Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2017, 10, 7-18
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Quantum Secret Broadcast for Wireless Quantum Networks

Tao Shang, Gang Du, Jianwei Liu

School of Electronic and Information Engineering, Beihang University, Beijing, China
Email: shangtao@buaa.edu.cn

How to cite this paper: Shang, T., Du, G. and Liu, J.W. (2017) Quantum Secret Broadcast for Wireless Quantum Networks. *Int. J. Communications, Network and System Sciences*, **10**, 7-18.
https://doi.org/10.4236/ijcns.2017.108B002

Received: March 10, 2017
Accepted: August 11, 2017
Published: August 14, 2017

Abstract

In wireless quantum networks, nodes communicate by means of pre-distribution for entangled pairs and relay path establishment for quantum teleportation. However, simple point-to-point communication seriously restricts the efficiency of quantum communication. Inspired by sharing idea of quantum secret sharing (QSS), which is based on three collaborative nodes with pre-shared GHZ (Greenberger-Horne-Zeilinger) states, we propose a quantum secret broadcast scheme to improve network performance. In a cluster network cored on three parties of QSS, three cluster heads with pre-shared GHZ states are senders, while cluster members are receivers. One cluster head encodes secret messages on auxiliary particles by performing certain operations on them with GHZ particles, then three cluster heads measure their own particles and broadcast measurement results honestly. Based on the specific correlation of measurement results and secret messages, all receivers can recover the secret messages. Furthermore, to prevent eavesdropping, cluster heads can update an encoding key periodically. Analysis shows the proposed scheme is more efficient than previous schemes in wireless quantum networks, especially when the number of receivers is larger. Besides, in the proposed scheme, attacks on quantum channel based on GHZ state can be detected, and eavesdroppers cannot recover messages correctly for lack of suitable decoding key.

Keywords

Quantum Secret Sharing, Quantum Secret Broadcast, Cluster Network

1. Introduction

Since the first quantum key distribution (QKD) protocol BB84 [1] was proposed, quantum communication has attracted much attention in the filed of information security. In order to meet the demand of adaptive quantum communication, quantum communication in the area of wireless network has been exploited. Cheng *et al.* [2] made the first attempt in wireless quantum networks (WQN) and proposed a quantum routing mechanism, which allows teleporting a quantum state from a node to another node. Li *et al.* [3] designed a framework for distributed wireless quantum networks. In 2013, Cao *et al.* [4] applied a cluster mesh structure and addressed the problems of EPR resources and quantum channel establishment. The above researches gradually enhance the feasibility of wireless quantum networks. However, there are still a problem in WQN, that is inefficient, *i.e.*, a source node will consume relay nodes' resources , and it can only send a message to one destination node once instead of several nodes.

Quantum secret sharing (QSS) is an important branch of quantum cryptography, which is a generalization of the classical secret sharing into the quantum domain. Since the first QSS protocol was presented by Hillery *et al.* [5], various QSS schemes have been proposed [6] [7] [8] [9]. In a typical three-party QSS scheme [8], a sender, Alice, splits a secret message into two shares and distributes the shares to two receivers, Bob and Charlie, so that none of them can recover the secret from their own shares. Only if Bob and Charlie publish their own measurement results honestly, can they read out the secret message correctly.

Inspired by the feature of QSS that more than one party can receive secret message each time, we introduce the idea of QSS into a wireless quantum network, and propose a quantum secret broadcast scheme to solve the troubling efficiency problem. In a cluster network cored on three parties of QSS, three cluster heads, Alice, Bob, and Charlie will collaborate honestly to broadcast messages to cluster members by using pre-shared GHZ states. The communication mode can be whole-network broadcast or intra-cluster broadcast. Furthermore, to prevent illegal eavesdropping, three cluster heads will periodically update a encoding key Y. Consequently, illegal nodes cannot read out the message correctly for lack of suitable decoding key.

2. Related Works

2.1. Wireless Quantum Networks

Wireless quantum networks (WQN) has been studied by many groups [2] [3] [4] [10] to exploit quantum communication into the area of wireless network. The basic method of communication between nodes in WQN is quantum teleportation. **Figure 1** shows an example of wireless quantum network, where dotted line represents quantum channel based on EPR pairs. We assume node A is a source node and node E is a destination node. A possible routing path is $A \rightarrow C \rightarrow D \rightarrow E$, which means the relay node C and D will also consume their EPR pairs and classical bits to assist this communication.

Although WQN has been explored further in the aspects of EPR-pair allocation [3], routing optimization, network architecture construction [4] [10], and so on, the basic issues of the WQN are still EPR-pair distribution and quantum

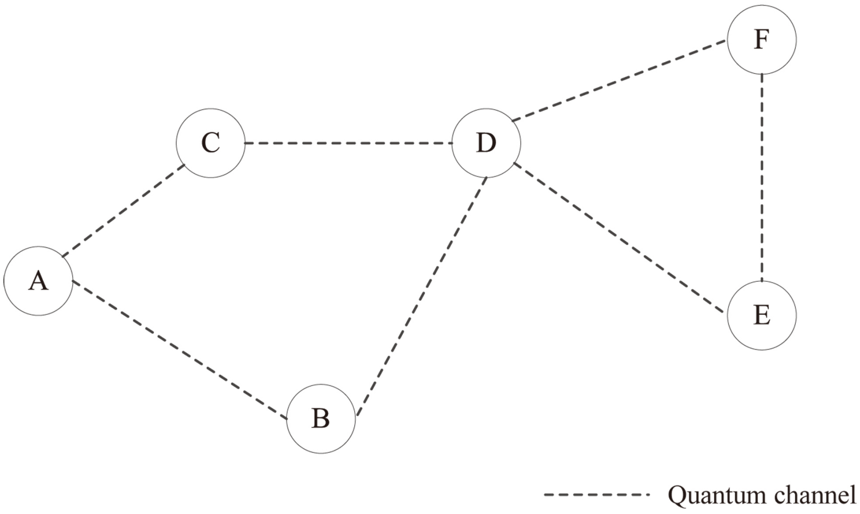

Figure 1. Wireless quantum network.

relay path establishment.

2.2. Three-Party QSS

In 2009, Liu *et al.* [8] proposed a three-party QSS scheme with pre-shared GHZ states, which uses an auxiliary EPR pair to encode two secret message bits.

By convention, the sender is denoted as Alice (A), and the receivers is denoted as Bob (B) and Charlie (C). First, they share three-particle GHZ states, each of which is:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ABC} \tag{1}$$

After eavesdropping check to ensure the security of quantum channel (GHZ states), Alice prepares an EPR pair in the state:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{a_1a_2} \tag{2}$$

Four unitary operators are defined as: $U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} = |1\rangle\langle 0| + |0\rangle\langle 1|$, $U_{10} = |0\rangle\langle 1| - |1\rangle\langle 0|$, $U_{11} = |0\rangle\langle 0| - |1\rangle\langle 1|$.

The system state after encoding can be expressed as:

$$|\Phi\rangle_{a_1a_2ABC} = U_X\,|\phi^+\rangle_{a_1a_2} \otimes |\Phi\rangle_{ABC} \tag{3}$$

where U_X is one of four operations U_{00}, U_{01}, U_{10}, U_{11}, which encodes a two-bit message "00", "01", "10", and "11", respectively.

Next, Alice applies a controlled-NOT (CNOT) gate on both particle A and particle a_1, here a_1 is the controller and A is the target. Then she sends the particle a_1 and a_2 through the Hadamard (H) gate, respectively.

Then Alice applies a Bell-state measurement on both particles a_1 and a_2, Bob and Charlie measure the particle B and C with diagonal basis $\sigma_X = \{|+\rangle, |-\rangle\}$, respectively. After that, they all publish measurement results.

Their measurement results will be correlated in certain forms according to different encoding operation U_X Alice performs. Thus Bob and Charlie can consider three parties' measurement results and further recover secret messages.

3. The Proposed Scheme

In Liu's QSS scheme [8], the correlation between the measurement results and secret message play a important role in decoding. Assume that other nodes are also aware of the correlation, they can also recover the secret messages.

The main idea of our scheme is that in a cluster network cored on three parties of QSS, Alice (A), Bob (B), and Charlie (C) are cluster heads. In each communication period, one cluster head plays the role of a message sender, other two cluster heads are assistants to help sender broadcast messages. Moreover, we design two types of communication modes, namely whole-network broadcast and intra-cluster broadcast, to meet different requirement of a sender.

The quantum secret broadcast scheme is described as follows:

Step 0: *Initializing*

Figure 2 shows initializing phase of the scheme. We apply a cluster structure for network, three cluster heads *A*, *B*, and *C*, own three-party GHZ states, each GHZ state is:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)_{ABC} \tag{4}$$

where A, B and C indicate the particle held by *A*, *B*, *C* respectively. Each cluster head has its own cluster members, we denote *A*'s members as $[A_1, A_2, A_3, \ldots]$, *B*'s and *C*'s members as $[B_1, B_2, B_3, \ldots]$ and $[C_1, C_2, C_3, \ldots]$, respectively. Moreover, each cluster head shares EPR pairs with its own cluster members, respectively.

Before communication, quantum channel of GHZ states should be checked for potential attacks, the GHZ among *A*, *B* and *C* can be rewritten as:

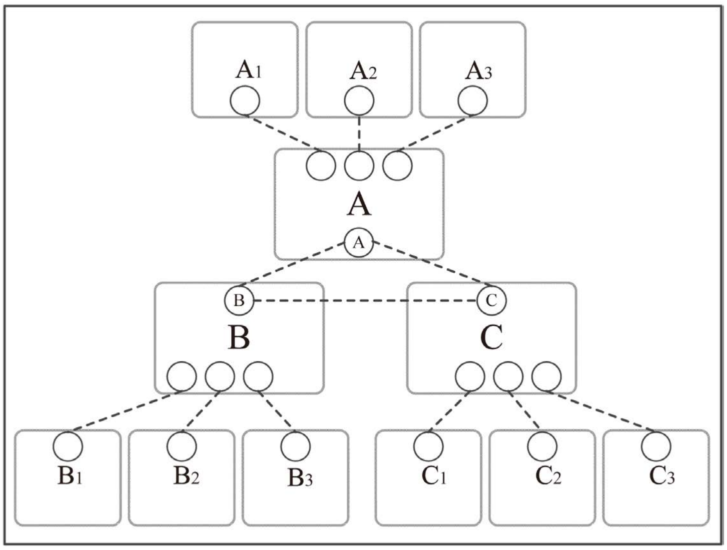

Figure 2. Initializing phase.

$$|\Phi\rangle = \frac{1}{2}\left(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle\right)_{ABC} \tag{5}$$

where $|+\rangle = \frac{\sqrt{2}}{2}\left(|0\rangle + |1\rangle\right)$, $|-\rangle = \frac{\sqrt{2}}{2}\left(|0\rangle - |1\rangle\right)$. According to Equation (7), if *A* performs measurement under basis σ_x on her particle and the result is $|+\rangle$ or $|-\rangle$, the measurement results of *B* and *C* should be $|++\rangle$, $|--\rangle$ or $|+-\rangle$, $|-+\rangle$. For a secure channel without disturbing, three parties' measurement results must be correlated as Equation (7). By using this method, A can choose a subset of particles to detect if there exists a attack. If the error rate of measurement results is under the threshold, the channel is secure and the scheme continues, otherwise, if the channel is insecure, the scheme is terminated.

Step 1: *Encoding key updating*. When each communication period begins, three cluster heads generate a two-bit "encoding key" Y by turns, and then transmit it to other two cluster heads by quantum teleportation.

Assume that it is A's turn to produce the "encoding key" Y, which is one of the four possible encoding key "00", "01", "10", and "11". Then she prepares two qubits for *B* and *C*, respectively, in which the state $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ means "1", and the state $|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ means "0". After that, A sends two qubits represented Y to *B* and *C* by controlled quantum teleportation [11], respectively.

When *B*, *C* both receive the encoding key Y, three cluster heads transmit the key to their own cluster members by quantum teleportation based on shared EPR pairs.

After that, the whole network knows the latest encoding key. So the encoding key updating phase is completed.

Step 2: *Communication mode selecting*. To meet different requirement of cluster heads, the communication mode can be selected to whole-network broadcast or intra-cluster broadcast.

If a cluster head needs to broadcast messages to the whole network, it will announce an application in this step. Then three cluster heads discuss to select one appropriate cluster heads to be the sender of whole-network broadcast. Otherwise, the communication switches into the mode of intra-cluster broadcast if no cluster heads announce an application.

1) Whole-network broadcast

Step 3: *Message encoding*. Assume that cluster head A is chosen to be the sender. For each shared GHZ state, she prepares an auxiliary EPR state as follows:

$$|\phi^+\rangle_{a_1a_2} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{a_1a_2} \tag{6}$$

Figure 3(a) shows the system states before encoding, where A, B, C form a three-particle entangled state, a_1 and a_2 form a two-particle entangled

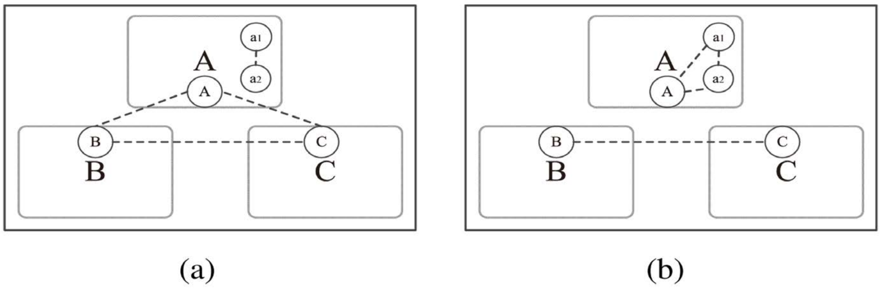

Figure 3. System state of whole-network broadcast.

state.

We define four unitary operators:

$$U_{00}=\begin{bmatrix}1&0\\0&1\end{bmatrix},U_{01}=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$
$$U_{10}=\begin{bmatrix}0&1\\-1&0\end{bmatrix},U_{11}=\begin{bmatrix}1&0\\0&-1\end{bmatrix} \tag{7}$$

Step (3.1) A encodes message on EPR state with two operators U_X and U_Y, the system state becomes:

$$|\Phi\rangle=U_XU_Y|\phi^+\rangle\otimes|\Phi\rangle_{ABC} \tag{8}$$

where X is the two bits message and Y is the encoding key.

For convenience, we assume the encoding key Y is "00". After encoding with two operators, we obtain:

$$\begin{aligned}|\Phi_{00}\rangle&=U_{00}U_{00}|\phi^+\rangle_{a_1a_2}\otimes|\Phi\rangle_{ABC}\\&=\frac{1}{2}(|00000\rangle+|11000\rangle+|00111\rangle+|11111\rangle)_{a_1a_2ABC}\end{aligned} \tag{9}$$

$$\begin{aligned}|\Phi_{01}\rangle&=U_{01}U_{00}|\phi^+\rangle_{a_1a_2}\otimes|\Phi\rangle_{ABC}\\&=\frac{1}{2}(|01000\rangle+|10000\rangle+|01111\rangle+|10111\rangle)_{a_1a_2ABC}\end{aligned} \tag{10}$$

$$\begin{aligned}|\Phi_{10}\rangle&=U_{10}U_{00}|\phi^+\rangle_{a_1a_2}\otimes|\Phi\rangle_{ABC}\\&=\frac{1}{2}(|01000\rangle-|10000\rangle+|01111\rangle-|10111\rangle)_{a_1a_2ABC}\end{aligned} \tag{11}$$

$$\begin{aligned}|\Phi_{11}\rangle&=U_{11}U_{00}|\phi^+\rangle_{a_1a_2}\otimes|\Phi\rangle_{ABC}\\&=\frac{1}{2}(|00000\rangle-|11000\rangle+|00111\rangle-|11111\rangle)_{a_1a_2ABC}\end{aligned} \tag{12}$$

Step (3.2) A applies a CNOT gate on both particles a_1 and A, here a_1 is the controller and A is the target.

Step (3.3) A performs a Hadamard gate on a_1 and a_2, respectively. After that, the system state can be written as:

$$\begin{aligned}|\Phi_{00}{}'\rangle=\frac{1}{\sqrt{2}}[&\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{a_1a_2}|+\rangle_A\otimes\frac{1}{\sqrt{2}}(|++\rangle+|--\rangle)_{BC}\\&+\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{a_1a_2}|-\rangle_A\otimes\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle)_{BC}]\end{aligned} \tag{13}$$

$$\begin{aligned}\left|\Phi_{01}{}'\right\rangle = \frac{1}{\sqrt{2}}[&\frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{a_1a_2}\left|+\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|++\right\rangle + \left|--\right\rangle)_{BC} \\ &-\frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)_{a_1a_2}\left|-\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|+-\right\rangle + \left|-+\right\rangle)_{BC}]\end{aligned} \tag{14}$$

$$\begin{aligned}\left|\Phi_{10}{}'\right\rangle = \frac{1}{\sqrt{2}}[&\frac{1}{\sqrt{2}}(\left|00\right\rangle - \left|11\right\rangle)_{a_1a_2}\left|-\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|+-\right\rangle + \left|-+\right\rangle)_{BC} \\ &-\frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)_{a_1a_2}\left|+\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|++\right\rangle + \left|--\right\rangle)_{BC}]\end{aligned} \tag{15}$$

$$\begin{aligned}\left|\Phi_{11}{}'\right\rangle = \frac{1}{\sqrt{2}}[&\frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{a_1a_2}\left|-\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|+-\right\rangle + \left|-+\right\rangle)_{BC} \\ &+\frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)_{a_1a_2}\left|+\right\rangle_A \otimes \frac{1}{\sqrt{2}}(\left|++\right\rangle + \left|--\right\rangle)_{BC}]\end{aligned} \tag{16}$$

System state after encoding is as shown in **Figure 3(b)**, where the original entangled GHZ state $\left|\Phi\right\rangle_{ABC}$ is destroyed, while particles a_1, a_2, A form a new three-party entangled state, B and C form a two-party entangled state.

*Step*4: *Measurement result broadcasting*. Sender A performs Bell-state measurement on both particles a_1 and a_2, *B* and *C* measures their own particle B and C with basis σ_x, respectively. Then, they broadcast own measurement results.

Step 5: *Message decoding*.

Step (5.1) All the cluster members consider three cluster heads' measurement results and can read out A's messages M by referring to the correlation of measurement results and messages, which can be inferred from Equations (13)-(16) and listed in **Table 1**.

Step (5.2) As M is a message encoded with the encoding key Y, so receivers need to decode the message with encoding key Y to obtain the original message M_o:

$$M_o = M \oplus Y \tag{17}$$

Let us take an example to illustrate how the mode of whole-network broadcast works. At first, we assume that the encoding key Y is "10", and it is informed to all nodes in Step 1 of *Encoding key updating*, and A is chosen to be the sender in the mode of whole-network broadcast. After encoding, *A*'s measurement results are $\left|\phi^+\right\rangle\left|\psi^-\right\rangle\left|\phi^-\right\rangle\ldots$, *B*'s results are $\left|+\right\rangle\left|-\right\rangle\left|+\right\rangle\ldots$, and *C*'s results are $\left|-\right\rangle\left|-\right\rangle\left|+\right\rangle\ldots$, all nodes consider three cluster heads' results and refer to **Table 1**

Table 1. Correlation of measurement results and messages in whole-network mode.

	B's and *C*'s results			
A's results	$\left\|+\right\rangle\left\|+\right\rangle$	$\left\|+\right\rangle\left\|-\right\rangle$	$\left\|-\right\rangle\left\|+\right\rangle$	$\left\|-\right\rangle\left\|-\right\rangle$
$\left\|\phi^+\right\rangle$	00	11	11	00
$\left\|\phi^-\right\rangle$	01	10	10	01
$\left\|\psi^+\right\rangle$	11	00	00	11
$\left\|\psi^-\right\rangle$	10	01	01	10

to read out massages M as “11”, “10”, “01”, …, then receivers XOR (exclusive OR) the encoding key $Y=10$ and M to recover original messages M_O as “01”, “00”, “11”, ….

2) Intra-cluster broadcast

Assume that no cluster heads announce an application, the communication will switch into the mode of intra-cluster broadcast, in which three cluster heads can send messages to their own cluster members. We take A as an example to illustrate this mode.

Step 3: *Message encoding*. Similarly, based on the idea of QSS, A randomly selects two cluster members (denote as A_1 and A_2) to be assistant. The system state of three parties is:

$$|\Phi\rangle_{1234}=|\phi^+\rangle_{12}\otimes|\phi^+\rangle_{34} \tag{18}$$

As is shown in **Figure 4(a)**, A holds particle 1 and 3, while A_1 and A_2 hold the particle 2 and 4, respectively. Particle 1 and 2 form an entangled state, 3 and 4 form an entangled state.

We define two unitary operators for encoding:

$$U_0=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},U_1=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \tag{19}$$

A encodes one bit message on particle 1 with two operators U_Z and $U_{Y'}$, system state will be :

$$|\Phi\rangle=U_Z U_{Y'}(|\phi^+\rangle\otimes|\phi^+\rangle) \tag{20}$$

where Z is the one bit message, Y' is a number by XORing the first digit and the second digit of the encoding key Y. For example, assume the encoding key Y is “11”, Y' should be $Y'=1\oplus 1=0$.

For convenience, we assume “Y'” as 0. After encoding, we obtain:

$$\begin{aligned}|\Phi\rangle_0&=U_0U_0\left(|\phi^+\rangle_{12}\otimes|\phi^+\rangle_{34}\right)\\&=\frac{1}{2}\left(|\phi^+\rangle+|\phi^-\rangle|\phi^-\rangle+|\psi^+\rangle|\psi^+\rangle+|\psi^-\rangle|\psi^-\rangle\right)_{1324}\end{aligned} \tag{21}$$

$$\begin{aligned}|\Phi\rangle_1&=U_1U_0\left(|\phi^+\rangle_{12}\otimes|\phi^+\rangle_{34}\right)\\&=\frac{1}{2}\left(|\phi^+\rangle|\psi^+\rangle-|\phi^-\rangle|\psi^-\rangle+|\psi^+\rangle|\phi^+\rangle-|\psi^-\rangle|\phi^-\rangle\right)_{1324}\end{aligned} \tag{22}$$

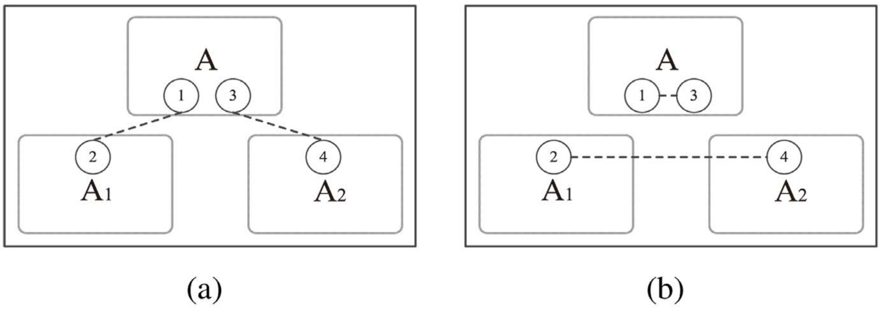

Figure 4. System state of intra-cluster broadcast.

From Equations (21)-(22), system state is changed as shown in **Figure 4(b)**, where the two original entangled pairs are all destroyed, and particle 1 and 3 form a new entangled state, 2 and 4 form a new entangled state.

Step 4: *Measurement result Broadcasting*. A performs a Bell-state measurement on both particles 1 and 3, A_1 and A_2 measures the particle 2 and 4 with basis σ_Z. Then, they all broadcast the measurement results.

Step 5: *Message decoding*.

Step (5.1) A's cluster members consider three parties' results and read out message M by referring to the correlation of measurement results and messages, which is inferred from Equations (21)-(22) and listed in **Table 2**.

Step (5.2) M is a message encoded with Y', so receivers need to decode the message with Y' to obtain the original message M_o:

$$M_o = M \oplus Y' \tag{23}$$

We take an example of A cluster to illustrate how intra-cluster mode works. Assume that the encoding key Y is still "10", so $Y' = 0 \oplus 1 = 1$. A's results are $|\phi^+\rangle|\phi^-\rangle|\psi^+\rangle\ldots$, A_1 's and A_2 's results are $|0\rangle|1\rangle|0\rangle\ldots$ and $|0\rangle|1\rangle|1\rangle\ldots$, respectively. A's cluster members consider three parties' results and refer to **Table 2** to read out messages M "0", "0", "0", …, then they XOR the M and Y' to recover original messages M_O as "1", "1", "1", ….

4. Scheme Analysis

4.1. Network

Our scheme aims to achieve message broadcast in WQN, which attempts to extend communication mode and improve network performance. Different from conventional schemes based on quantum teleportation [2] [3] [4] [10], we apply the method of QSS instead of teleportation.

For the reason of applying QSS, our scheme has differences with conventional schemes which are based on quantum teleportation in many aspects. Our scheme transmits classical messages by broadcast, while previous ones transmit quantum state by teleportation. Our scheme makes a attempt to achieve message broadcast, the number of receivers can be m or $3m$ under different communication mode, where m is the number of cluster members. Each sender needs two assistants in our scheme, while conventional schemes also needs

Table 2. Correlation of measurement results and messages in intra-cluster mode.

	A_1 's and A_2 's results			
A's results	$\lvert 0\rangle\lvert 0\rangle$	$\lvert 0\rangle\lvert 1\rangle$	$\lvert 1\rangle\lvert 0\rangle$	$\lvert 1\rangle\lvert 1\rangle$
$\lvert\phi^+\rangle$	0	1	1	0
$\lvert\phi^-\rangle$	0	1	1	0
$\lvert\psi^+\rangle$	1	0	0	1
$\lvert\psi^-\rangle$	1	0	0	1

nodes as assistants to build a routing path from source to destination, the farther distance between source and destination is, the more assistant nodes are needed. we denote d as the number of assistant nodes.

Table 3 gives a summary of comparison between our scheme and conventional schemes.

4.2. Efficiency

The efficiency in our quantum communication protocol can be defined as:

$$\eta = n\frac{m_u}{q_t} \tag{24}$$

where m_u is the number of transmitted qubits, q_t is the number of consumed qubits, n is the number of message receivers.

We make a comparison between our scheme and Cao's scheme [4], for the latter is a typical research of previous schemes and it also uses a cluster structure for WQN.

Consider a situation that a cluster head sends messages to his and other cluster heads' members. In our scheme, $m_u = 1$ for 2 classical bits are equivalent to 1 qubit, $q_t = 5$, $n = 3m$ (in the mode of whole-network broadcast), m is the number of one cluster members. In Cao's scheme, $m_u = 1$, $n = 1$, $q_t = d(d \geq 1)$, for the distance between sender and receiver is at least 1.

Table 4 makes a comparison between our scheme and Yang's scheme.

We can see from **Table 4** that the performance of our scheme is better than Yang's scheme, especially when the number of receivers n is larger and distance d is farther.

Table 3. Comprehensive comparison.

Items	Our scheme	Conventional schemes
Basic technology	QSS	Quantum teleportation
Things to transmit	Classical message	Qubit
Communication mode	Broadcast	Point-to-point
Assistant nodes	2	$d(d \geq 1)$
Number of receivers	m or $3m$	1

Table 4. Efficiency comparison.

Scheme	Our scheme	Cao's scheme
m_u	1	1
q_t	5	$d(\geq 1)$
n	$3m$	1
η for m = 5, d = 2	3	$\frac{1}{2}$
η for m = 10, d = 3	6	$\frac{1}{3}$

4.3. Security

In the proposed scheme, no qubits carrying messages are transmitted directly, so quantum channel only exists in the GHZ states. If an eavesdropper Eve cannot escape from the security check at the phase of *Step* 0: *Initializing*, our scheme is secure. The security check method of our scheme is the same as QSS schemes in [7] [8], which assumes Eve's attack $\hat{E}$ performs on Hilbert space $H_{ABC} \otimes H_E$, then the whole quantum system can be written as:

$$\begin{aligned}|\Omega\rangle = \frac{1}{\sqrt{2}}[(|0\rangle(\alpha_1|00\rangle|\varepsilon_{000}\rangle + \beta_1|01\rangle|\varepsilon_{001}\rangle \\ +\gamma_1|10\rangle|\varepsilon_{010}\rangle + \delta_1|11\rangle|\varepsilon_{011}\rangle) \\ +(|1\rangle(\delta_2|11\rangle|\varepsilon_{100}\rangle + \gamma_2|10\rangle|\varepsilon_{101}\rangle \\ +\beta_2|01\rangle|\varepsilon_{110}\rangle + \alpha_2|00\rangle|\varepsilon_{111}\rangle)]\end{aligned} \tag{25}$$

The error rate involved in Eve is $\lambda = 1-|\alpha_1|^2 = 1-|\delta_2|^2$, so Eve can be easily detected during the process of security check.

Considering that receivers read out messages according to the three cluster head's measurement results, another secure problem is that if an eavesdropper also knows the correlation between messages and measurement results, it can obtain messages. To solve this problem, our scheme generates an encoding key Y periodically to add an extra encoding operation. Just like one-time pad, the encoding key plays a role of periodically updating a key to encode and decode messages, and it will be informed to all network before communication. If an eavesdropper is not in the cluster of three heads, it will not obtain the latest key, so it can only randomly select one of "00", "01", "10", "11" as the key to recover messages.

In the whole-network mode, by randomly selecting a key, an eavesdropper will recover a message with the error rate 75%, while in the intra-cluster mode, the error rate is 50%. So our scheme uses security check for quantum channel and key updating for secret messages to ensure security.

5. Conclusion

In this paper, a quantum secret broadcast scheme was proposed to solve efficiency problem in WQN, where each two bits are encoded in an auxiliary EPR states. The proposed scheme constructs a cluster network cored on three-party QSS, three cluster heads share three-party GHZ states, and each cluster head shares EPR pairs with its own cluster members. For different requirement of cluster heads, the scheme can be selected into whole-network broadcast, in which one cluster head is message sender and other two cluster heads are assistants to help broadcast messages to whole network, or intra-cluster broadcast, in which each cluster head chooses two cluster members as assistants to help broadcast messages to its intra-cluster members. Furthermore, a wireless quantum network with more than three cluster heads needs to be investigated for extensive application.

Acknowledgements

This project was supported by the National Natural Science Foundation of China (No. 61571024) and the National Key Research and Development Program of China (No. 2016YFC1000307) for valuable helps.

References

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public-Key Distribution and Tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, IEEE Press, 175-179.

[2] Cheng, S.T., Wang, C.Y. and Tao, M.H. (2005) Quantum Communication for Wireless Wide-Area Networks. *IEEE Journal on Selected Areas in Communications*, **23**, 1424-1432. https://doi.org/10.1109/JSAC.2005.851157

[3] Li, J.S. and Yang, C.F. (2009) Quantum Communication in Distributed Wireless Sensor Networks. *IEEE 6th International Conference*, Macau, 12-15 Oct. 2009, 1024-1029. https://doi.org/10.1109/MOBHOC.2009.5337016

[4] Cao, Y., Yu, X.Y. and Cai, Y.X. (2013) Wireless Quantum Communication Networks with Mesh Structure. *IEEE 3rd International Conference on Information Science and Technology*, Yangzhou, 23-25 March 2013, 1485-1489. https://doi.org/10.1109/ICIST.2013.6747818

[5] Hillery, M., Buzek, V. and Berthiaume, A. (1999) Quantum Secret Sharing. *Physical Review A*, **59**, 1829-1834. https://doi.org/10.1103/PhysRevA.59.1829

[6] Deng, F.G., Zhou, H.Y. and Long, G.L. (2005) Bidirectional Quantum Secret Sharing and Secret Splitting with Polarized Single Photons. *Physics Letters A*, **337**, 329-334. https://doi.org/10.1016/j.physleta.2005.02.001

[7] Wang, J., Zhang, Q. and Tang, C.J. (2007) Multiparty Quantum Secret Sharing of Secure Direct Communication Using Teleportation. *Communications in Theoretical Physics*, **47**, 454-458. https://doi.org/10.1088/0253-6102/47/3/015

[8] Liu, Y. and Xu, C. (2009) Three-Party Quantum Secret Sharing Based on Secret Direct Communication. *International Forum on Information Technology and Applications*, **1**, 126-130.

[9] Hwang, T., Hwang, C.C. and Li, C.M. (2011) Multiparty Quantum Secret Sharing Based on GHZ States. *Physica Scripta*, **83**, 045004. https://doi.org/10.1088/0031-8949/83/04/045004

[10] Nguyen, T.M.T., Sfaxi, M.A. and Ghernaouti-Helie, S. (2006) Integration of Quantum Cryptography in 802.11 Networks. *Proc. 1st Int. Conf. on Availability, Reliability and Security*, Vienna, 20-22 April 2006, 116-123. https://doi.org/10.1109/ARES.2006.75

[11] Zhou, J.D., How, G. and Wu, S.J. (2007) Controlled Teleportation of an Arbitrary Multi-Qudit State in a General Form with d-Dimensional Greenberger-Horne-Zeilinger States. *Chinese Physics Letters*, **24**, 1151-1153. https://doi.org/10.1088/0256-307X/24/5/007