Quantum Wireless Intrusion Detection Mechanism

Tien-Sheng Lin[1,2], I-Ming Tsai[1], and Sy-Yen Kuo[1]
[1]Department of the Electrical Engineering, National Taiwan University, Taipei, Taiwan
[2]Department of the International Business Management, Lan Yang Institute of Technology, ILan, Taiwan
sykuo@cc.ee.ntu.edu.tw

Abstract

The wireless communication network is unsafe topology, because an attacker can easily intercept the transmitted information. In a mobile ad hoc network, it is difficult to detect the malicious behavior; an attacker can execute man-in-the-middle attack at any part of a routing path from source to destination. In the classical field, the routing security is conditional security. To detect eavesdropper is difficult task. In the quantum field, quantum cryptography is unconditional security. This paper proposes a new concept, a collaborative working circuit, which can detect the intrusive behavior of malicious nodes in the routing path. Based on this circuit, the receiver can obtain the original quantum state of sending quantum qubits, which are produced by the sender, to detect the behaviors of malicious nodes. Based on this circuit, the secure routing path can be achieved.

Index Terms--Mobile ad hoc network, man-in-the-middle attack, eavesdropper, unconditional security, collaborative working circuit.

1. Introduction

Along with the growth of several wireless security technologies, the applications for wireless mobile devices are being developed. These applications include military, commerce or industry, and they require a secure wireless network [1]. For a mobile ad hoc network, to build a secure communication between the sender and receiver needs to solve the following problems: authentication [2], routing security [2], [3], and data security [4].

In the wireless communication network, the sender and receiver must set up a secure routing path from source to destination. To ensure the routing security of mobile ad hoc network, the system verifies a compromised node or malicious node in the routing path is not effective work, because this network is a vulnerable topology.

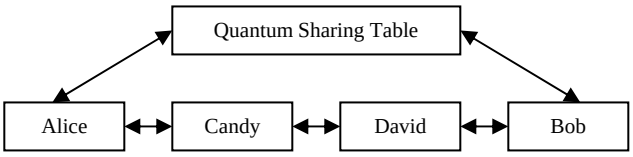

Fig.1. Connection topology.

In regard to the classical cryptography, Sun *at al.* [5] used an information theoretic framework to evaluate trust node and detect malicious behaviors in ad hoc networks. But, this mechanism has two weak points. First, this mechanism relies on the assumption that all communication channels will be secure. Second, to evaluate trust node needs multi-path recommendations from adjacent nodes. This method needs the multiple communication rounds for exchanging messages, and produces the high cost of security management.

In the quantum cryptography, the quantum channel is based on the laws of physics such as no-cloning theorem [6], uncertainty principle and quantum teleportation. Based on these properties, the quantum channel is more secure than the classical channel. In literary, Hwang *at al.* [7] used a quantum channel to eliminate eavesdropping and replay attacks. By using these properties, the quantum routing mechanism [8] teleports a quantum state from source to destination to set up the quantum routing path in the wireless communication network.

As shown in Fig. 1, at the first time, Alice and Bob are connected to previously share a series of the quantum sharing tables, which act as a secret quantum key. During a period of time, Alice and Bob are disconnected, when the mobile devices move. The transferring quantum information from Alice to Bob must pass through Candy and David. However, Candy or David may be a malicious node. Based on this situation, this paper proposes a quantum instruction detection mechanism to detect man-in-the-middle attack. Based on the secret quantum key, the sender and receiver can detect the behaviors of malicious nodes to improve the routing security.

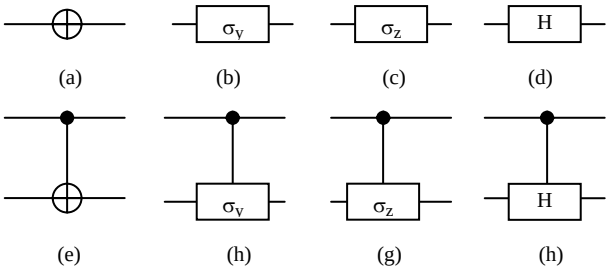

Fig.2. Symbols for related quantum gates.

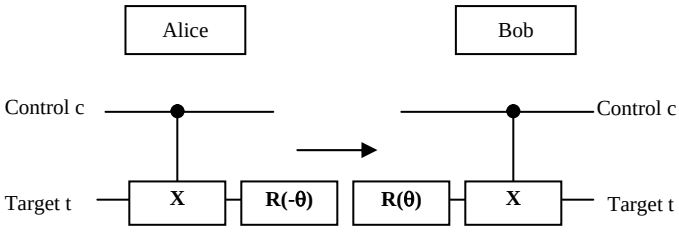

Fig.3. Quantum identification circuit.

2. Preliminaries

2.1 Quantum State and No-cloning Theorem

In a simple quantum system, a qubit can be represented as a linear combination of the two orthogonal states, denoted by state $|0\rangle$ and state $|1\rangle$. The state $|0\rangle$ represents the ground state and the state $|1\rangle$ represents the excited state. In general, a qubit state $|\psi\rangle$ can be written in the form of

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where α and β are complex numbers and $|\alpha|^2+|\beta|^2 =1$. The state $|\psi\rangle$ presents a special phenomenon of quantum mechanism, called superposition state. In general, we use Einstein-Podolsky-Rosen (EPR) pair to denote the quantum entanglement. An EPR pair in the two-qubit system can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \quad (2)$$

where A and B denote Alice and Bob, respectively.

According to the definition in [9], three types of measurement basis, $B=\{b_1, b_2, b_3\}$, are defined. The first basis is $b_1=\{|z^+\rangle, |z^-\rangle\}$ to denote the z-basis. The second basis is $b_2=\{|x^+\rangle, |x^-\rangle\}$ to denote the x-basis. The third basis is $b_3=\{|y^+\rangle, |y^-\rangle\}$ to denote the y-basis. The three measurement bases are conjugate. If we use a wrong measurement basis to measure a quantum qubit, then we have the probability 1/2 to get the wrong outcome. For example, if we use z-basis to measure a qubit derived from the basis b_2 or b_3, the error rate will be 1/2. According to the no-cloning theorem, an unknown quantum state can not duplicate.

2.2 Quantum Identification Circuit for Verification

The 'Rotation' R (θ) gate is presented as follows

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}. \quad (3)$$

The R (θ) gate is the quantum unitary gate, where $\theta \in \{0...2\pi\}$. To use the R(θ), the quantum identification operation can be preserved, i.e. $I_1=R(\theta_1)*R(\theta_2)$, where $\theta_1=-\theta_2$. Alice and Bob perform the opposite angle of the R(θ) gate on a single qubit. Another quantum unitary gate is the X gate, which could be an σ_x, σ_y, σ_z or Hadamard gate, as shown in Fig. 2(a)~2(d). The σ_x gate is the **N** gate, which can change a single qubit from $|0\rangle$ to $|1\rangle$ or from $|1\rangle$ to $|0\rangle$. This gate is called bit flip gate. The σ_y gate can flip bit and phase. The σ_z gate can leave $|0\rangle$ unchanged and flip the sign of $|1\rangle$ to $-|1\rangle$. This gate is called phase flip gate. The H gate can turn $|0\rangle$ to $|x^+\rangle$ and turn $|1\rangle$ to $|x^-\rangle$. Based on the X gate, the CX gate includes the control qubit C and the target qubit X. The CX gate could be a $C\sigma_x$, $C\sigma_y$, $C\sigma_z$ or CH gate, as shown in Fig. 2(e)~(f). For example, CN gate has not change the state of target qubit if the control qubit is in state $|0\rangle$. Otherwise, this gate flips the state of target qubit if the control qubit is in state $|1\rangle$. Based on the CX gates, the quantum identification operation can then be preserved, i.e. $I_2=CX_1*CX_2$, where $X_1=X_2$.

As shown in Fig. 3, Alice and Bob have the control qubit c and the target qubit t. The circuit system has two quantum identification operations: $I_1=R(\theta_1)*R(\theta_2)$ where $\theta_1=-\theta_2$, and $I_2=CX_1*CX_2$ where $X_1=X_2$. The verification test is to preserve the original quantum state from sender to receiver. For example, Alice prepares the control and target qubits in state $|1\rangle$ and $\alpha|0\rangle+\beta|1\rangle$, respectively. The circuit system becomes $|1\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)=\alpha|10\rangle+\beta|11\rangle$. The CX_1 and CX_2 gates are the $C\sigma_z$. Alice performs the $C\sigma_z$ gate operation and the circuit system becomes $\alpha|10\rangle-\beta|11\rangle=|1\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)$. Next, Alice performs R(-90^0) operation on the target qubit and the circuit system becomes $\beta|10\rangle+\alpha|11\rangle$. Alice sends these qubits to Bob. Then, Bob performs R (90^0) operation on the target qubit and the circuit system becomes $\alpha|10\rangle-\beta|11\rangle$. After that, Bob executes the $C\sigma_z$ gate operation on these qubits and the circuit system becomes $\alpha|10\rangle+\beta|11\rangle=|1\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)$ that is the same as Alice's original quantum states.

3. Mechanism

3.1 Quantum Sharing Table

Initially, Alice and Bob previously share a series of quantum sharing tables. The series are denoted by s= $\{s_1, s_2, ...s_x\}$, where x is equal to 2^n and n is a positive integer; and s_i denotes one quantum sharing table as described in Table I. For example, if n=3, the quantum sharing table set s=$\{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8\}$ has eight items. The table index $|\psi_{xyz}\rangle$ represents a quantum sharing table. The content index $|\psi_{123}\rangle$ points the content of this table. For example, $|\psi_{xyz}\rangle=|000\rangle$ and $|\psi_{123}\rangle=|000\rangle$ represents the first row element of the quantum sharing table s_1. Alice sends $|\psi_{xyz}\rangle$ and $|\psi_{123}\rangle$ to Bob. Alice and Bob use the same measurement basis to measure the public key: $|\psi_{xyz}\rangle$ and $|\psi_{123}\rangle$. The content of quantum sharing table is shown as follows.

- Measurement bases $b_ib_jb_k$.
- Control qubit$|\psi_c\rangle$.
- Target qubit $|\psi_t\rangle$.
- First CX gate CX_1.
- Second CX gate CX_2.
- First rotation gate $R(\theta_1)$.
- Second rotation gate $R(\theta_2)$.

The measurement bases, $b_ib_jb_k$, are used to measure the public key and the secure qubits. The symbol b_i is the measurement basis to measure the next public key. Initially, Alice and Bob have the agreement to use the measurement basis to measure the first public key. The secure qubits includes the control qubit $|\psi_c\rangle$ and the target qubit $|\psi_t\rangle$. The symbols b_j and b_k are used to measure the control qubit $|\psi_c\rangle$ and target qubit $|\psi_t\rangle$, respectively. The secure qubits are used to design the testing rules to prevent attacks from malicious node. The following quantum gates, CX_1, CX_2, $R(\theta_1)$ and $R(\theta_2)$, can preserve quantum identification operations, $I_1=R(-\theta)*R(\theta)$ and $I_2=CX_1*CX_2$.

Table I. Quantum sharing table: s_1

$\|\psi_{123}\rangle$	Bases	$\|\psi_c\rangle$	$\|\psi_t\rangle$	CX_1	CX_2	$R(\theta_1)$	$R(\theta_2)$
$\|000\rangle$	$b_1b_1b_3$	$\|z^-\rangle$	$\|y^-\rangle$	$C\sigma_z$	$C\sigma_x$	$R(90^0)$	$R(30^0)$
$\|001\rangle$	$b_2b_1b_3$	$\|z^-\rangle$	$\|y^-\rangle$	$C\sigma_x$	$C\sigma_y$	$R(60^0)$	$R(90^0)$
$\|010\rangle$	$b_1b_1b_1$	$\|z^-\rangle$	$\|z^+\rangle$	CH	$C\sigma_x$	$R(90^0)$	$R(30^0)$
$\|011\rangle$	$b_2b_2b_3$	$\|x^+\rangle$	$\|y^-\rangle$	$C\sigma_y$	$C\sigma_y$	$R(60^0)$	$R(60^0)$
$\|100\rangle$	$b_3b_1b_2$	$\|z^-\rangle$	$\|x^-\rangle$	$C\sigma_z$	$C\sigma_x$	$R(90^0)$	$R(45^0)$
$\|101\rangle$	$b_2b_2b_2$	$\|x^-\rangle$	$\|x^+\rangle$	CH	$C\sigma_x$	$R(80^0)$	$R(50^0)$
$\|110\rangle$	$b_3b_3b_1$	$\|y^+\rangle$	$\|z^-\rangle$	$C\sigma_x$	CH	$R(60^0)$	$R(40^0)$
$\|111\rangle$	$b_1b_2b_2$	$\|x^-\rangle$	$\|x^+\rangle$	CH	$C\sigma_y$	$R(90^0)$	$R(90^0)$

3.2. Collaborative Working Circuit

It needs the expensive computation to build a secure routing protocol [10] from source to destination. While Alice and Bob set up the routing path with the indirect communication, they perform quantum authentication protocol [11] to authenticate each other. In order to verify man-in-the-middle attack, the mechanism defines an honest node as follows.

Definition 1: An intermediate node is an honest node if it satisfies the following conditions:

1). Transferring quantum information is honest.
2). Performing the quantum circuit is honest.
3). The cheating rate is less than the threshold.

In order to confirm an honest node, the mechanism uses the threshold to verify an honest node. The cheating rate is defined as the probability that an attacker's behavior is success. When the above first and second conditions are satisfied, the cheating rate is less than the threshold to denote an honest node. Otherwise, this node is a dishonest node. Fig. 4 illustrates the procedure shown as follow.

- Sending quantum information.
- Performing the circuit.
- Verifying the testing rules.

For sending quantum information, Alice sends the public key to Bob via Candy and David. According to the public key, Alice and Bob send the related quantum information, as shown in Fig. 4, to David and Candy. Four nodes, Alice, Bob, Candy and David, have the agreement to use the measurement outcome that can differentiate different quantum gate. Furthermore, Alice prepares the secure qubits and performs the related quantum operations on these qubits. After that, Alice sends these qubits to Candy. With the same procedure, Candy and David execute the related quantum operations, and David sends these qubits to Bob. Bob performs the related quantum operations and uses the correct measurement bases to measure the secure qubits. By using the testing rules, Alice and Bob deduce whether Candy and David are honest or not.

STEP 1: Sending Message

As shown in Fig. 4, Alice prepares the public keys, $|\psi_{xyz}\rangle$ and $|\psi_{123}\rangle$, and sends these qubits to Bob. According to the public key, Alice finds the corresponding information of CX_2 and $R(\theta_2)$ gates, and sends them to David. As the same time, Bob finds the corresponding information of CX_1 and $R(\theta_1)$ gates and sends them to Candy. After Candy or David receives the corresponding information, then she or he sends the acknowledge message to Alice or Bob.

Fig. 5 illustrates the collaborative working circuit. The circuit system has two parts: Alice-Candy part and David-Bob part. In the Alice-Candy part, The circuit system performs two operations, $I_1=R(-\theta_1)*R(\theta_1)$ and

$I_2=CX_1*CX_1$. In the David-Bob part, The circuit system executes two quantum identification operations, $I_3=R(-\theta_2)*R(\theta_2)$ and $I_4=CX_2*\ CX_2$. For example, the public keys, $|\psi_{xyz}\rangle$ and $|\psi_{123}\rangle$, are in state $|000\rangle$ and $|100\rangle$, respectively. The secure qubits, $|\psi_c\rangle$ and $|\psi_t\rangle$, are in state $|z^-\rangle$ and $|x^-\rangle$, respectively. In addition, four quantum gates, CX_1, CX_2, $R(\theta_1)$ and $R(\theta_2)$, are $C\sigma_z$, $C\sigma_x$, $R(90^0)$ and $R(45^0)$, respectively.

STEP 2: Quantum Operations by Alice

As shown in Fig. 5, Alice performs $C\sigma_z$ operation on the qubits, c=$|z^-\rangle$ and t=$|x^-\rangle$, and the circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|10\rangle+|11\rangle)_{ct}. \tag{4}$$

Next, Alice executes the $R(-90^0)$ gate operation on the qubit s. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(-|10\rangle+|11\rangle)_{ct}. \tag{5}$$

Alice then sends two qubits, c and t, to Candy.

STEP 3: Quantum Operations by Candy

After receiving c and t qubits from Alice, Candy executes two quantum operations. First is the $R(90^0)$ gate operation on the target qubit t. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|10\rangle+|11\rangle)_{ct}. \tag{6}$$

Second is the $C\sigma_z$ gate operation on the secure qubits. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|10\rangle-|11\rangle)_{ct}. \tag{7}$$

Candy then sends two qubits, c and t, to David.

STEP 4: Quantum Operations by David

After receiving c and t qubits from Candy, David performs two quantum operations. First is the $C\sigma_x$ gate operation on the secure qubits. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|11\rangle-|10\rangle)_{ct}. \tag{8}$$

Second is the $R(-45^0)$ gate operation on the target qubit t. The circuit system becomes

$$|\psi\rangle=-|10\rangle_{ct}. \tag{9}$$

David then sends two qubits, c and t, to Bob.

STEP 5: Quantum Operations by Bob

After receiving David's qubits, Bob executes two quantum operations. First is the $R(45^0)$ gate operation on the target qubit t. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|11\rangle-|10\rangle)_{ct}. \tag{10}$$

Second is the $C\sigma_x$ gate operation on the secure qubits. The circuit system becomes

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|10\rangle-|11\rangle)_{ct}=|z^-\rangle\otimes|x^-\rangle. \tag{11}$$

After that, Bob uses b_1 and b_2 bases to measure $|\psi_c\rangle$ and $|\psi_t\rangle$, respectively. The qubits $|\psi_c\rangle$ and $|\psi_t\rangle$ are in state $|z^-\rangle$ and $|x^-\rangle$. If all the measurement outcomes are the same as the content of the secure qubit of s_1, Bob judges that Candy and David are honest. Otherwise, Bob judges that Candy and David are dishonest. When Bob judges that Candy and David are honest nodes, Bob performs the reverse procedure that is the opposite direction of the forward procedure from Bob to Alice. The function of the reverse procedure is the same as the forward procedure. If the reverse procedure is secure, Alice and Bob check the other intermediate nodes in the routing path; otherwise, they judges that Candy and David are dishonest nodes. For example, Bob sends the public keys, $|\psi_{xyz}\rangle=|000\rangle$ and $|\psi_{123}\rangle=|111\rangle$, to Alice. Bob and Alice perform the reverse procedure from step 1 to step 5. Finally, Alice judges whether Candy and David are honest or not.

STEP 6: Verifying the Testing Rules

The testing rules are to verify whether the measurement outcomes of the secure qubits are equal to the content of quantum sharing table. As the previous example, $|\psi_c\rangle$ and $|\psi_t\rangle$ are in state $|z^-\rangle$ and $|x^-\rangle$, respectively. Then, Alice and Bob can reconstruct the original quantum states of the secure qubits. This means Candy and David honestly perform transmitted quantum information and the working circuit.

In regard to the cheating rate of the public key, eight qubits have 64 possible outcomes. Then the probability is 1/64. The probability to correctly guess CX gate is 1/4, where the CX gate has four possible outcomes. In addition, the probability to correctly guess rotation gate is 1/m, where m is the number of rotation angles. To consider the secure qubits, $|\psi_t\rangle$ and $|\psi_c\rangle$ has four possible outcomes, and this mechanism includes forward and reverse procedures. The cheating rate of the proposed mechanism is $(1/4)^{2n}$, where n is the number of communication rounds.

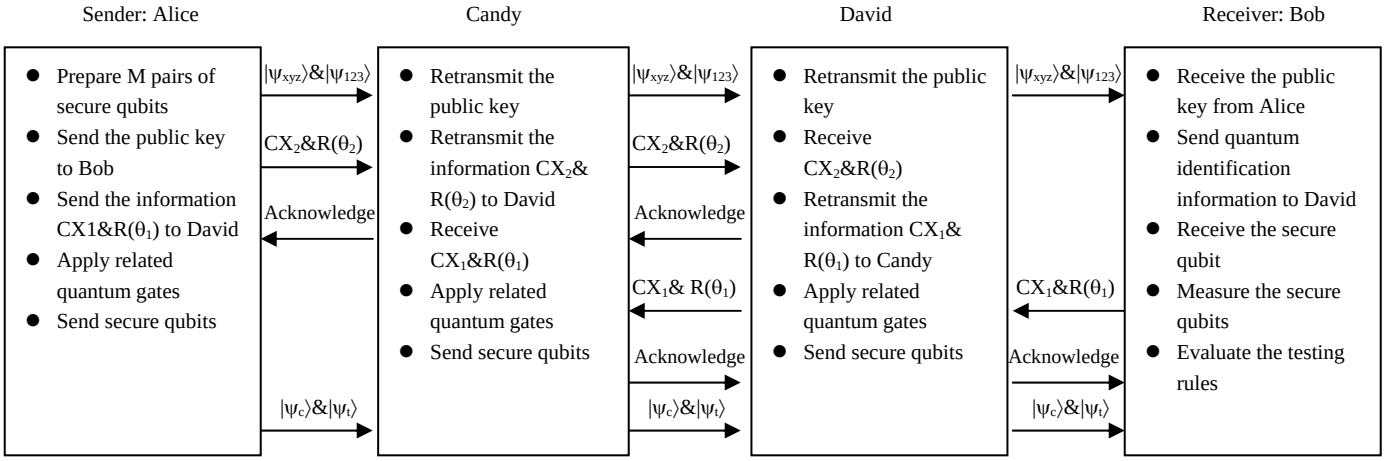

Fig. 4. The procedure of the mechanism.

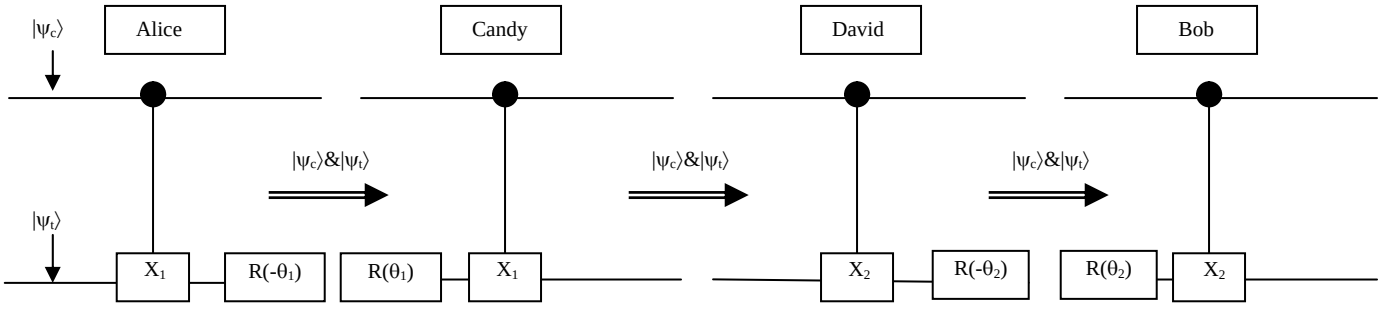

Fig. 5. The collaborative working circuit.

This mechanism uses the symbols, $E_p(i,j)$ and H_p, to denote the cheating rate of the intermediate nodes and the threshold of the collaborative working circuit, where p represents the ordinal number of routing path. To consider the $E_p(i,j)$, index i represents the total number of intermediates nodes in this path and index j represents the two adjacent nodes: j and j+1. For example, $E_1(2,1)$ represents the first routing path which has two intermediate nodes. To consider the H_p, all intermediate nodes must satisfy $E_p(i,j) \leq H_P$. For example, when the condition is satisfied, $E_1(2,1) \leq H_P$, two intermediate nodes are honest. Otherwise, Alice and Bob abort this mechanism. Based on the above mechanism, the detection circuit is used to determine whether one routing path with multiple intermediates nodes is secure or not.

4. Security Analysis

4.1 Benefit of Quantum Sharing Table

The quantum sharing table, a new secret quantum key, can not be known by any attacker, and this table is used to resist several attacks from the man-in-the-middle attacker. In the indirect communication, the man-in-the-middle attacker wants to break the routing security by using intercept-measure-resend attack. The receiver can not reconstruct the original quantum states of sending qubits, which is the same as the content of the quantum sharing table. Then, the testing rules will be broken. The receiver judges that the man-in-the-middle attacker exists in the routing path.

In order to cheat successfully in the receiver, an attacker must correctly guess the following items: the public key, the measurement bases, the CX gates and the rotation gates. To consider the public key, if an attacker sends the wrong public key, then the receiver can not find the correct content of quantum sharing table. The testing rulers will be broken. To consider the measurement bases, an attacker uses the wrong measurement basis to measure the secure qubits such that the measurement outcomes are wrong. To consider the CX and R(θ) gates, these quantum operations are used to produce the correct quantum states of the secure qubits. While an attacker performs incorrect quantum operations on the secure qubits, the quantum

identification circuit can not be preserved so that the receiver can not reconstruct the original quantum states of the secure qubits.

4.2 Benefit of Detection Circuit

Compared with the classical mechanism [5], the detection circuit efficiently verifies whether Candy and David are honest or not. This circuit only needs two communication rounds: sending quantum information and performing the circuit. Based on the quantum channel, transmitting quantum information is secure. In regard to prevent the malicious node, Candy and David perform the collaborative working circuit for sending the secure qubits. If Candy or David can not honestly carry out the related quantum operations, the testing rules for the secure qubits can not be satisfied. Then the routing security can not be achieved.

4.3 Security Capability

Based on the quantum channel, the proposed mechanism can resist eavesdropping. In advance, the quantum sharing table is unconditional secure key distribution to resist several attacks from Eve. Eve intercepts two qubits, $|\psi_c\rangle$ and $|\psi_t\rangle$. Then, he performs quantum operations on these qubits or measures these qubits. The secure qubits, $|\psi_c\rangle$ and $|\psi_t\rangle$, are selected from the orthogonal set B, and Eve can not know which is the correct measurement basis to measure these qubits. To consider the quantum error rate, the probability to guess the correct measurement basis for Eve is 1/3. The probability to detect one secure qubit for Bob is 1/2.

The purpose of the threshold H_p is used to verify whether each intermediate node is honest or not. The cheating rate for each node must less than H_p. The proposed mechanism not only increases the number of communication rounds but also uses the more secure qubits to promote the secure capability. To increase the number of communication rounds is to increase the high cost of security management. To use the more secure qubits is to add the content of the quantum sharing table. It is not a good approach to share a large quantum sharing table for mobile devices.

In the distributed environment, to set up a routing path from source to destination by using EPR pairs will face with EPR problem [8]. The sender and receiver may be far away from the EPR generator. To distribute EPR pairs and to supply EPR pairs are difficult tasks, due to the shortage EPR pairs. Therefore, the routing path for the multiple-hops hardly maintains many EPR pairs.

5. Conclusions

This paper presents the design of quantum detection circuit which can improve the routing security between source and destination. The proposed mechanism uses quantum channel and collaborative working circuit to resist man-in-the-middle attack. The testing rules based on quantum sharing table and quantum channel resist several attacks from malicious node and eavesdropper. Compared with the classical mechanism, the proposed mechanism is the low cost of security management. Furthermore, the proposed mechanism has no EPR pair problem. In the future, we will develop a secure quantum mechanism to solve the data security of mobile ad hoc network.

References

[1] H. Yang, F. Ricciato, S. Lu, and L. Zhang, "Securing a wireless world," *Proceedings of the IEEE* vol. 94, no. 2, pp. 442–454, Feb. 2006.

[2] Y.R. Tsai; and S.J. Wang, "Routing security and authentication mechanism for mobile ad hoc networks," *IEEE Conference on Vehicular Technology*, vol.7, pp. 4716 -4720. Sep 2004.

[3] K.S. Ng, and K.G. Seah, "Routing security and data confidentiality for mobile ad hoc networks," *IEEE Conference on Vehicular Technology*, vol. 3, pp.1821-1825 2003.

[4] S. Bouam, and B.O. Jalel, "Data security in ad hoc networks using multipath routing," *Proc. of the IEEE PIMRC*, vol. 2, pp. 1331-1335, 2003

[5] Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE JASC*, vol. 24, no. 2, pp. 305–316, Feb 2006.

[6] W.K. Wooters and W.H. Zurek,"A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802-803, 1982.

[7] T. Hwang, K. C. Lee, and C. M. Li, "Provably secure three-party authenticated quantum key distribution protocols," *IEEE Trans. Dependable and Secure Computing*, vol. 4, no 1, pp. 71–80, Jan-March 2007.

[8] S. T. Cheng, C. Y. Wang, and M. H. Tao, "Quantum communication for wireless wide-area networks," *IEEE JASC*, vol. 23, no. 7, pp. 1424-1432, July 2005.

[9] J. Gruska, *Quantum Computing*. Masaryk UK, McGraw-Hill Pulishing Company 1999.

[10] Y.C. Hu, and A. Perrig, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks* vol. 11, pp. 21-38, 2005.

[11] T. S. Lin, I. M. Tsai, H. W. Wang, and S. Y. Kuo, "Quantum authentication and secure communication protocols," *Proc. of the 6th IEEE Conference on Nanotechnology*, pp. 863-866, 2006.