Multiparty Secure Communication by Using Quantum Key Distribution Protocols

K.Gopinath [1], B.J.Job karuna sagar [2]

1. Associate Professor,Department of Computer Science and Engineering, K.S.R.M.College of Engineering (AP.), India

2. Assistant Professor,Department of Computer Science and Engineering, K.S.R.M.College of Engineering (AP.), India

Abstract

By using the order rearrangement of the single photon sequence and unitary transformations, a multiparty controlled quantum communication scheme for Carrier Sense Multiple Access with Collision Detection(CSMA/CD) is presented .In this scheme, messages can only be recovered by the receivers with the permission of all controllers .It is shown that the security of messages transformation can be ensured and the performance of the proposed scheme enhances significantly since the collision can be avoided. In the communication network, transmitting messages from source to destination may traverse several intermediate nodes. For a long period of time, multiple authentications and secure communications between the sender and the receiver are needed for us to transmit messages. In the classical field, authentication provides only conditional security and classical channel cannot provide secure communication for liar detection .In the quantum field , multiple quantum entanglement pairs can be used for liar detection, In this paper, we design quantum authentication protocol and secure communication protocol by only using quantum channel . these protocols previously share a quantum key distribution to detect the dishonest node. The quantum Key distribution can promote authentication and secure communication for achieving higher liar detection probability.

Index Terms—single photon sequence, CSMA/CD, multiparty control, quantum communication

1. Introduction

Quantum Communication is one of the most remarkable applications of quantum mechanics in quantum information, including quantum key distribution(QKD)[1],quantumsecret sharing(QSS)[2-5],quantum secure direct communication (QSDC)[6-8],quantum identity authentication(QIA)[9,10],quantum encryption[11] and so on .The works on quantum communication attract much attention, and a lot of schemes have been proposed for quantum communication in theoretic research recently. In 1993, Bennett et al.[12] proposed the first quantum teleportation scheme with an unknown single-particle state. Bouwmeester et al.[13] first realized quantum teleportation experimentally in 1997.By employing the non-locality of Einstein-Podolsky-Rosen(EPR)correlation pairs and quantum teleportation, a novel quantum synchronous communication protocol to resolve the two army problem effectively is proposed in reference[14].Based on quantum entanglement correlation, Zhou[15] presented a quantum communication protocol for data link layer, in which the maximum throughput enhanced significantly and the performance of the stop-and wait protocol improved effectively. However, there are few references about how to improve the performance of the classical CSMA/CD protocol with quantum method.In this paper, we will protocol with quantum controlled quantum CSMA/CD communication scheme utilizing the order rearrangement of single photon sequence and unitary transformations. In this scheme, the security of the messages transmission can be enhanced and the receivers can recover the messages only with the permission of all controllers.

Authentication is a process that can be used to verify personal identification. In the classical field, authentication is conditionally secure. Transmitting message in the classical channel cannot guarantee secure communication. In the quantum field , quantum channel is based on the laws of physics such as de-coherence time, no-cloning theorem, uncertainty principle and quantum teleportation. These physical properties make quantum channel more secure than the classical channel.In the wired communication network, the Byzantine general problem [1] was discussed on how to reach agreement and the Byzantine system [2] was focused on fault detection. To reach agreement and to detect fault component, we need more message exchange and routing path. Authentication and secure communication can be used to achieve these purposes quickly. In the quantum wireless environment, the quantum routing mechanism [5] can be established in the quantum wireless network. We can use this quantum routing path to do authentication and lair detection. To consider authentication, Barnum et al. [3] proposed a secure non-interactive quantum authentication scheme using multiple classical keys. Ju et al, [4] proposed an authenticating server to verify transmitter and receiver suing quantum channel and classical channel. To consider secure communication, the sharing quantum private keys [6] are able to avoid any Eve to steal entanglement pairs.In this paper, we propose a model to implement authentication and liar detection. The sender and receiver use flexible unitary operation to verify each other. Then they sue a verity of measured basis tables defined in between, as a quantum key distribution for the communication. In order to prevent any Eavesdropper attacks, we can use more qubits for authentication and secure communication. The more qubits are used for the verification, the more reliable performance can be achieved We transfer quantum information from sender to receiver by using quantum channel. This procedure needs three steps. The first step is authentication which is to verify sender and receiver themselves. The second step is secure communication which transmits messages safely from sender to receiver via several intermediate nodes. The third step is quantum data transfer which safely sends quantum information from source to destination. In order to describe this procedure, we employ three persons, Mice, Bob and Candy. Alice is the sending node and Bob is the receiver node. However Candy is the intermediate node which may be the dishonest node. Initial, Alice and Bob share N quantum pairs with entangled states as described in the following.

2. Multiparty Controlled Csma/Cd Communication Scheme

The structure of the multiparty controlled CSMA/CD communication scheme based on order rearrangement and unitary transformations is shown in Fig.1. Suppose Alice needs to send messages to Bob, Charlie and other receivers simultaneously, and the messages can only be recovered by the receivers with the agreement of all their relative controllers. Quantum controllers C_n, where n represents the number of the controllers. Eve on the channel can be detected by the validate communicators through the order rearrangement of single photon sequence and unitary transformations. If there exists Eve in the process of communication, Alice and Bob must terminate the communication and repeat the process from the beginning. Otherwise, quantum controllers n C proclaim the order of the single photon sequence and corresponding operations carried out on each photon. Suppose quantum controllers n C are believable, now let us describe the quantum communication scheme in detail as follows:

(S1) Each sending station, at leisure time, on the one hand, sets delay resend time t , quantum ACK measurement time γ [15] and sends a request frame to the bus for communication. On the other hand, each sending station prepares photon sequence M including Q photons. Suppose there are r receivers on the bus, and then the sending station divides the photon sequence M into r parts according to different messages. Each photon among M is in one of the following four states (0) , (1) and ($\pm = \frac{1}{\sqrt{2}}(0 \pm 1)$.randomly.

(S2) After hearing from Alice, the bus is to see whether it is currently available. If available, the bus feeds back the quantum ACK to the station and allows the station to send messages; if not, the bus defers the attempt until the end of the current carrier event. At the same time, quantum controllers C_n choose the appropriate value of n for each receiver and make unitary transformation I or U on each single photon.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \quad \text{............ (1)}$$

$$U = |0\rangle\langle 1| - |1\rangle\langle 0|$$

It is easy to show that the states will evolve another under the operation U , i.e.,

$$U|-\rangle = -|+\rangle, U|+\rangle = |-\rangle,$$

$$U|0\rangle = -|1\rangle, U|1\rangle = |0\rangle,$$

It doesn't matter whichever controller receives M first. Suppose the controller C_1 receivers M first, then C_1 carries

out unitary transformation H on each single photon and disorders the sequence M .

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{...............(2)}$$

It is also easy to show that the states will evolve another under the operation H , i.e.,

$$H|+\rangle = |0\rangle, H|-\rangle = |1\rangle,$$

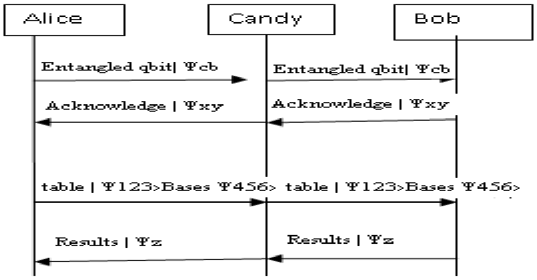
$$H|0\rangle = |+\rangle,\ H|1\rangle = |-\rangle,$$

Like C1 , C_2 carries out quantum transformation on each photon and disorders the sequence received from C_n with the same procedures, and then sends the photon sequence to the next controller C_3 . Those procedures stop at C_n . Finally, a new photon sequence Q' is generated and then sent to receivers. (S3) After receiving the sequence Q' , each receiver chooses randomly a sufficiently large subset K_i (i = 1, 2,L , r) from Q' sequence for eavesdropping check. K_1 , K_2,… , K_r correspond to Bob, Charlie and other receiver's checking sequence, respectively. Then each receiver announces the position of its checking sequence. For each checking photon, Alice chooses randomly a controller to inform each receiver of the quantum transformation H and then choose other controllers to announce their H operation in turn. Thus each receiver can choose the correct measurement basis to make measurement on his or her corresponding checking sequence and publish his or her measurement results in a classical channel.

(S4) On receiving the measurement results, quantum controllers C_n determine whether to announce the order of their relative sequence and operation information or not. If the error rate is lower than the error probability threshold set in advance, quantum controllers proclaim the relative photon sequence order and the operation information; if not, turns to (S1). (S5) Each receiver recovers the messages from the photon sequence Q' with the helps of the photon sequence order and quantum transformation information announced by their relative controllers.

3. Secure Communication Protocol

Based on the operation model, in Fig. 1, in each period time, we do secure communication before we transfer quantum qubit. The purpose of the secure communication protocol is focused on liar detection in the intermediate node.Fig.1 shows four negotiable steps which only use quantum channel to do secure communication. In the initial time, Alice and Bob previously share a quantum key distribution which includes two sequences in the measured basis. But candy can not know these sequences. The first sequence is a measured bases table set, denoted s+{s1,s2,……sx} ,where x is equal to 2n and n is the number of positive integers, where si denotes one basis table. Given an example, for n=3, the measured bases table set s={s1,s2,s3,s4,s5,s6,s7,s8} and three qubits represents one measured bases table set. We assume that qubits |000>123 represents s1.Table I denotes s1.The procedure is shown a follows.
STEP1:Prepared T1-T3 Bases Alice prepares N entanglement pairs for verification. Each entanglement pairs has three particles as follows.



F

fig.1.Secure communication steps

$$|\Psi_{acb}\rangle=1/\sqrt{2}(|000\rangle+|111\rangle)_{acb} \rightarrow (3)$$

Alice uses three types the entangled pairs which can be regarded as three measured bases. lice prepares N entanglement pairs with three particles for verification. Type I entanglement pairs can be written as

$$T1=1/\sqrt{2}(|000\rangle+|111\rangle)_{acb} \rightarrow (4)$$

Type II entanglement pairs are to rotate qubit b for π/4 along x axis, shown in the following.

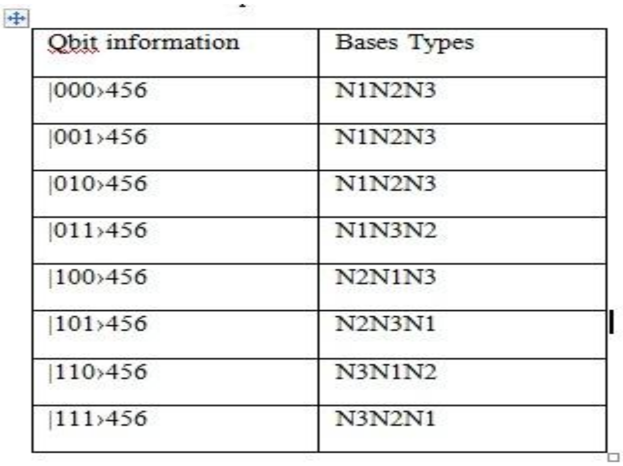
$$T2=1/\sqrt{2}(|00\rangle_{ac}(|0\rangle+|1\rangle)_b+|11\rangle_{ac}(|0\rangle-|1\rangle)_b) \rightarrow (5)$$

Type III entanglement pairs are to rotate qubit b for π/4 along y axis, shown in the following.

$$T3=1/\sqrt{2}(|00\rangle_{ac}(|0\rangle+i|\rangle)_b+|11\rangle_{ac}(|0\rangle-i|1\rangle)_b) \rightarrow (6)$$

Table 1 presents the second sequence which denotes a physical measured basis. Bob receives three qubits information|111>456, where the suffix 4 represents Candy’s measure basis and the suffix 6 represents Bob’s measured basis.To consider the Bob’s measured basis, the bases typesN1N2N3 are corresponding to the bases types T1T2T3, wherein represents the measured basis of the qubit b which is Ti.For example, Alice transfers qubits|111>456 to Bob. then Bob checks table 1 and finds N1 basis. Then Bob uses T1 as his measured basis.

Table.1.Sequence of measured basis



Qbit information	Bases Types
|000›456	N1N2N3
|001›456	N1N2N3
|010›456	N1N2N3
|011›456	N1N3N2
|100›456	N2N1N3
|101›456	N2N3N1
|110›456	N3N1N2
|111›456	N3N2N1

STEP 2: Sending Entangled Quantum Qubit

When Alice sends the entangled quantum |Ψcb> to Candy, then Candy preserves|Ψb>to Bob.

STEP 3: Sending Acknowledge Message

When bob has received all the entangled qubits from alice,all the qubits will be checked by bob. then bob sends an acknowledge message to candy. Alice and bob have previously defined which is corrective acknowledge message. We assume that is corrective acknowledge message. If Alice receives acknowledge message is not ,then Alice judges that candy is not honest.

STEP 4:Anouncing Quantum Bases

When Alice has received a acknowledge message from bob, Alice announces the type of all entangled pairs and passes all the quantum qubit information to candy. If Alice announces quantum bases in the quantum channel, bob can use this measured bases table to measure the quantum qubit correctly. Alice sends table basis set and basis element to bob. According to the agreement of measured table, bob can find the measured basis table and the measured basis element from Alice’s qubit information.

STEP 5: Checking Quantum Results

Bob transfers all the measured results to Alice by using quantum qubits only. Alice and bob can check all the measured results. If all the measured results are the same, then candy is honest. Otherwise, candy is dishonest

4. Conclusion

In summary, we provide a multiparty controlled CSMA/CD scheme for quantum communication using the order rearrangement of single photon sequence and unitary transformation. It is shown that messages can be transmitted to receivers securely at one time without revealing any information to a potential eavesdropper.Compared with the previous CSMA/CD, this new scheme has many distinct advantages. In our scheme, the collision is avoided by utilizing quantum ACK and messages can only be recovered by the receivers with the permission of all controllers, which ensures the security of message transmission and realizes message sharing. For each receiver, the controllers can be different in order to enhance the applicability of the proposed quantum communication scheme. Different messages can be sent to their respective receivers simultaneously, which improves the channel utilization. So our scheme is a more efficient and feasible one with current techniques.

References

[1] F.G.Deng and G.L.Long, "Controlled order rearrangement encryption for quantum key distribution," phys.Rev.A,vol.68,pp.042311-042315,October 2003.

[2] G.P.Guo and G. C. Guo, "Quantum secreat sharing without entanglement, "Phys, Lett . A,vol.310, pp.247-251,April2003.

[3] Z.J.Zhang and Z. X. Man, "Multiparty quantum quantum secret sharing,"Phys.Rev.A,vol.71,pp.04430-044304,April2005.

[4] P.Huang N.R. Zhou, and Y.Liu,"Secret sharing protocol based on multi-target quantum teleportation," Journal on Communications, vol.29, pp.114-118, March 2008.

[5] S.J. Qin,Q.Y.Wen, and F.C.Zhu,"Cryptanalysis of multiparty quantum secret sharing of quantum state using entangled states," chin,Phys.Lett.A,vol.25,pp.3351-3554,October 2006.

[6] F.G.Deng, X.H.Li, C.Y.Li, P.Zhou, and H.Y.Zhou,"Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs,"Phys.Lett.A,vol.359,pp.359-365,October 2006.

[7] Hwayean Lee,Jongin Lim, and Hyungjin Yang,"Quantum direct Communication with authentication,"phys.Lett.A,vol.73,pp.2301-2305,April 2006.

[8] J.Wang,H.Q.Chen, Q. Zhang, C. J. Tang,"Multiparty controlled quantum secure direct communication protocol,"Acta Physica Sinica,vol.56,pp.673-677,February 2007.

[9] T.Mihara," Quantum identification schemes with entanglements,"Phys.Rev.A,vol.65,pp.052361- 052364,May 2002.

[10] N. R.Zhou,G.H.Zeng, w. j. Zeng, and F.C.Zhu,"Cross-center quantum identification scheme based on teleportation and entanglement swapping,"Opt.Communication vol.254,pp.380-388,October2005.

[11] N.R.Zhou, Y.Liu,G.H.Zeng,J.xiong, and F.C.Zhu, "Novel qubit block encryption algorithm with hybrid keys,"Physica A,Vol.375,pp.693-698,March 2007.

[12] c. H. Bennett, G.Brassard, C.Crepeau, R.Jozsa,A.Peres, and Wk.Wotters,"Teleporting an unknown Quantum state via dual classical and Einstein-Podolsky-Rosen channels,"Phys.Rev.Lett.,vol.70,pp.1895-1899,March 1993.

[13] D.Bouwmeester, J. W. Pan, K. Mattle, M.Eibl, H.Weinfurter, and A.zeilinger,"Experimental quantum teleportion,"Nature, vol 390,pp.575-579,December 1997.

[14] N. R. Zhou,G.H.Zeng,F.C.Zhu, and S.Q.Liu,"The Quantum Synchronous Communication Protocol for Two-army problem,"Journal of Shanghai Jiaotong University, vol.40,pp.1885-1889,Novenber 2006.

[15] N. R.Zhou, G.H. Zeng,L.H.Gong,and S. Q. Liu," Quantum Communication protocol for data link layer based on entanglement,"Acta Physica Sinica ,vol.56,pp.5066-5070,September 2007.

[16] G. H. Zeng,Quantum Cryptography.Beijjing: Science Press,2006.

[17] K.Bostrom and T.Felbinger,"Deterministic secure direct communication using entanglement,"Phys.Rev.Lett,vol.89,pp.187902-187904,October2002.

[18] Y.D. Zhang, Principles of quantum information physics.Beijing:Science Press,2006.