Ad Hoc Quantum Network Routing Protocol based on Quantum Teleportation

Cai Xiaofei[1) †] ,Yu Xutao[2)], Shi Xiaoxiang[3)], Qian Jin[4)], Shi Lihui[5)], Cai Youxun[5)]
1) 2) 5) 6) State Key Laboratory of Millimeter Waves
Southeast University
Nanjing, P. R. China
3) Nanjing Guobo electronics Co., Ltd 4) Jiangsu Province Water Conservancy Internet Data Center

***Abstract*-In this paper, a quantum communication routing protocol is designed for quantum ad hoc network. This protocol is on-demand routing based on EPR numbers shared by adjacent nodes, concerning that it is a limited source. When quantum channel is established, quantum states from one quantum device can be teleport to another even when they do not share EPR pairs wirelessly. Part of information transferred by classic channel can be dealt with using simple logics. In this way, the goal of safety communication between source and destination is realized, improving the weakness of ad hoc network such as Eavesdropping and Active attacks. In terms of time complexity, the mechanism transports a quantum bit in time almost the same as the quantum teleportation does regardless of the number of hops between the source and destination.**

***Index Terms*-EPR pair, quantum route, quantum entanglement, ad hoc network, quantum teleportation.**

I. INTRODUCTION

In quantum mechanics, there is some kind of entangled relationship between two microscopic particles from same source, no matter how far away they are separated from each other, the state of a particle would immediately change according to another particle's change, which is called quantum entanglement. There is a certain degree of confidentiality in quantum teleportation. Based on the above characteristics, there is a article proposes a quantum routing mechanism in hierarchical network[1]. Another article designs a two-way secure communication protocol, which can set up the secure routing path from sender to receiver when they already share EPR pairs[3]. Communication Protocol Based on Classical Network Coding is also proposed[4].

This article introduces quantum communication technologies into an ad hoc network protocol to increase communication security[2]. In order to realize the quantum routing mechanism in a peer-to-peer network, first part of the article introduces how to build up a quantum network. The rest of this paper describes a routing process. Section IV discussed the some of the simulation results. And Section V discussed some related issues. Finally, conclusion are drawn in Section VI.

II. THE MODEL OF QUANTUM AD HOC NETWORK

Base on ordinary ad hoc network, this network assumes each mobile device has a quantum communication functions, including the capacity of holding and manipulate EPR pairs, and they support classical communication at the same time. The scenario assumed as follows:

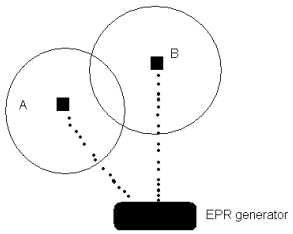

Figure 1. Skeleton diagram for EPR pairs generator

Therefore, a model of the ad hoc network can be simplified as follows:

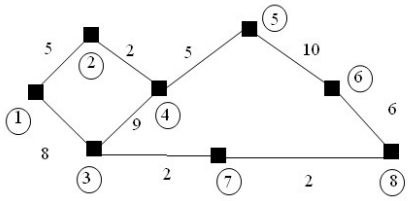

Figure 2. Model for quantum ad hoc network

Connection between points represents that entangled quantum channel has been established between them in the figure. Numbers marked in the solid line are the remaining number of EPR pairs between the two nodes. As shown, the path from node 1 to node 5, we tend to choose the path1-3-4-5, since there is a smaller number of the EPR pairs between node 2 and 4. Otherwise, a path is lost after EPR pairs are consumed out.

III. QUANTUM PROTOCOL

A. Route establishment process

When a node can not find an available route to a node, it broadcasts a RREQ message. This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination expires or is broken .

The Originator Sequence Number in the RREQ message is the node's own sequence number. The RREQ ID field is

*This work has been supported by Science Project of Ministry of Transport of China (No. 2012-364-222-203).

incremented by one from the last RREQ ID used by the current node. Each node maintains only one RREQ ID.

When a node receives a RREQ, it first checks to determine whether it has received a RREQ with the same Originator IP Address and RREQ ID within at least the last PATH_TRAVERSAL_TIME milliseconds. If such a RREQ has been received, the node discards the received RREQ[1].

In quantum communication, we need to adopt the path of more EPR pairs, so weights will be modified: First, we take the reciprocal of the remaining number of EPR pairs to replace the path length as a measure of algorithms. Consider this, a transfer between two nodes will the consume the least EPR pairs. In consideration of the fairness of each node, if adjacent nodes has a high number of EPR pairs, an nodes with few remaining EPR pairs may be picked , this design is incomplete.

Therefore, redo some processing on the weight case: the weight can be reset as $n^{1/\alpha}$ (n represent the number of remaining EPR, $\alpha > 1$) In addition, the number 1 is special in inverse proportion, so if a node keeps only one EPR pair, its adjacent nodes automatically set its own weight to, but when the node itself need to communicate, it assumes the channel exists. Then normalized EPR numbers are used, and each received valid message will be recorded and compared of the EPR numbers.

After EPR number is processed, the node will record the source node IP address of the reverse routing. If necessary, this route will be created, or update according to the serial number of the source node in the RREQ message. The initiating node serial number in RREQ message will be used to compare with the corresponding destination node serial number in the reverse routing table, if bigger than that in the table, it will be added into the routing table. Entry "Normalized EPR number " in reverse route table is added directly from the RREQ message. Then the node further forwarded this RREQ message to other neighbors.

After a certain period of time, if an intermediate node received a second RREQ message from a different path, it compares the source node serial number first, found serial number is same to that in the table, further examine if the new path correspond to more EPR pairs number, then update the reverse routing in routing table, and change the "Normalized EPR number", then once again forwarded the message to other neighbors.

When destination node finally generates a RREP message, it propagates along the reverse route. The prior established quantum channel is usually a classical less hops or shorter distance path. The rest of the RREQ message reach the destination node one after another will be checked about the serial number and EPR number. If the RREP is enough fresh, compare remaining EPR pairs number, if more than the existing line, namely it corresponds to a smaller "Normalized EPR number ", destination note will broadcasts new RREP of the same serial number to its neighbor node, informing that there is a better path. Since time delay is limited, before the optimal path is found, messages can transmitted through earlier paths. When better path is found, source node received the RREQ message again, then a new quantum channel is established. Source node will take the new quantum channel.

B. *Routing example*

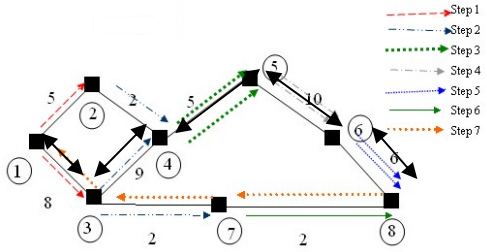

Figure 3. Route discovery process

The routing process is as follows:

1) Node 1 wants to communicate with node 8, first generate a RREQ message. And the serial number is set to 1.

2) Neighbor nodes 2, 3 received the RREQ, generate the reverse routing tables to record a path to the source node, then add remaining EPR numbers on the "Normalized EPR number ", record the sequence number as 1. Node 2 forwards the RREQ message to node 4 (EPR normalized number = 1/5). Node 3 forwards the RREQ message to node 4 (EPR normalized number = 1/8).

3) Node 4 receives two RREQ message, assuming that first received the message from node 2, it repeats the previous process: generate reverse routing table, record the path to node 2, then add the reciprocal of remaining EPR number to "Normalized EPR number ", record the serial number 1. Then the RREQ is forwarded to node 5. At this time the node received a message from node 3. It compares the serial number, found the serial number is same, so further compare the "Normalized EPR number ", found that there remains more EPR pairs in the path from nodes 3 (EPR normalized quantity = 1/8 +1 / 9 <1/5 +1 / 2), then forwards a new RREQ message to the downstream node, and change upstream path node in reverse routing table to node 3. Node 3 will also sent the RREQ message from node 1 to node 7. (EPR normalized quantity = 1/8 +1 / 2)

4) Node 5 twice received the RREQ message from node 4, the remaining amount in the second EPR records is more (EPR normalized quantity = 1/8 +1 / 8 +1 / 5), node 5 also update its routing table, sent a new RREQ message to the neighbor node 6. Node 8 also received the RREQ from node 7, then find out that the destination IP address in message matches its own IP address, prepare to send a RREP message to node 7.

5) Node 8 reply a RREP message along the prior arrival path.. In each hop, the node verifies the serial number first, and then record the positive route. The source node find the sequence number in RREP message sequence number meet that pre-issued serial number of the destination node set in RREQ message, so the path is set up.

Node 8 will receive two other RREQ messages from path 5-6-8, the destination node find that new message have the same serial number, but there are less remaining EPR pairs. Node 8

will send a new RREP message to the source node along the new reverse route. If there is other RREQ message through a different path to node 8, but the remaining EPR pairs did not outnumber the previous one, the message will not be processed.

6) Node 8 sends a new RREP message.

The first RREQ choose the path 8-6-5-4-2-1.

The second RREQ choose the path 8-6-5-4-3-1.

Source node already communicate with node 8 in other path , but after it received RREP message from node 2, found the serial number is same while the path is better, source node choose the new paths.

C. Communication example

There are two communication cases:

1) Case of Quantum Relay

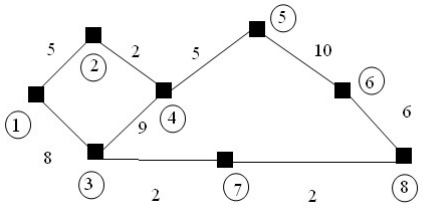

Figure 4. Model for Quantum Relay

The optimal path is 1-3-4-5-6-8, in the quantum relay scheme, communication process between node 1 and 8 should be as follow:

A qubit 0 can be symbolized in the form of

$$|y\rangle = a|0\rangle_0 + b|1\rangle_0 \tag{1}$$

Node 1 hope to sent the quantum state $|y\rangle$ to node 8. And the shared entanglement between node 1 and node 3 is :

$$|\phi\rangle_{13} = 1/\sqrt{2}(|0\rangle_1|1\rangle_3 - |1\rangle_1|0\rangle_3) \tag{2}$$

The statement of 3 qubits is shown as follows:

$$\begin{aligned}|\varphi\rangle_{130} &= |y\rangle_0 \otimes |\phi\rangle_{13} \\ &= (a|0\rangle_0 + b|1\rangle_0) \otimes 1/\sqrt{2}(|0\rangle_1|1\rangle_3 - |1\rangle_1|0\rangle_3) \\ &= 1/\sqrt{2}(a|0\rangle_0|0\rangle_1|1\rangle_3 + b|1\rangle_0|0\rangle_1|1\rangle_3 \\ &\quad - a|0\rangle_0|1\rangle_1|0\rangle_3 - b|1\rangle_0|1\rangle_1|0\rangle_3) \\ &= a/\sqrt{2}(|0\rangle_0|0\rangle_1|1\rangle_3 - |0\rangle_0|1\rangle_1|0\rangle_3) \\ &\quad + b/\sqrt{2}(|1\rangle_0|0\rangle_1|1\rangle_3 - |1\rangle_0|1\rangle_1|0\rangle_3)\end{aligned} \tag{3}$$

In order to complete quantum teleportation, node 1 must measure qubit 1 and 3. Thus, the wave function of the three particle system can be expressed as:

$$\begin{aligned}|\varphi\rangle_{130} = 1/2[&|\theta^-\rangle_{10}(-a|0\rangle_3 - b|1\rangle_3) \\ &+ |\theta^+\rangle_{10}(-a|0\rangle_3 + b|1\rangle_3) \\ &+ |\phi^-\rangle_{10}(a|1\rangle_3 + b|0\rangle_3) \\ &+ |\phi^+\rangle_{10}(a|1\rangle_3 - b|0\rangle_3)]\end{aligned} \tag{4}$$

Node 1 uses the analyzer that can identify Bell base to measure qubit 1 and EPR qubit 0 together, and then transport measurement result to node 3.

Node 3 accordingly implement unitary transformation on qubit 3 correspond to the results, so as to achieve the quantum teleportation.

So that the information is transmitted from node 1 to node 3, and similarly in turn transmitted to the destination node 8.

As can be seen, the shortcoming of quantum relay plan is: the target qubit is transmitted through intermediate nodes, which results in the lack of security and confidentiality. In addition, the time it requires of data transfer is proportional to the number of routing hops. In order to overcome the above drawbacks, EPR-pair bridging program is proposed.

2) Case of EPR-Pair Bridging

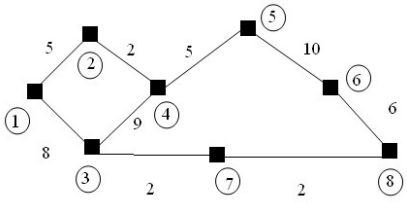

Figure 5. Model for RPR-pair Bridging

The optimal path is 1-3-4-5-6-8.

Quantum circuit makes quantum teleportation and measurement transmission of classical information be parallel, which is equivalent to transmit results for once.

The Quantum circuit is as below[1]:

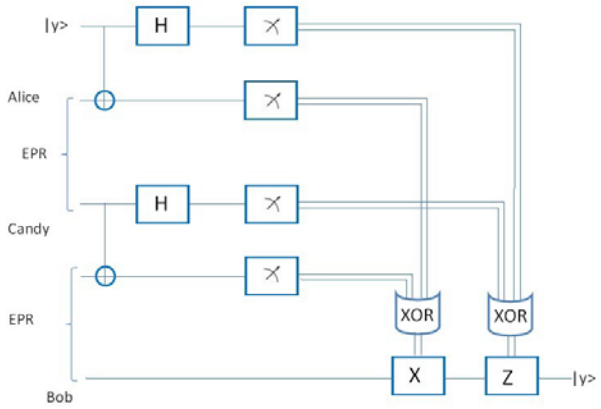

Figure 6. Quantum circuit for RPR-pair Bridging

Node 1 make $|y\rangle$ serve as the control bit of the NAND gate control terminal to act on the EPR pair shared by node 1 and node 3. Then H gate is applied on $|y\rangle$ and this measurement result is transmitted to XOR logic before Z gate of destination node. The other measurement result of EPR pairs is sent to XOR logic before X gate.

Node 3 make the EPR-pair shared with node 1 serve as the control bit of the NAND gate control terminal to act on the

EPR pair shared by node 3 and node destination node. Then make H-transform on the first EPR pair shared with node 1, send the measurement results to the Z gate XOR logic of destination node 8, and the other EPR pair measurement result to the X gate XOR logic of the destination node.

Then destination node exclusive XOR processing on measurement results transferred through classical channel, and send then into the quantum gates.

Finally, the EPR pair that destination node 8 shared with node 6 transformed into $|y>$ through X gate and Z gate ,which realizes the secure communications between two nodes that do not share EPR-pairs directly.

IV. SIMULATION

Assume there are 8 nodes in a communication net. Source node and destination node are generated randomly. Different length of destination and different numbers of EPR pairs are distributed to each nodes.

C =

0	0	0	0	3	0	9	1
0	0	0	9	0	0	0	0
0	0	0	9	0	0	0	8
0	9	9	0	6	9	0	0
3	0	0	6	0	7	6	5
0	0	0	9	7	0	0	8
9	0	0	0	6	0	0	2
1	0	8	0	5	8	2	0

Figure 7. Model for network

Numbers in Matrix C shows length of destination between nodes. Then source node is node 4 and destination node is node 7. All the routes from node 4 to node 7 should be found out. EPR pairs [2 4 5 2 1 6 3 7].

ans =

4	2	4	2	4	2	4	2
5	3	30	3	50	3	70	3
8	5	4	5	4	5	4	5
10	6	8	6	8	6	8	6
0	20	30	40	50	60	70	80
0	1	1	2	1	2	1	2
0	4	4	3	4	3	4	3
0	-1	-1	5	-1	5	-1	5
0	7	7	6	7	6	7	6
0	8	8	40	8	60	8	80
0	20	30	0	50	0	70	0
0	1	0	0	0	0	0	0
0	3	0	0	0	0	0	0
0	5	0	0	0	0	0	0
0	6	0	0	0	0	0	0
0	7	0	0	0	0	0	0
0	20	0	0	0	0	0	0

Figure 8. Transpose for result matrix

When element is -1,it means destination is found out. And when element is greater than 10, it means following elements are belong to another upstream node. There are 4 paths together. Path discovery order is according to distance between nodes: 4-5-7, 4-6-8-7,4-3-8-7,4-5-6-8-7.

Then first path to be found out is 4-5-7. Time is 2*(6km+6km)/c. At first communication is using this path. Traditional routing protocol will always use this path.While quantum protocol will take EPR numbers into concern. So the final path is 4-6-8-7.

V. DISCUSSION

When quantum channel is established, messages can be transmitted through the new path. There are usually two ways to teleport a quantum state from one quantum device to another that do not share EPR pairs wirelessly.

Due to space constraints, the route maintenance mechanism is not completely explained. And we can further consider to add the quantum communication technology to Routing Protocol contents. In addition, random routing on multistage interconnection networks can also be taken into concern[5]. The security and credibility of the intermediate nodes shall also be concerned, since teleportation through a long path rely much on the path[6].The concept of control qubits is a new idea[7].

VI. CONCLUSION

This paper introduced quantum communication technology into Ad hoc network to improve its security of communication, Then proposed a quantum routing mechanism in peer-to-peer network, which enables a quantum mobile device to teleport a quantum state to a remote site even if they do not share EPR pairs mutually. In terms of the time complexity, the time that quantum network takes to teleport a quantum state is independent of the number of routing hops. Among the route protocol, remaining EPR pair number is also taken into concern since EPR pairs is a limited source.

REFERENCES

[1] Sheng-Tzong Cheng, Chun-Yen Wang, and Ming-Hon Tao, "Quantum Communication for Wireless Wide-Area Networks," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, vol. 23, NO.7, JULY 2005, pp. 1426–1430.

[2] Ad hoc On-Demand Distance Vector (AODV) Routing. IETF RFC 3561, 19 July 2002, pp 10-11.

[3] Tien-Sheng Lin, Tien-ShengLin, Sy-Yen Kuo, *QUANTUM WIRELESS SECURE COMMUNICATION PROTOCOL*., ICCST 2007, pp 146-154.

[4] Hirotada Kobayashi, Franc¸ois Le Gall, "Perfect Quantum Network Communication Protocol Based on Classical Network Coding," ISIT 2010, Austin, Texas, U.S.A., June 13 - 18, 2010

[5] Rahul Ratan, Manish K. Shukla, A. Yavuz Oruc, "On Random Routing and its Application to Quantum Interconnection Networks," 40th Annual Conference on Information Sciences and Systems, pp. 1744 - 1749 .

[6] Stefan Rass and Peter Schartner, "A Unified Framework for the Analysis of Availability, Reliability and Security, With Applications to Quantum Networks," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 41, NO. 1, JANUARY 2011.

[7] Tien-Sheng Lin, Tien-ShengLin, Sy-Yen Kuo. SECURE QUANTUM PACKET TRANSMISSION MECHANISM FOR WIRELESS NETWORKS. IEEE2008, ICCST2008, pp29-35.