Quantum communication for satellite-to-ground networks with partially entangled states*

Chen Na(陈 娜)†, Quan Dong-Xiao(权东晓), Pei Chang-Xing(裴昌幸), and Yang-Hong(杨 宏)

State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, *China*

(Received 26 July 2014; revised manuscript received 13 September 2014; published online 10 December 2014)

To realize practical wide-area quantum communication, a satellite-to-ground network with partially entangled states is developed in this paper. For efficiency and security reasons, the existing method of quantum communication in distributed wireless quantum networks with partially entangled states cannot be applied directly to the proposed quantum network. Based on this point, an efficient and secure quantum communication scheme with partially entangled states is presented. In our scheme, the source node performs teleportation only after an end-to-end entangled state has been established by entanglement swapping with partially entangled states. Thus, the security of quantum communication is guaranteed. The destination node recovers the transmitted quantum bit with the help of an auxiliary quantum bit and specially defined unitary matrices. Detailed calculations and simulation analyses show that the probability of successfully transferring a quantum bit in the presented scheme is high. In addition, the auxiliary quantum bit provides a heralded mechanism for successful communication. Based on the critical components that are presented in this article an efficient, secure, and practical wide-area quantum communication can be achieved.

Keywords: satellite-to-ground quantum communication network, partially entangled states, entanglement swapping, quantum teleportation

PACS: 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/24/2/020304

1. Introduction

Quantum information science is an emerging research field that provides various protocols for secure communication and efficient computation beyond the capabilities of its classical counterparts. Quantum communication deals with the problem of transferring quantum bits (qubits).[1–3] It has potential applications in quantum networks, in which an unknown qubit can be transmitted directly from one node to another. However, due to the inevitable interaction of the qubits with the environment, direct transmission is not practicable for long-distance quantum communication. The most common method to transfer qubits is quantum teleportation,[4] where pre-shared entangled particle pairs are exploited to deliver qubits, which is suitable for transmission over any distance. In this paper, quantum teleportation is adopted to transfer qubits.

Existing research[5–10] on complicated quantum communication networks is based on the maximally entangled states, ignoring the influence of long-distance quantum channel on maximally entangled states, such as the decoherence effect. However, in real world implementations, some decoherence mechanisms can take maximally entangled states to partially entangled states or mixed states. However, the latter has not been dealt with in their studies. We thus focus with great interest on quantum communication with partially entangled states.

In recent years, many efforts have been devoted to the research of quantum information processing with partially entangled states.[11–17] However, little has been done in the study of transferring qubits in a quantum network with partially entangled states. To the best of our knowledge, a quantum communication network with partially entangled pairs was first analyzed by Yu X T, Zhang Z C and Xu J[18] (we shorten this to the YZX protocol below), whose research was based on a distributed wireless quantum communication network model and who proposed a quantum routing mechanism. Their work shows that multi-hop teleportation in distributed wireless quantum networks with partially entangled states is feasible.

The increasing amount of research available in quantum information science makes a global quantum communication network desirable. Taking technological feasibility into account, it is necessary to investigate quantum communication for wide-area networks with partially entangled states. However, directly applying the YZX protocol[18] to quantum wide-area networks achieves a low probability of successfully transferring a qubit; moreover, security and privacy cannot be guaranteed. Therefore, in this paper we further explore how to perform quantum network tasks efficiently by utilizing partially entangled states. One of our goals is to increase the probability of successfully transferring a qubit and at the same time achieve a high level of security.

This paper represents an efficient quantum communication scheme enabling qubits transmission between any two nodes in a satellite-to-ground quantum network with partially

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61072067 and 61372076), the 111 Project (Grant No. B08038), the Fund from the State Key Laboratory of Integrated Services Networks (Grant No. ISN 1001004), and the Fundamental Research Funds for the Central Universities (Grant Nos. K5051301059 and K5051201021).

†Corresponding author. E-mail: na_chen@outlook.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

entangled states. Here, partially entangled states are directly used without any entanglement distillation strategies.[19,20] In our scheme, the source node performs quantum teleportation only after the end-to-end entangled state has been set up between itself and the destination node. In addition, local operations to reconstruct the transmitted qubit are only needed at the destination node. Together, these guarantee the security of communication. And most of all, with the aid of an auxiliary qubit and specially defined unitary matrices, the probability of successfully transferring a qubit is significantly increased, which is demonstrated by detailed calculations and simulations. Classical information necessary for transferring qubits is transmitted through well-developed classical wireless networks. The results of this paper provide a valuable reference for convergence of the quantum and classical networks.

The rest of this paper is organized as follows. In Section 2, general concepts about entanglement swapping with partially entangled states are introduced. Section 3 describes a system model for satellite-to-ground quantum communication network. In Section 4, qubits transmission in the proposed satellite-to-ground quantum communication network is investigated in detail. Performance evaluation and simulation analyses are presented in Section 5. Finally, some conclusions are drawn in Section 6.

2. Entanglement swapping with partially entangled states

In this section, we introduce the basic idea of entanglement swapping with partially entangled states. Prior to which, some notations and preliminaries used throughout this paper are briefly described.

The Bell states that are used in quantum communication are generally defined as[2]

$$\begin{aligned}|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle),\\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle).\end{aligned} \tag{1}$$

They can be transformed into each other through unitary operations defined by Pauli matrices, such as

$$\begin{aligned}|\Phi^+\rangle &= I\otimes\sigma_x|\Psi^+\rangle\\ &= I\otimes \mathrm{i}\sigma_y|\Psi^-\rangle\\ &= I\otimes\sigma_z|\Phi^-\rangle,\end{aligned} \tag{2}$$

where $\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_y=\begin{pmatrix}0&-\mathrm{i}\\ \mathrm{i}&0\end{pmatrix}$, $\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ are Pauli matrices and $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ is the identity matrix.

A maximally entangled state, without loss of generality, which is denoted as $|\Phi^+\rangle$, may degrade with decoherence induced by the quantum channel to

$$|\Phi_a^+\rangle=\frac{1}{\sqrt{1+a^2}}|00\rangle+\frac{a}{\sqrt{1+a^2}}|11\rangle, \tag{3}$$

where $0\le a\le 1$. When $a=0$, there is no entanglement, while for $a=1$, equation (3) denotes a maximally entangled state. $|0\rangle$ and $|1\rangle$ represent the horizontal and vertical polarizations, respectively. We illustrate the entanglement degree of $|\Phi_a^+\rangle$ in Fig. 1 as functions of entanglement indicator a, which is consistent with the description of entanglement presented by Schlienz and Mahler.[21]

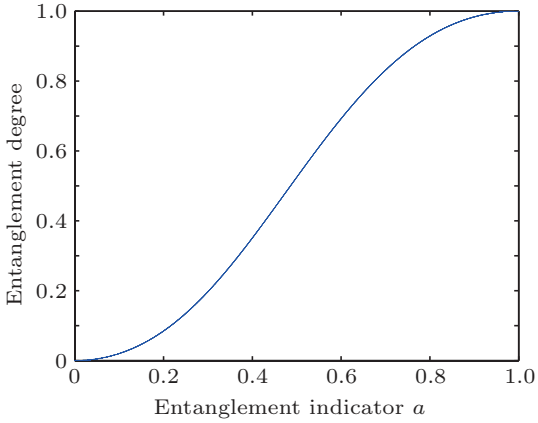


Fig. 1. (color online) Entanglement degree as a function of the entanglement indicator a.

Here, let us consider the simplest case of two pairs of particles 1, 2 and 3, 4 that are initially in partially entangled states described by

$$\begin{aligned}|\Phi_a^+\rangle_{12}&=\frac{1}{\sqrt{1+a^2}}|00\rangle_{12}+\frac{a}{\sqrt{1+a^2}}|11\rangle_{12},\\ |\Phi_a^+\rangle_{34}&=\frac{1}{\sqrt{1+a^2}}|00\rangle_{34}+\frac{a}{\sqrt{1+a^2}}|11\rangle_{34},\end{aligned} \tag{4}$$

where particles 2 and 3 are in the same laboratory, particle 1 and particle 4 are in another two different laboratories. Three laboratories are spatially remote from each other. Entanglement swapping can readily be written as

$$\begin{aligned}&|\Phi_a^+\rangle_{12}\otimes|\Phi_a^+\rangle_{34}\\ &=\frac{\sqrt{1+a^4}}{\sqrt{2}(1+a^2)}(|00\rangle_{23}\otimes|\Phi_{a^2}^+\rangle_{14}+|10\rangle_{23}\otimes|\Phi_{a^2}^-\rangle_{14})\\ &\quad+\frac{a}{1+a^2}(|01\rangle_{23}\otimes|\Psi^+\rangle_{14}+|11\rangle_{23}\otimes|\Psi^-\rangle_{14}),\end{aligned} \tag{5}$$

where

$$|\Phi_{a^2}^\pm\rangle_{14}=\frac{1}{\sqrt{1+a^4}}|00\rangle_{14}\pm\frac{a^2}{\sqrt{1+a^4}}|11\rangle_{14}. \tag{6}$$

From Eq. (5) we can see that when particles 2 and 3 are projected onto one of the basis states $\{|01\rangle,|11\rangle\}$, the particle pair

1, 4 is projected accordingly onto one of the Bell states $|\Psi^{\pm}\rangle_{14}$ with probability $a^2/(1+a^2)^2$. Otherwise, when particles 2 and 3 are projected onto one of the basis states $\{|00\rangle, |10\rangle\}$, the particle pair 1, 4 is projected as well onto one of the partially entangled states $|\Phi^{\pm}_{a^2}\rangle_{14}$ with probability $(1+a^4)/2(1+a^2)^2$. When $a = 1$, the above discussion corresponds to entanglement swapping with maximally entangled states.

3. Network model

Considering that satellites provide a unique solution for distributing entangled quantum pairs in a wide-area quantum network, a satellite-to-ground quantum communication network is constructed thereby. As shown in Fig. 2, it is composed of a global position database (GPD), satellite-borne EPR generators and several metropolitan area networks. Each metropolitan area network is equipped with a powerful, high-reliability satellite ground station (SGS) and several standby devices. These SGSs constitute the interface between quantum communication terminals and the backbone network system. The main function of an SGS is to manage the quantum entangled states shared between itself and the quantum communication terminals that are inside its service area. When a quantum communication terminal inside an SGS's service area sends or receives qubits, then the SGS functions as an intermediate node. Each SGS can provide communication services for multiple terminals at the same time using the identity authentication mechanism. In addition, each SGS is equipped with multiple radio transceivers, which are responsible for sending and receiving classical information over classical wireless channels.

A two-tier database structure is adopted in the network. Each SGS is equipped with a local position database (LPD) to manage the information of quantum communication terminals inside its service area. An LPD can also be used to determine whether or not a specific quantum communication terminal is inside this metropolitan area. Moreover, a GPD exists in the backbone network to record the position information of all quantum communication terminals in the satellite-to-ground quantum communication network. By inquiring the GPD, one can ascertain which metropolitan area a specific quantum communication terminal resides in.

In the network shown in Fig. 2, the satellite-borne EPR generators are responsible for generating and distributing EPR pairs. Once two SGSs need to establish quantum entangled states, the specified satellite-borne EPR generator would distribute the generated EPR pairs, which are uniformly described as $|\Phi^+\rangle$ in our scheme, through quantum channels. Due to the decoherence induced by quantum channels, these two SGSs possibly share various partially entangled states with different entanglement degrees, sometimes even mixed states. But in this paper, we consider the simplest situation where two involved SGSs share a partially entangled state $|\Phi^+_a\rangle$, which is consistent with the preconditions of existing publications.[13,14,18]

There are two kinds of communication channels for qubits transmission. Optical free-space links are generally employed as a quantum channel since they theoretically allow a much longer propagation distance for the photons due to the low absorption of the atmosphere in certain wavelength ranges. Classical data are transmitted through classical wireless channels. In Fig. 2, the dashed and solid lines represent quantum and classical wireless channels, respectively. SGSs access the GPD though classical channels, which are not depicted in Fig. 2 for simplicity.

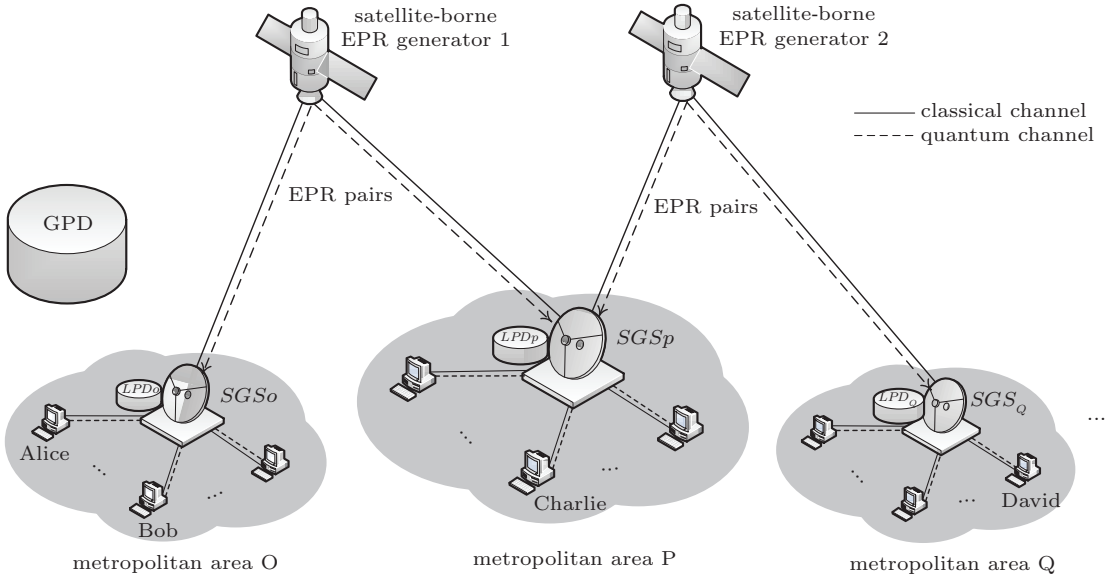


Fig. 2. (color online) Structure of satellite-to-ground quantum communication network.

Quantum communication terminals are quantum devices with wireless communication capabilities, they can store and process quantum information.

4. Quantum communication scheme

In the present quantum communication scheme the classical information necessary for delivering qubits is transmitted over well-developed classical wireless networks with various routing schemes.[22,23] In order to maximize the probability of successfully transferring a qubit, the quantum path with minimum hops will be selected by referring to previous proposed quantum routing algorithms.[5,8,10,18] The concrete rules of routing are not discussed in this paper.

Before discussing specific communication scenarios, we might as well make the following assumptions. Suppose that the target qubit to be transmitted is $|\phi\rangle_X = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. To simplify our discussion, we assume that each quantum communication terminal shares in advance enough partially entangled states, which are uniformly described as $|\Phi_a^+\rangle$, with the SGS that serves it.

In the satellite-to-ground quantum communication network described in Section 3, we consider a circumstance in which a quantum terminal called Alice intends to transfer a qubit to another terminal (the destination node). Firstly, Alice requests the SGS that serves it, i.e. SGS_O, to establish communication to the destination node. Then, SGS_O would query its own LPD, i.e. LPD_O, to determine whether or not the destination node is inside metropolitan area O. Accordingly, we will discuss in detail the following two communication scenarios.

Scenario 1 Alice would like to transfer a qubit to the destination node called Bob, as shown in Fig. 2.

According to previous assumptions, Bob also shares partially entangled states $|\Phi_a^+\rangle$ with SGS_O. After applying an appropriate quantum routing protocol, Alice $\rightarrow SGS_O \rightarrow$ Bob is assumed to be the selected quantum path. As the unique intermediate node, SGS_O will implement entanglement swapping with two partially entangled states $|\Phi_a^+\rangle_{AO_1}$ and $|\Phi_a^+\rangle_{BO_2}$, similarly described by Eq. (5). Here subscripts O_1 and O_2 stand for SGS_O's first and second particles, respectively, A presents Alice's particle, and B corresponds to Bob's. After entanglement swapping, SGS_O will send the measurement result represented by 2 bits of classical information to Bob. Then Bob performs a proper unitary operation related to the received measurement result on his qubit. In Table 1, four types of unitary operations are listed, corresponding to different entanglement swapping measurement results. For example, if SGS_O's measurement result is $|01\rangle$, then Bob will perform σ_x on his qubit, and then the entangled state shared between himself and Alice will be $|\Phi^+\rangle_{AB}$. According to Eq. (5) and Table 1, we can see that after Bob's unitary operation, the end-to-end entangled state shared between Alice and Bob will be $|\Phi_{a^2}^+\rangle_{AB}$ with probability $(1+a^4)/(1+a^2)^2$, or $|\Phi^+\rangle_{AB}$ with probability $(2a^2)/(1+a^2)^2$. After receiving the notification from Bob that the end-to-end entangled state is ready, Alice transfers the target qubit $|\phi\rangle_X$ by quantum teleportation. The following two cases correspond to the two possible end-to-end entangled states shared between Alice and Bob.

Table 1. Relation between entanglement swapping measurement results received and local unitary operations.

Measurement results	Unitary operations
$\|00\rangle$	I
$\|01\rangle$	σ_x
$\|10\rangle$	σ_z
$\|11\rangle$	$\mathrm{i}\sigma_y$

(i) The end-to-end entangled state shared between Alice and Bob is $|\Phi_{a^2}^+\rangle_{AB}$.

The state of the entire system before teleportation is represented by $|\phi\rangle_X \otimes |\Phi_{a^2}^+\rangle_{AB}$. Alice performs Bell-state measurements on particles X and A, which can be written as

$$\begin{aligned}
&|\text{total}\rangle_{XAB} \\
&= |\phi\rangle_X \otimes |\Phi_{a^2}^+\rangle_{AB} \\
&= (\alpha|0\rangle_X + \beta|1\rangle_X) \otimes \left(\frac{1}{\sqrt{1+a^4}}|00\rangle_{AB} + \frac{a^2}{\sqrt{1+a^4}}|11\rangle_{AB}\right) \\
&= \sqrt{\frac{|\alpha|^2 + a^4|\beta|^2}{2(1+a^4)}}(|\Phi^+\rangle_{XA} \otimes |\phi_1\rangle_B + |\Phi^-\rangle_{XA} \otimes |\phi_2\rangle_B) \\
&\quad + \sqrt{\frac{a^4|\alpha|^2 + |\beta|^2}{2(1+a^4)}}(|\Psi^+\rangle_{XA} \otimes |\phi_3\rangle_B \\
&\quad + |\Psi^-\rangle_{XA} \otimes |\phi_4\rangle_B). \qquad (7)
\end{aligned}$$

At the same time, the state of particle B with Bob turns into one of the following four possibilities

$$\begin{aligned}
|\phi_1\rangle_B &= \frac{\alpha|0\rangle_B + a^2\beta|1\rangle_B}{\sqrt{|\alpha|^2 + a^4|\beta|^2}}, \\
|\phi_2\rangle_B &= \frac{\alpha|0\rangle_B - a^2\beta|1\rangle_B}{\sqrt{|\alpha|^2 + a^4|\beta|^2}}, \\
|\phi_3\rangle_B &= \frac{\beta|0\rangle_B + a^2\alpha|1\rangle_B}{\sqrt{a^4|\alpha|^2 + |\beta|^2}}, \\
|\phi_4\rangle_B &= \frac{-\beta|0\rangle_B + a^2\alpha|1\rangle_B}{\sqrt{a^4|\alpha|^2 + |\beta|^2}}. \qquad (8)
\end{aligned}$$

It can be seen from Eqs. (7) and (8) that particles X and A are projected onto one of the four Bell states and accordingly particle B is projected onto a state which is related to the original state of particle X. Then Alice informs Bob about her measurement results (2 bits of classical information). According to Alice's Bell-state measurement result, Bob performs a proper unitary operation on particle B, as shown in Table 2. After unitary operation, Bob's qubit evolves as follows:

$$|\phi_1\rangle_B \xrightarrow{I} |\varphi_1\rangle_B = \frac{\alpha|0\rangle_B + a^2\beta|1\rangle_B}{\sqrt{|\alpha|^2 + a^4|\beta|^2}},$$

$$
\begin{aligned}
|\phi_2\rangle_B \xrightarrow{\sigma_z} |\varphi_2\rangle_B &= \frac{\alpha|0\rangle_B+a^2\beta|1\rangle_B}{\sqrt{|\alpha|^2+a^4|\beta|^2}},\\
|\phi_3\rangle_B \xrightarrow{\sigma_x} |\varphi_3\rangle_B &= \frac{a^2\alpha|0\rangle_B+\beta|1\rangle_B}{\sqrt{a^4|\alpha|^2+|\beta|^2}},\\
|\phi_4\rangle_B \xrightarrow{i\sigma_y} |\varphi_4\rangle_B &= \frac{a^2\alpha|0\rangle_B+\beta|1\rangle_B}{\sqrt{a^4|\alpha|^2+|\beta|^2}}.
\end{aligned} \tag{9}
$$

From Eq. (9), we see obviously $|\varphi_1\rangle_B = |\varphi_2\rangle_B, |\varphi_3\rangle_B = |\varphi_4\rangle_B$.

Table 2. Relation between Alice's Bell-state measurement results and local unitary operations.

Measurement results	Unitary operations
$\|\Phi^+\rangle_{XA}$	I
$\|\Phi^-\rangle_{XA}$	σ_z
$\|\Psi^+\rangle_{XA}$	σ_x
$\|\Psi^-\rangle_{XA}$	$\mathrm{i}\sigma_y$

In order to recover the target qubit $|\phi\rangle_X$, Bob prepares an auxiliary qubit, which is initially described by $|0\rangle_{\rm aux}$. If Alice's measurement result is $|\Phi^+\rangle_{XA}$ or $|\Phi^-\rangle_{XA}$, then Bob will implement unitary matrix

$$
U_{B1}^{(1)} = \begin{pmatrix} a^2 & \sqrt{1-a^4} & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ \sqrt{1-a^4} & -a^2 & 0 & 0 \end{pmatrix} \tag{10}
$$

on $|\varphi_1\rangle_B|0\rangle_{\rm aux}$ or $|\varphi_2\rangle_B|0\rangle_{\rm aux}$, reads

$$
\begin{aligned}
&U_{B1}^{(1)}|\varphi_1\rangle_B|0\rangle_{\rm aux}\\
&= U_{B1}^{(1)}|\varphi_2\rangle_B|0\rangle_{\rm aux}\\
&= \frac{a^2}{\sqrt{|\alpha|^2+a^4|\beta|^2}}(\alpha|0\rangle_B+\beta|1\rangle_B)\otimes|0\rangle_{\rm aux}\\
&\quad+\sqrt{\frac{1-a^4}{|\alpha|^2+a^4|\beta|^2}}\alpha|1\rangle_B\otimes|1\rangle_{\rm aux}.
\end{aligned} \tag{11}
$$

From Eq. (11), it can be seen that if Bob projects the auxiliary qubit onto the basis $\{|0\rangle,|1\rangle\}$ and he obtains $|0\rangle_{\rm aux}$, then his particle B definitely collapses to the target qubit $|\phi\rangle_X$, thereby qubit transmission is successful. Otherwise, if he gets $|1\rangle_{\rm aux}$, no information about $|\phi\rangle_X$ is obtained and the transmission fails. Apparently, the state of auxiliary qubit indicates whether or not the qubit transmission is successful, which is a heralded mechanism.

In another case, when Alice's measurement result is $|\Psi^+\rangle_{XA}$ or $|\Psi^-\rangle_{XA}$, Bob implements unitary matrix

$$
U_{B2}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & \sqrt{1-a^4} & a^2 & 0\\ 0 & -a^2 & \sqrt{1-a^4} & 0 \end{pmatrix} \tag{12}
$$

on $|\varphi_3\rangle_B|0\rangle_{\rm aux}$ and $|\varphi_4\rangle_B|0\rangle_{\rm aux}$, reads

$$
\begin{aligned}
&U_{B2}^{(1)}|\varphi_3\rangle_B|0\rangle_{\rm aux}\\
&= U_{B2}^{(1)}|\varphi_4\rangle_B|0\rangle_{\rm aux}\\
&= \frac{a^2}{\sqrt{a^4|\alpha|^2+|\beta|^2}}(\alpha|0\rangle_B+\beta|1\rangle_B)\otimes|0\rangle_{\rm aux}\\
&\quad+\sqrt{\frac{1-a^4}{a^4|\alpha|^2+|\beta|^2}}\beta|1\rangle_B\otimes|1\rangle_{\rm aux}.
\end{aligned} \tag{13}
$$

After projecting the auxiliary qubit onto basis $\{|0\rangle,|1\rangle\}$, qubit transmission is successful only when Bob obtains $|0\rangle_{\rm aux}$. In the same way, the state of auxiliary qubit shows if the qubit transmission is successful.

Based on the above analyses, when Alice and Bob share $|\Phi_{a^2}^+\rangle_{AB}$, the probability of successfully transferring the target qubit $|\phi\rangle_X$ is given by

$$
\begin{aligned}
P_{\rm suc}^{(1)} &= (P_{\Phi^+}+P_{\Phi^-})\times P_{|0\rangle_{\rm aux}}+(P_{\Psi^+}+P_{\Psi^-})\times P'_{|0\rangle_{\rm aux}}\\
&= 2\left(\sqrt{\frac{|\alpha|^2+a^4|\beta|^2}{2(1+a^4)}}\right)^2\left(\frac{a^2}{\sqrt{|\alpha|^2+a^4|\beta|^2}}\right)^2\\
&\quad+2\left(\sqrt{\frac{a^4|\alpha|^2+|\beta|^2}{2(1+a^4)}}\right)^2\left(\frac{a^2}{\sqrt{a^4|\alpha|^2+|\beta|^2}}\right)^2\\
&= \frac{2a^4}{1+a^4},
\end{aligned} \tag{14}
$$

where, based on Eqs. (7), (11), and (13), we make the following denotations

$$
\begin{aligned}
P_{\Phi^+} = P_{\Phi^-} &= \left(\sqrt{\frac{|\alpha|^2+a^4|\beta|^2}{2(1+a^4)}}\right)^2,\\
P_{\Psi^+} = P_{\Psi^-} &= \left(\sqrt{\frac{a^4|\alpha|^2+|\beta|^2}{2(1+a^4)}}\right)^2,\\
P_{|0\rangle_{\rm aux}} &= \left(\frac{a^2}{\sqrt{|\alpha|^2+a^4|\beta|^2}}\right)^2,\\
P'_{|0\rangle_{\rm aux}} &= \left(\frac{a^2}{\sqrt{a^4|\alpha|^2+|\beta|^2}}\right)^2.
\end{aligned}
$$

(ii) The end-to-end entangled state shared between Alice and Bob is $|\Phi^+\rangle_{AB}$.

This case corresponds to teleportation with a maximally entangled state, which is a deterministic protocol. Hence, the probability of successfully transferring the target qubit $|\phi\rangle_X$ is 1, that is $P_{\rm suc}^{(2)}=1$.

From the above discussion we can see that in Scenario 1 the probability of successfully transferring a qubit from Alice to Bob reads

$$
P_1 = \frac{1+a^4}{(1+a^2)^2}\times P_{\rm suc}^{(1)}+\frac{2a^2}{(1+a^2)^2}\times P_{\rm suc}^{(2)}
$$

$$= \frac{2a^2}{1+a^2}. \tag{15}$$

Scenario 2 Alice would like to transfer a qubit to the destination node called Charlie, as shown in Fig. 2.

After querying LPD_O, SGS_O learns that Charlie is not inside metropolitan area O, it then proceeds to inquire the GPD to determine which metropolitan area Charlie resides in. The GPD will respond to SGS_O that Charlie is inside metropolitan area P. After applying a quantum routing protocol, each involved node will be informed that the selected quantum path is Alice $\rightarrow SGS_O \rightarrow SGS_P \rightarrow$ Charlie. Then SGS_O asks the satellite-borne EPR generator 1 to set up an entangled state between SGS_O and SGS_P. Afterwards, the satellite-borne EPR generator 1 will distribute an EPR pair $|\Phi^+\rangle$ by sending one particle of it to SGS_O and sending the other particle to SGS_P. Due to the decoherence effect induced by the quantum channel, SGS_O and SGS_P finally share a partially entangled state denoted as

$$|\Phi_a^+\rangle_{O_2P_1} = \frac{1}{\sqrt{1+a^2}}|00\rangle_{O_2P_1} + \frac{a}{\sqrt{1+a^2}}|11\rangle_{O_2P_1}.$$

After SGS_O's entanglement swapping, as similarly expressed by Eq. (5), and SGS_P's unitary operations, according to Table 1, the possible entangled states shared between Alice and SGS_P can be expressed as follows:

$$\begin{aligned}
&|\Phi^+\rangle_{AP_1} = \frac{1}{\sqrt{2}}(|00\rangle_{AP_1} + |11\rangle_{AP_1}),\\
&P_{AP_1}^{(1)} = \frac{2a^2}{(1+a^2)^2},\\
&|\Phi_{a^2}^+\rangle_{AP_1} = \frac{1}{\sqrt{1+a^4}}|00\rangle_{AP_1} + \frac{a^2}{\sqrt{1+a^4}}|11\rangle_{AP_1},\\
&P_{AP_1}^{(2)} = \frac{1+a^4}{(1+a^2)^2}.
\end{aligned} \tag{16}$$

Then, after SGS_P's entanglement swapping and Charlie's unitary operations, the possible end-to-end entangled states shared between Alice and Charlie and corresponding probabilities are given by the first column in Table 3. Upon receiving the notification from Charlie that the end-to-end entangled state is ready, Alice will transfer the target qubit $|\phi\rangle_X$ by quantum teleportation. Analogous to the analyses in Scenario 1, the critical ingredients referring to the follow-up target qubit recovery in quantum teleportation are listed in Table 3. When performing quantum teleportation, Alice's possible measurement results for particles X and A are described by the second column. The third column represents Charlie's unitary operations implemented on $|\varphi\rangle_C|0\rangle_{\text{aux}}$ to recover the target qubit, and the last column in Table 3 shows the probabilities of successful teleportation.

Table 3. Possible end-to-end entangled states shared between Alice and Charlie, and the follow-up target qubit recovery operations in Scenario 2.

Possible end-to-end entangled states	Alice's measurement results	Charlie's unitary matrices	Success probability
$\|\Phi_a^+\rangle_{AC} = \frac{1}{\sqrt{1+a^2}}\|00\rangle_{AC} + \frac{a}{\sqrt{1+a^2}}\|11\rangle_{AC}$	$\|\Phi^+\rangle_{XA}$ or $\|\Phi^-\rangle_{XA}$	$U_{C1}^{(1)}$	$P_{\text{suc}}^{(1)} = \frac{2a^2}{1+a^2}$
$P_{AC}^{(1)} = \frac{2a^2}{(1+a^2)^2}$	$\|\Psi^+\rangle_{XA}$ or $\|\Psi^-\rangle_{XA}$	$U_{C2}^{(1)}$	
$\|\Phi_a^{+'}\rangle_{AC} = \frac{a}{\sqrt{1+a^2}}\|00\rangle_{AC} + \frac{1}{\sqrt{1+a^2}}\|11\rangle_{AC}$	$\|\Phi^+\rangle_{XA}$ or $\|\Phi^-\rangle_{XA}$	$U_{C1}^{(2)} = U_{C2}^{(1)}$	$P_{\text{suc}}^{(2)} = \frac{2a^2}{1+a^2}$
$P_{AC}^{(2)} = \frac{a^2}{(1+a^2)^2}$	$\|\Psi^+\rangle_{XA}$ or $\|\Psi^-\rangle_{XA}$	$U_{C2}^{(2)} = U_{C1}^{(1)}$	
$\|\Phi_{a^3}^+\rangle_{AC} = \frac{1}{\sqrt{1+a^6}}\|00\rangle_{AC} + \frac{a^3}{\sqrt{1+a^6}}\|11\rangle_{AC}$	$\|\Phi^+\rangle_{XA}$ or $\|\Phi^-\rangle_{XA}$	$U_{C1}^{(3)}$	$P_{\text{suc}}^{(3)} = \frac{2a^6}{1+a^6}$
$P_{AC}^{(3)} = \frac{a^4-a^2+1}{(1+a^2)^2}$	$\|\Psi^+\rangle_{XA}$ or $\|\Psi^-\rangle_{XA}$	$U_{C2}^{(3)}$	

where,

$$U_{C1}^{(1)} = \begin{pmatrix} a & \sqrt{1-a^2} & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ \sqrt{1-a^2} & -a & 0 & 0 \end{pmatrix},$$

$$U_{C2}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & \sqrt{1-a^2} & a & 0\\ 0 & -a & \sqrt{1-a^2} & 0 \end{pmatrix},$$

$$U_{C1}^{(3)} = \begin{pmatrix} a^3 & \sqrt{1-a^6} & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ \sqrt{1-a^6} & -a^3 & 0 & 0 \end{pmatrix},$$

$$U_{C2}^{(3)} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & \sqrt{1-a^6} & a^3 & 0\\ 0 & -a^3 & \sqrt{1-a^6} & 0 \end{pmatrix}. \tag{17}$$

In Scenario 2, the probability of successfully transferring

a qubit from Alice to Charlie reads

$$P_2 = P_{AC}^{(1)} \times P_{\text{suc}}^{(1)} + P_{AC}^{(2)} \times P_{\text{suc}}^{(2)} + P_{AC}^{(3)} \times P_{\text{suc}}^{(3)} = \frac{2a^6+6a^4}{(1+a^2)^3}. \quad (18)$$

If the destination node is farther apart from the source node, then many more satellite-borne EPR generators are needed. For example, Alice would like to transfer a qubit to David, as shown in Fig. 2. By successively inquiring LPD_O and the GPD, SGS_O learns that David is inside the metropolitan area Q. After applying a quantum routing algorithm, each involved node will be informed that the selected quantum path is Alice $\rightarrow SGS_O \rightarrow SGS_P \rightarrow SGS_Q \rightarrow$ David. Then, SGS_O requests the satellite-borne EPR generator 1 to set up an entangled state between SGS_O and SGS_P. Similarly, at the request of SGS_P, the satellite-borne EPR generator 2 will distribute an EPR pair $|\Phi^+\rangle$ to SGS_P and SGS_Q as well. Due to the decoherence effect, the partially entangled state shared between SGS_O and SGS_P is

$$|\Phi_a^+\rangle_{O_2P_1} = \frac{1}{\sqrt{1+a^2}}|00\rangle_{O_2P_1} + \frac{a}{\sqrt{1+a^2}}|11\rangle_{O_2P_1},$$

similarly SGS_P and SGS_Q share

$$|\Phi_a^+\rangle_{P_2Q_1} = \frac{1}{\sqrt{1+a^2}}|00\rangle_{P_2Q_1} + \frac{a}{\sqrt{1+a^2}}|11\rangle_{P_2Q_1}.$$

After sequential entanglement swapping performed by each intermediate node and proper unitary operations implemented by its next-hop node on the selected quantum path, the end-to-end entangled state shared between Alice and David has been established. At last, Alice transfers the target qubit $|\phi\rangle_X$ by quantum teleportation and David recovers it with the help of the auxiliary qubit and special unitary matrices. Detailed mathematical expressions describing the qubit transmission process are analogous to those mentioned in the two scenarios given above. The probability of successfully transferring a qubit from Alice to David reads

$$P_3 = \frac{2a^6+6a^4}{(1+a^2)^3}. \quad (19)$$

Similar analyses can be applied to quantum communication scenarios involving more nodes. In this way, two geographically distant networks can be connected together. The realization of a worldwide quantum network will be possible with the help of satellites.

5. Performance analysis

In this section, the performance of the satellite-to-ground quantum communication network with partially entangled states is analyzed. Compared with quantum networks[5–10] based on maximally entangled states, the scheme proposed here takes the influence of quantum channel on maximally entangled states into consideration. Therefore, this scheme will be more suitable for practical implementations. Though based on partially entangled states, YZX protocol[18] cannot be applied to the satellite-to-ground quantum communication network described in Section 3 because of its security flaws and the low probability of successfully transferring a qubit. However, neither of these problems exists in our quantum communication scheme.

The principle of the YZX protocol[18] is to perform teleportation hop by hop from the source to its destination. This is based on the idea that a qubit may be transferred successfully if a balanced sequence of $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ is obtained.[14] Assume that the number of nodes on a selected quantum path is N ($N > 3$). It is possible that on a certain intermediate node labelled node n ($n < N$) a balanced sequence of $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ is obtained. In this situation, if node n is compromised, then the target qubit will be exposed. While in our scheme, the quantum teleportation will be performed by the source, so as to transfer the target qubit, only after the end-to-end entangled state has been shared between the source and the destination has been set up. In this way, the communication security is guaranteed.

When YZX protocol[18] is applied to the satellite-to-ground quantum communication network, it gains a low probability of successfully transferring a qubit. However, in our scheme, an auxiliary qubit and special unitary matrices similar to expressions in Eqs. (10), (12), and (17), are utilized by the destination to recover the target qubit. Such ingenious strategies lead to an increase in communication efficiency. In addition, the auxiliary qubit provides a heralded mechanism for successful qubit transmission. The probabilities of successfully transferring a qubit in quantum paths with 3 nodes, 4 nodes, and 5 nodes are given by Eqs. (15), (18), and (19), respectively. Similar to the analyses presented in Section 4, when there are 6 nodes on the selected quantum path, the probability of successfully transferring a qubit is written as

$$P_{6\text{ nodes}} = \frac{2a^{10}+10a^8+20a^6}{(1+a^2)^5}. \quad (20)$$

When 7 nodes exist on the selected quantum path, the success probability reads

$$P_{7\text{ nodes}} = \frac{2a^{10}+10a^8+20a^6}{(1+a^2)^5}. \quad (21)$$

The probabilities of successfully transferring a qubit as discussed above are depicted in Fig. 3. According to the entanglement degree that is shown as Fig. 1, we take entanglement indicators $a = 1$, $a = 0.9$, $a = 0.8$, and $a = 0.6$ as examples. From Fig. 3, first of all we can see that when $a = 1$, the probability of successfully transferring a qubit equals 1, regardless of the number of nodes involved, which coincides with the quantum communication with maximally entangled states. Secondly, for a specific quantum path, with the decrease of entanglement degree, the probability of successfully transferring a qubit is reduced. Furthermore, for a constant

entanglement degree, the probability of successfully transferring a qubit is trending downward along with the increasing number of nodes. But we need not be too concerned about this point because only a small number of satellites are needed to achieve global quantum communication.

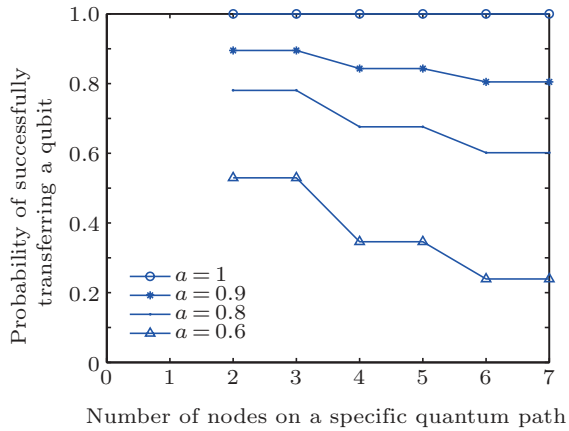


Fig. 3. (color online) Probability of successfully transferring a qubit versus the number of nodes.

In Fig. 4 the blue solid lines represent the probabilities of successfully transferring a qubit in the proposed scheme and the red dashed lines correspond to the success probabilities of YZX protocol.[18] Entanglement indicators $a = 0.9$ and $a = 0.8$ are taken as examples. From the simulation results shown in Fig. 4, it can be seen that when YZX protocol[18] is applied to satellite-to-ground quantum communication network, its efficiency is significantly lower than that of our scheme.

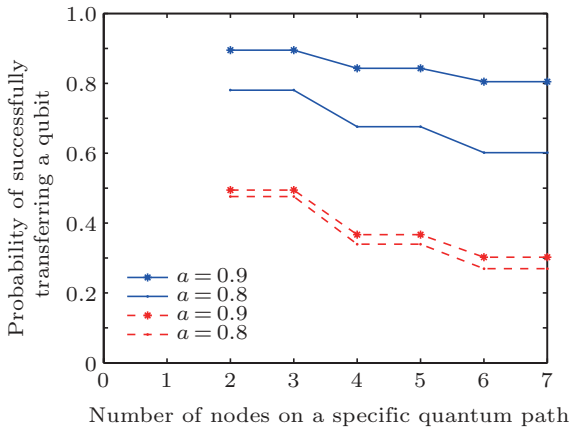


Fig. 4. (color online) Probability of successfully transferring a qubit in two different schemes.

The probability of successfully transferring a qubit on a quantum path with two nodes is also plotted in Figs. 3 and 4, although it is not discussed in the constructed satellite-to-ground quantum communication network. This situation will appear when the proposed scheme is applied to a distributed quantum communication network.

6. Conclusions

In this paper, a satellite-to-ground quantum communication network is constructed and, based on this communication scenario, an efficient and secure quantum communication scheme with partially entangled states is presented. We have solved the problem that the existing method of quantum communication in distributed wireless quantum networks with partially entangled states cannot be applied directly to wide-area quantum networks because of its security flaws and low efficiency. In the proposed scheme, end-to-end entangled states are set up by sequential entanglement swapping with partially entangled states; afterwards, the source node performs teleportation to transfer qubits. In this way the security of the quantum communication is guaranteed. When the destination node recovers the transmitted qubits, the auxiliary qubit and specially defined unitary matrices are utilized. Such ingenious strategies increase the probability of successfully transferring a qubit, which has been shown in detailed calculations and simulation analyses. Moreover, the auxiliary qubit provides a heralded mechanism for successful communication. In the proposed scheme, classical information necessary for qubits transmission is transferred through well-developed classical wireless networks. The results of this paper provide a valuable reference for the convergence of quantum and classical networks.

Considering the time complexity of establishing end-to-end entangled states caused by sequential entanglement swapping, it can be performed from both ends to the middle on a specific quantum path. Thus the communication delay in the proposed scheme will be reduced.

Finally, we would like to emphasize that, for the sake of simple analysis, we have considered an ideal situation in which all of the quantum channels are assumed to possess the same entanglement. But when it comes to more realistic settings this precondition is difficult to fulfill and various changes to the quantum channels will occur; for example, decoherence possibly leads to mixed state channels. Currently, no research on teleportation and entanglement swapping with various entanglement is yet available. Actually, we have tested some channels with different entanglements and obtained no better performance. We are now devoting ourselves to a generalized wide-area quantum communication network in which irregular entangled states, imperfect measurements, and imperfect unitary operations are taken into consideration.

References

[1] Wootters W and Zurek W 1982 *Nature* **299** 802
[2] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[3] Chen P, Long G L and Deng F G 2006 *Chin. Phys.* **15** 2228
[4] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wooters W K 1993 *Phys. Rev. Lett.* **70** 1895
[5] Cheng S T, Wang C Y and Tao M H 2005 *IEEE J. Sel. Area Comm.* **23** 1424

[6] Zhou N R, Zeng G H, Zhu F C and Liu S Q 2006 *J. Shanghai Jiaotong University* **40** 1885 (in Chinese)
[7] Bacinoglu T, Glubahar B and Akan O B 2010 *Proceedings of IEEE Global Communications Conference*, December 6–10, 2010, Miami, USA, p. 1
[8] Yu X T, Xu J and Zhang Z C 2012 *Acta Phys. Sin.* **61** 220303 (in Chinese)
[9] Wang K, Yu X T, Lu S L and Gong Y X 2014 *Phys. Rev. A* **89** 022329
[10] Yu X T, Xu J and Zhang Z C 2013 *Chin. Phys. B* **22** 090311
[11] Li W L, Li C F and Guo G C 2000 *Phys. Rev. A* **61** 034301
[12] Agrawal P and Pati A K 2002 *Phys. Lett. A* **305** 12
[13] Modlawska J and Grudka A 2008 *Phys. Rev. Lett.* **100** 110503
[14] Rigolin G 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 235504
[15] Wang M Y and Yan F L 2009 *Eur. Phys. J. D* **54** 111
[16] Gordon G and Rigolin G 2010 *Opt. Commun.* **283** 184
[17] Sheng Y B, Zhou L, Zhao S M and Zheng B Y 2012 *Phys. Rev. A* **85** 012307
[18] Yu X T, Zhang Z C and Xu J 2014 *Chin. Phys. B* **23** 010303
[19] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett* **76** 722
[20] Chen P X, Liang L M, Li C Z and Huang M Q 2002 *Phys. Rev. A* **66** 022309
[21] Schlienz J and Mahler G 1995 *Phys. Rev. A* **52** 4396
[22] Perkins C E and Royer E M 1999 *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications* (*IEEE*)
[23] Yang D N and Liao W J 2008 *IEEE T Veh. Technol.* **57** 2560