

In accordance with the above steps, users A_{11} and A_{mn} share quantum key K' 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 key K' needs to be transferred and negotiated directly by both the user using the method of quantum teleportation, and by quantum relay nodes. Therefore, the common "intercept/resend," "middle man" and other attacks are unable to succeed [12].

4 System Performance and Efficiency Analysis

4.1 System Performance Analysis

According to the above scheme, the quantum entanglement channel with multiple relay nodes must first be established between the two users, so the performance of the system is influenced by the time of entanglement between each node. It is assumed that $TQRS_1$ and $TQRS_2$ are adjacent relay nodes, when they have successfully established a quantum entanglement channel, and some scholars have already analyzed the total time needed to transmit a quantum bit [13]. It can be expressed as:

$$T = T_n + T_s + T_e + T_m + T_t + T_d \tag{17}$$

In formula 17, T_n is the average time that it takes for $TQRS_1$ to notify $TQRS_2$ which is ready to receive quantum information. T_s is the average time that the entangled light source of $TQRS_1$ and $TQRS_2$ synchronous is established. T_e is the average time that it takes for $TQRS_1$ and $TQRS_2$ to establish entangled photon pairs. T_m is the average time that is required for $TQRS_1$ to conduct the Bell measurement. T_t is the average amount of time that the measurement results are transmitted in the classical network. And, T_d is the average time that it takes for $TQRS_2$ to detect the transmitted quantum bits.

The following assumptions are made:

(1) P_e is the probability of the successful establishment of entanglement between $TQRS_1$ and $TQRS_2$. P_m is the probability of $TQRS_1$ successful Bell measurements. P_d is the probability of a $TQRS_2$ successful detection of the quantum bits. The three probabilities of P_e, P_m and P_d are independent.

(2) They all obey the geometric distribution, the required number of entangled pairs that $TQRS_1$ and $TQRS_2$ successfully established, and the required number of times that the Bell measurement was successful, and the required transmission times that $TQRS_2$ successfully detected the quantum bits.

(3) τ_e is the required time to establish an entanglement. τ_m is the required time to do a Bell measurement. τ_d is required time that the receiver requires to detect the quantum bits.

The probability P that $TQRS_1$ and $TQRS_2$ is able to successfully transmit a quantum bit can be obtained by:

$$P=P_e \times P_m \times P_d \tag{18}$$

So, the throughput rate of the quantum information between $TQRS_2$ and $TQRS_1$ can be expressed as:

$$T_p=P/T= P_e \times P_m \times P_d/(T_n + T_s + T_e + T_m + T_t + T_d)$$

$$T_e= \tau_e/P_e \quad T_m= \tau_m/P_m \quad T_d= \tau_d/P_d \tag{19}$$

According to the establishment scheme of the quantum remote entanglement channel as stated above in Section 2.3, it is assumed that the number of relay nodes between the user A_{11} and A_{mn} is N, and that

T_n, T_s, T_e, T_m, T_d and other times on each entanglement in the establishment of the quantum entanglement channel will be produced. Thus, the throughput of the quantum information between user A_{mn} and A_{11} can be described as:

$$T_p = P_e \times P_m \times P_d / N(T_n + T_s + T_e + T_m + T_d) + T_t \quad \textbf{(20)}$$

The following assumptions are made:

1. Because the sender always notifies the receiver to receive the quantum bits and that they transmit all the measurement results in the classical network, and the classical channel is currently based on CSMA/CD Ethernet, it can be set so that the time required for transmitting a message is 1us (i.e., T_t and T_n).
2. In the quantum channel, the time of the entanglement is 2ns, the time for detecting the transmitted quantum bits is 5ns, the synchronization time of the entangled source is 10ns, and the time of obtaining the Bell measurement is 2ns.
3. The probability of the successful measurement of the sender and the successful detection of the receiver is 70%.

According to formula 20, it can be calculated as:

$$T_p = P_e \times 0.49 \times 10\text{^}9 / [N(1020 + 2/P_e) + 1000](\text{qubit/s}) \quad \textbf{(21)}$$

According to formula 21, the throughput rate of the quantum information transmitted by the two parties can be obtained as shown in Fig. 4.

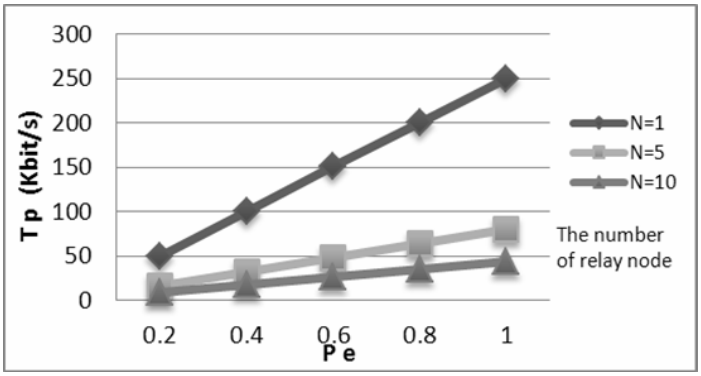

Fig. 4. The relational graph among the throughput rate of the quantum information, the probability of successful entanglement and the number of relay node

From the graph it can be seen that the information throughput of the quantum relay system clearly increased with the increase of P_e between user A_{11} and A_{mn}, which is in accordance with the basic features of the quantum operation system. In addition, the throughput of the quantum information is also influenced by the number of relay nodes. When the number of relay nodes increases, the throughput of the quantum information also decreases.

All of the assumptions are ideal. In fact, the quantum entanglement channel in free space is affected by the noise and the particles state in the entangled state change. So, with the increase of the relay nodes number in the quantum system, the throughput of quantum information will also decrease. However, the noise interference of the throughput of quantum information will be reduced as P_e increases.

In addition, it can be seen from formulas 20 and 21 that the throughput of the quantum information is greatly affected by the transmission time of the classical network. The throughput rate of quantum information can also be increased by 10 times if the time required to pass information in the classical network can be increased by 10 times and reaches 0.1us. This shows that in the quantum relay transmission system, the information transmission efficiency of the classical network plays an important role in the throughput rate.

4.2 System Efficiency Analysis

In the analysis of the quantum relay transmission system, the system efficiency can be calculated using the efficiency formula of the QKD scheme proposed by Cabello [9].

$$\varepsilon = b_s/(q_t+b_t) \quad \textbf{(22)}$$

In formula 22, b_s is the total number of quantum information bits received by Bob, and q_t and b_t are the total number of quantum information bits and the total number of classical information bits which are transmitted by Alice and Bob, respectively, in the generation key process, but they do not contain exchanged information bits for the detection of the quantum channel security. Previous studies show that the quantum key generates no longer needs to exchange any information except for the required information for the quantum channel security detection. Therefore, b_s =M, q_t =M, b_t =0, and the relay system efficiency is ε = 100%.

Of course, in the quantum relay system, user A_{11} and A_{mn} must spend a number of entangled quantum pairs to complete the establishment of the quantum entanglement channel for the shared quantum. The system efficiency can then be calculated using an improved efficiency formula proposed by Li et al. [14].

$$\eta_t=b_s/(q'_t+b_t) \quad \textbf{(23)}$$

In formula 23, q'_t is the total quantum number of quantum entanglement channels except for the quantum for quantum channel security detection. According to the previous relay scheme, b_s =M, q'_t= (2N+1) M, and b_t = 0(here N is the number of relay nodes). So the total efficiency of the relay system can be calculated as η_t =1/(2N+1), and the quantum efficiency is changed by the number of relay nodes.

5 Conclusion

In this paper, a quantum key relay model by quantum entanglement swapping is proposed. In this model, the security and legitimacy of relay nodes in quantum key relay transmission channels are guaranteed by using a network structure based on TCC. Because of the establishment of the quantum entanglement channel, the quantum key is not transmitted directly in the relay node and quantum channel, and therefore the security of the quantum key is ensured. Using the characteristics of quantum teleportation, the users can directly carry out quantum key agreement and determine the quantum shared secret key which cannot be obtained by the quantum relay node. These methods effectively prevent common attack modes, and ensure the security of the shared quantum key. The system performance and the efficiency of the model are analyzed and the results are satisfactory.

Acknowledgements

The work was supported by Natural Science Foundation of Guangdong Province (No. S20130100 15471) and Shenzhen Basic Research Project (No. JCYJ20120617140737337, JCYJ2013033115180 3073).

References

[1] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Physical Review Letters 68(21)(1992) 3121-3124.

[2] D. BruB, Optimal eavesdropping in quantum cryptography with six states, Physical Review Letters 81(14)(1998) 3018-3021.

[3] Y. Guo, G.H. Zeng, Deterministic quantum key distribution using two non-orthogonal entangled states, Communications in Theoretical Physics 47(3)(2007) 459-463.

[4] X.L. Zhang, Y.X. Zhang, K.L. Gao, Quantum key distribution scheme based on dense encoding in entangled states, Communications in Theoretical Physics 43(4)(2005) 627-630.

[5] X.C. Pei, G. Yan, D. Liu, B.-B. Han, N. Zhao, A quantum repeater communication system based on entanglement, Acta Photonica Sinica 37(12)(2008) 2422-2426.

[6] T. Lian, M. Nie, Model and simulation of entanglement signaling repeater network based on entanglement swapping, Acta Photonica Sinica 41(10)(2012) 1251-1255.

[7] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, N. Gisin, Long distance quantum teleportation in a quantum relay configuration, Physical Review Letters 92(4)(2004) 706-718.

[8] R.-F. Xu, Z.-X. Xiao, Y.-P. Li, Z. Nie, X.-J. Wen, Quantum key relay protocols between the any terminals in Internet, Application Research of Computers 30(2)(2012) 507-509.

[9] A. Cabello, Quantum key distribution in the holevo limit, Physical Review Letters 85(26)(2000) 5635-5638.

[10] S.S. Jiang, R.N. Chi, X.J. Wen, Quantum key relay scheme based on trusted control center, Telecommunications Science 30(6)(2014) 102-107.

[11] C. Jose, R. Carlos, Optimum design for BB84 quantum key distribution in tree-type passive optical networks, Journal of the Optical Society of America B 27(6)(2010) A146-A151.

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

[13] C.-H. Zhu, X.-C. Pei, H.-X. Ma, X.-F. Yu, A scheme for quantum local area networks and performance analysis, Journal of Xidian University 33(6)(2006) 839-843.

[14] X.-H. Li, F.-G. Deng, C.-Y. Li, Y.-J. Liang, P. Zhou, H.-Y. Zhou, Deterministic secure quantum communication without maximally entangled states, Journal of the Korean Physical Society 49(4)(2006) 1354-1359.