Secure End-To-End Data Transport in Quantum Networks

Yi-Chang Shih and Hung-Yu Wei*
Department of Electrical Engineering, National Taiwan University
Corresponding Author*: hywei@cc.ee.ntu.edu.tw

Abstract—A secure end-to-end data transport protocol in quantum network is presented. A quantum network means we transport data by encoding a data into a certain quantum state on a qubit, and transmitting the qubit from sender to receiver. Because of the network scalability and physical technology limit in long distance teleportation, a fully connected quantum network model is impossible. Hence, in our quantum network model, the qubit is transported node by node to the receiver. However, this model arises two new security issues. The first is that intermediate nodes, which forward the qubit in the route, can snoop on information during the data transport. The second is that intermediate nodes can maliciously and illegally modify the transported qubit and forward it to the successor. In this paper, we present a protocol that can (1) prevent from snooping and (2) imperceptibly determine the node that maliciously modifies the transported data. By the presented protocol, we can transport information securely through the entire route in the quantum network.

Index Terms—Quantum network, Network Security, End-to-End Protocol, Quantum Teleportation, Distributed Quantum Computation.

1 Introduction

Quantum mechanics has great potential in computation and communication. The nature of superposition reduces the complexity of some algorithms, such as RSA breaking[1], disordered database searching[2], and quantum fourier transform[3]. In communication, its properties of superposition and measurement can secure data transmission and data sharing. In 1984, Bennett proposed a secure quantum key distribution (QKD)[4], that could prevent eavesdropping in the communication channel with a trade off between data transmission security and key generation rate. Other modified QKD protocols were proposed later by Bennett in 1992[5]. In 1992, Bennett proposed quantum teleportation[6] for transmitting a quantum state through a Bell state $|\beta_{00}\rangle$. The sender transmits data using the correlation of a qubit pair held by both the sender and receiver. In 2002, Bostrom and Felbinger proposed a quantum deterministic secure direct communication (QSDC) protocol that involves the entanglement of qubits. This is also called ping-pong protocol[7][8]. QSDC allows the transmission of information to be determined by the source, and hence it is very useful in data communication. These protocols served as the basis for a quantum network. The quantum network can transfer a quantum state as data through a quantum channel. However, all these studies have mainly focused on communication between adjacent nodes. They achieved success in preventing attacks by eavesdroppers in the channel between adjacent nodes, but they did not focus on the entire quantum network.

In order to achieve the quantum communication between multiple quantum nodes, we need a quantum network. Tsai and Kuo proposed a quantum switch[9]. Ratan *et al.* presented a framework for analyzing random routing in multistage interconnection networks[10]. Shi and Soljanin considered a quantum multicast mechanism in a quantum network[11]. Rodney *et al.* studied the transmission of data between nodes on the basis of teleportation, and they used different types of quantum error correction code to lower the error probability[12]. Cheng *et al.* proposed a quantum routing mechanism to deal with quantum communication for a wireless wide area network. The time complexity of communication from end to end is constant with respect to the number of nodes in the route[13]. However, the above studies did not address the security issue in the quantum network.

Intuitively, one simple secure quantum network is a fully connected quantum network, in which each node pair connects with one of the conventional quantum protocols mentioned previously [4][5][7][14]. However, as the size of quantum network increases, scalability issue needs to be taken into consideration. In this simple case, when the number of quantum nodes N increases, it is costly to link every quantum node pair because the number of links are $O(N^2)$. Hence, quantum routers or quantum repeaters may be needed to realize a quantum network with a more sophisticated network topology. Butterfly network that connects multiple transmitter and receivers with two quantum routers is one of the feasible quantum network settings [15]. In another case, quantum communications may need to go through multiple routing domains and may even be deployed under untrusted quantum network architecture [16].

Recently, experimental quantum network testbeds are created. In the DARPA Quantum Network, a 2-by-2 switch is applied to connect between 2 transmitters and 2 receivers [17]. In a generalized N-transmitter and N-receiver quantum network, connecting those transmitter and receivers with one N-by-N switch may not be easy.

Applying multiple 2-by-2 quantum switches to connect the networking nodes might be an alternative solution. Bleach of a quantum switch or quantum router may become a security threat. SeCoQC QKD network architecture is composed of multiple quantum backbone (QBB) nodes to route traffic [18]. In current SeCoQC network, the QBB nodes are assumed to be located within secure domain and have not yet considered security threats by malicious QBB node. Quantum networking traffic will be routed through multiple network domains as the size of network increases. The security threat of malicious quantum router is worth investigation.

This observation motivates us to search for a scalable secure network with $O(N)$ links. Like the classical computer network, we can solve this difficulty by a quantum network that qubits will be forwarded by intermediate quantum nodes. In this case, a new attack model occurs: an illegal intermediate node might (1) snoop on the transported data, or (2) maliciously modify the transported data. This case differs from the case of an eavesdropper in the channel. Previous works on two-party secure communication assume that both the two parties are legal, so the protocols fail in security if there is an illegal intermediate node[4], [5], [7], [14]. The network is useless without the security, so it is important to solve the new attack model. Our goal is to utilize the features of quantum mechanics, such as the uncertainty and irreversibility of measurement, to avoid this new attack mode.

It is worthy to mention why one cannot just use the network to create an end-to-end Bell pair, which can be used to teleport the data qubit in one step regardless of the number of intermediate nodes. Besides the network scalability, one main reason is the physical technology limits. To date, the distance for successful teleportation between two quantum nodes is relative short [19][20][21]. If we use end-to-end Bell pairs, the network is not scalable when the number of node increases or when we need to transport the data through a long distance up to several kilometers. Moreover, according to the physical experiment, the success rate of teleportation decreases when the distance between the two nodes increases[20][21]. Hence, one should avoid use a long distance Bell pair.

Our work is not only important to quantum network security, but also important to distributed quantum computation. Because of the physical technology limits, a single quantum computer in the recent future have only a small number of qubits, which limits the computation ability in a single quantum computer[22], [23], [24]. Distributed quantum computation combines two or more quantum computers as computing nodes to enhance the computation ability for practical problems solving[12], [22], [23], [25]. Hence, it is important that the quantum computers could be connected to form a quantum network. In this case, reliable communication in the quantum network becomes an important issue. Our work could be applied to malfunctioning quantum computer detection. The malfunctioning quantum computer performs like a malicious node when it incorrectly modifies the transmitted data in quantum computer networks, and the presented protocol can determine where it is.

To summarize, we aim to design a protocol for the secure end-to-end transportation of data. The attacker in our model is not an eavesdropper in the channel between one node and another, as in BB84 or QSDC[4], [5], [7], [8], [14]. Rather, the attacker is an illegal node in the network. We will discuss a teleportation-based quantum network model, and some attackers camouflaged as normal nodes in the network. We present a protocol for end-to-end data transport, which is secure against illegal attack in the route.

This paper is organized as follows. Section 2 briefly introduces the necessary operations in the proposed protocol. Section 3 describes the network model and defines the attackers. Section 4 proposes the first part of the protocol that protect against the attacker known as *snooper*. Section 5 proposes the second part of the protocol that protect against the attacker known as *malicious node*. Both types of attackers are described in section 3. We discuss the condition for our protocol in section 6, and present conclusions in section 7.

2 Basic operation in quantum communication

Here, we introduce basic operations and notations in quantum communication. We only introduce those operations that we use in this paper.

2.1 Quantum states and qubit

The quantum state, denoted in Dirac notation as $|\psi\rangle$, is a vector in linear space. We use this state to describe the situation of a qubit. A qubit is a physical unit with two-dimensional state space. We often use $|0\rangle$ and $|1\rangle$ as the basis of $|\psi\rangle$. Hence, the general state of a qubit is $\alpha|0\rangle + \beta|1\rangle$, where α and β are the coefficients representing the qubit's state. α and β are determined by the qubit's initial state and the quantum gates that act on the qubit. Note that $|0\rangle$ is like the zero value of a classical bit, and $|1\rangle$ is like 1.

2.2 Measurement

In the scope of this paper, we can regard a measurement as a process for determining the value of a qubit. Though a qubit can be $\alpha|0\rangle + \beta|1\rangle$, the state after measurement is either $|0\rangle$ or $|1\rangle$ with a probability $\langle 0|\psi|0\rangle = \alpha^2$ or $\langle 1|\psi|1\rangle = \beta^2$, respectively. The measurement is irreversible. The measurement results of $|0\rangle$ and $|1\rangle$ are definitely 0 and 1, respectively. We refer to this basis as a computational basis. This type of measurement is referred to as a positive operator-valued measurement (POVM). Fig. 1(a) symbolically illustrates a measurement in a quantum circuit.

2.3 Quantum gates

A quantum gate can change the state of a qubit. All quantum gates can be represented as unitary transform acting on a quantum state.

2.3.1 Bit flip gate

A bit flip gate is denoted as X, and it is shown symbolically in Fig. 1(b). It acts like not gate in a classical circuit. The matrix representation of X is

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2.3.2 Z gate

A Z gate is denoted as Z, and it is shown symbolically in Fig. 1(c). It changes the phase of a qubit. The matrix representation of Z is

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1)$$

2.3.3 Hadamard gate

A Hadamard gate is denoted as H, and it is shown symbolically in Fig. 1(d). This gate can change the computational basis to a state that has measurement result of 0 or 1 with equal probability. The matrix representation of H is

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

2.3.4 Controlled NOT gate

A controlled NOT gate is denoted as $CNOT$, and it is shown symbolically in Fig. 1(e). It is a two-input two-output gate, and its function is like that of an XOR gate in a classical circuit. The matrix representation of $CNOT$ is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (2)$$

2.3.5 Conditional X gate

Fig. 1(f) shows the symbolic representation of the conditional X gate. If the measurement result is 1, then the gate operates like an X gate on a qubit. Otherwise, the gate does not operate on the qubit. By conditional X gate we mean a single qubit gate whose operation is controlled by the action of the measurement on the other qubit. The X gate can be replaced by any other gates, such as a Z gate.

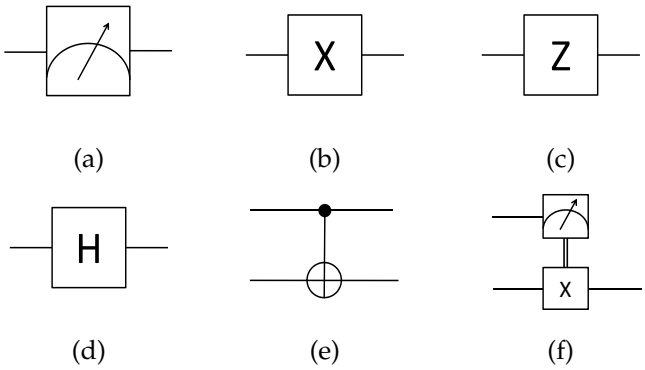

Fig. 1. Notations of basic operations in a quantum circuit. (a) Measurement, (b) bit flip gate, (c) Z gate, (d) Hadamard gate, (e) control not gate, and (f) conditional X gate.

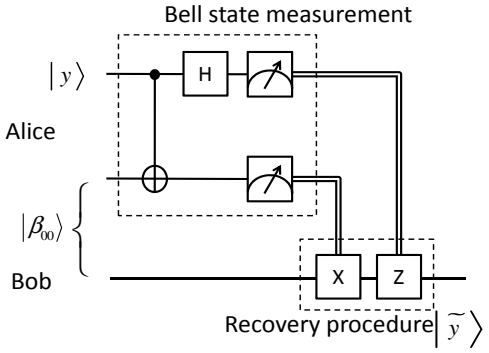

Fig. 2. Scheme for conventional quantum teleportation.

3 Network Model Based on Conventional Quantum Teleportation

3.1 Conventional quantum teleportation

Fig. 2 presents the scheme for conventional quantum teleportation. The sender Alice shares a Bell state $|\beta_{00}\rangle$ as a channel with the receiver Bob. The data bit is $|y\rangle$. Alice performs the following steps to transmit her data $|y\rangle$ to Bob.

1) Alice applies the $CNOT$ gate to the data bit $|y\rangle$ and to the half of the Bell state that she possesses.
2) Alice applies the Hadamard gate to the data bit.
3) Alice makes a measurement of both the data bit and the half of the Bell state that she possesses. The above three steps are also referred to as the Bell state measurement.
4) Alice sends her measured result to Bob.
5) As shown in Fig. 2, Bob performs the corresponding operation according to Alice's measurement result to obtain the recovered state $|\tilde{y}\rangle$. $|\tilde{y}\rangle = |y\rangle$. We refer to steps 4 and 5 as the recovery procedure.

Bob can forward the state $|y\rangle$ to a successor using the same scheme. The entire teleportation process can be regarded as the combination of a Bell state measurement

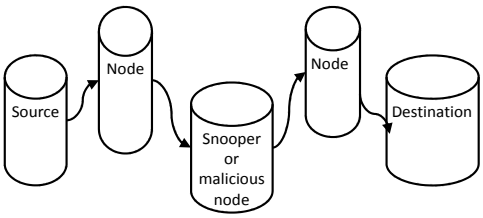

Fig. 3. Our quantum network model. The adjacent nodes are linked by Bell state for teleportation. Note that the model is at the risk of two new attack model, and is not secure.

and recovery procedure. We can transmit a quantum state using this conventional quantum teleportation protocol node by node and finally to the destination, as shown in Fig. 3. The network is almost the same as a classical network but it uses a Bell state $|\beta_{00}\rangle$ as the channel. However, this network model is obviously not secure. There might be snoopers and malicious nodes in the route that are camouflaged as normal intermediate nodes.

3.2 Definitions of attackers

The explicit definitions of attackers considered in this paper are as follow:

- *Snooper*: A snooper is a node that attempts to snoop the transported data. The data is encoded in the qubit $|y\rangle$. The snooper snoops the data by measurement on $|y\rangle$ to obtain data α and β. Notice that a snooper is different from the eavesdropper considered in most previous papers[4], [5], [7], [14]. The eavesdropper promiscuously listens to the quantum channel, while the snooper is an illegal node that snoops the transported data in the route.
- *Malicious node*: An intermediate node that attempts to modify the qubit without authorization before forwarding to the successor.

Therefore, we propose a new scheme for avoiding attacks. Specifically, we (1) prevent information α and β carried by state $|y\rangle$ from being revealed to the snooper and (2) imperceptibly determine the malicious node that modifies and forwards the qubit.

4 Protocol for the Prevention of Snooping

4.1 The scheme of the protocol

In this protocol, all the intermediate nodes, including snoopers, cannot obtain the complete state $|y\rangle$ during end-to-end data transport.

The scheme of this protocol is different for the source, the intermediate node immediately after the source, other intermediate nodes, and the destination. The procedures are elucidated as follows. The entire scheme is illustrated in Fig. 4. Notice that for clarity, we do not mark the Bell state pairs between two adjacent nodes.

Source

1) The source applies a $CNOT$ gate to both data bit $|y\rangle$ and the Bell state $|\beta_{00}\rangle$ shared with the successor. Then it applies the Hadamard gate to the data bit.
2) Instead of measuring both the data bit and the half of the Bell state held by the source in conventional teleportation, the source only measures the data bit (the qubit that carries the original information.)
3) The source sends the measurement result to all nodes.
4) Once the source receives a destination's acknowledgement (ACK), it measures the other qubit (the half of the Bell state held by the source). After measurement, the source sends the measurement result to all the nodes.

Notice that the snooper node may pretend to be the destination and may send an ACK to the source asking the measurement result of the other qubit in possession of the source. This can be used to obtain the transmitted state. To avoid this case, we can apply some standard verification technologies. For example, we can allocate different secret and private identification numbers to different nodes, and asking the destination to send ACK with its own allocated identification number. By doing this, the source can verify whether the ACK is sent by the correct destination.

Intermediate node immediately after the source

1) This first intermediate node applies the Z gate according to the measurement result from the source. This node receives part of the data instead of full data.
2) The first intermediate node makes a Bell state measurement of the received data bit and the Bell state shared with the successor. This step is a part of conventional quantum teleportation with a successor.

Other Intermediate nodes

1) Other intermediate nodes conduct the recovery procedure according to the measurement result from their predecessor. This is a part of conventional quantum teleportation with a predecessor.
2) The intermediate node makes a Bell state measurement of the received data bit and the Bell state shared with the successor. This step is a part of conventional quantum teleportation with a successor.

It should be noted that if any intermediate node does not follow this protocol, it is regarded as a malicious nodes that is modifying the qubit. Such a node is detected using the mechanism discussed in section 5.

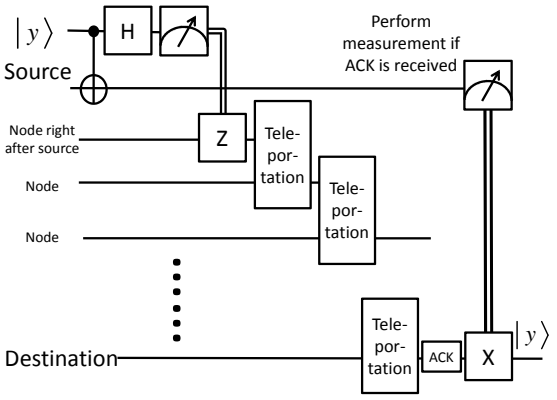

Fig. 4. Schemes for different types of nodes in the network for the prevention of snooping

Notice that the only different operation at the intermediate node right after the source, is the Conditional Z gate operation, in our current design. In theory, one can observe that the protocol is still effective even if the Conditional Z gate is operated by another intermediate node. Nevertheless, due to the physical technology limit, the Conditional Z gate is better to be operated as close to the source as possible.

Destination:

1) The destination performs the recovery procedure according to the measurement result from the predecessor.
2) It sends an ACK to the source.
3) It applies an X gate to recover the data bit according to the measurement result sent from the source.

4.2 Analysis of the protocol

In this subsection, we demonstrate how the proposed protocol prevents the snooping of data. We first decompose the quantum teleportation into three steps: the inverse Bell state $|\beta_{00}\rangle$ transform, measurement, and recovery. The main idea of the proposed scheme is to change the order of the measurement to conceal information from snoopers. The inverse Bell state transform can be regarded as the mapping in Table 1. The transform is unitary and invertible.

Assuming $|y\rangle = \alpha|0\rangle + \beta|1\rangle$, the initial state at the source is as follows.

$$|y\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)/\sqrt{2}$$

$$= \frac{\alpha}{2\sqrt{2}}(|\beta_{00}\rangle + |\beta_{10}\rangle)|0\rangle + \frac{\alpha}{2\sqrt{2}}(|\beta_{01}\rangle + |\beta_{11}\rangle)|1\rangle$$
$$+\frac{\beta}{2\sqrt{2}}(|\beta_{01}\rangle - |\beta_{11}\rangle)|0\rangle + \frac{\beta}{2\sqrt{2}}(|\beta_{00}\rangle - |\beta_{10}\rangle)|1\rangle$$

$$= \sum_{i=0,1} \frac{\alpha}{2\sqrt{2}}(|\beta_{0i}\rangle + |\beta_{1i}\rangle)|i\rangle + \frac{\beta}{2\sqrt{2}}(|\beta_{0i}\rangle - |\beta_{1i}\rangle)|\bar{i}\rangle \quad (3)$$

$$= \sum_{i=0,1} \frac{|\beta_{0i}\rangle(\alpha|i\rangle + \beta|\bar{i}\rangle)}{2\sqrt{2}} + \frac{|\beta_{1i}\rangle(\alpha|i\rangle - \beta|\bar{i}\rangle)}{2\sqrt{2}} \quad (4)$$

where $|\bar{0}\rangle = |1\rangle$ and $|\bar{1}\rangle = |0\rangle$.

We change the order of parentheses in Eq. 3 and Eq. 4 for explicit observation. After the inverse Bell state transform, all $|\beta_{ij}\rangle$ are transformed to $|ij\rangle$. Hence, the transformed state, denoted as $|\phi\rangle$, becomes

$$|\phi\rangle = \sum_{i=0,1} \frac{\alpha}{2\sqrt{2}}(|0i\rangle + |1i\rangle)|i\rangle + \frac{\beta}{2\sqrt{2}}(|0i\rangle - |1i\rangle)|\bar{i}\rangle \quad (5)$$

$$= \sum_{i=0,1} \frac{|0i\rangle(\alpha|i\rangle + \beta|\bar{i}\rangle)}{2\sqrt{2}} + \frac{|1i\rangle(\alpha|i\rangle - \beta|\bar{i}\rangle)}{2\sqrt{2}} \quad (6)$$

If the source measures both qubits it possesses (that is, does Bell state measurement), like in conventional quantum teleportation, the intermediate nodes can obtain the complete quantum state and the information α and β.

However, if the source follows the proposed protocol and measures the first bit, then from Eq. 6, the state for the source becomes

$$\begin{cases} \frac{1}{\sqrt{2}}\alpha(|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}}\beta(|10\rangle + |01\rangle) & \text{if } i = 0 \\ \frac{1}{\sqrt{2}}\alpha(|00\rangle - |11\rangle) - \frac{1}{\sqrt{2}}\beta(|10\rangle - |01\rangle) & \text{if } i = 1 \end{cases} \quad (7)$$

We neglect the state of the first bit for simplicity.

The state is transmitted to each intermediate node by teleportation. The measurement result of the intermediate node immediately after the source has an equal probability of being 0 or 1 irrespective of the values of α and β. Thus, this node cannot obtain any information α and β on the transmitted data. Notice that no intermediate node physically holds the first qubit in this state, and cannot obtain α and β by any gate or measurement.

With conventional quantum teleportation, each intermediate node has the same state correlated with the source. The proof is given in Appendix A. This means that no intermediate node can obtain information from the transmitted data. Hence, end-to-end data transportation through the entire routing path is secure, even if there is a snooper that pretends to be a normal intermediate node.

Unlike conventional quantum teleportation, the proposed protocol does not transmit all information to the intermediate nodes, but transmits only part of the information. This can prevent intermediate nodes from obtaining the full information. The intermediate nodes perform conventional quantum teleportation and forward the data bit to their successors, and the state is finally transmitted to the destination. When the destination receives the state from the last intermediate node, the destination sends an ACK to the source. The source then measures the remaining qubit (the second bit in Eq. 6) and sends the measurement result to the destination through the public channel. Finally, the destination executes a corresponding unitary transform according to the source's measurement result for recovery.

TABLE 1
Inverse Bell state transform

Symbol of the input state	Input state	Output state
$\|\beta_{00}\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\|00\rangle$
$\|\beta_{01}\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}}$	$\|01\rangle$
$\|\beta_{10}\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$	$\|10\rangle$
$\|\beta_{11}\rangle$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}}$	$\|11\rangle$

There are two recovery steps in conventional quantum teleportation: X and Z gate transforms. In our protocol, we apply the Z gate immediately after the measurement. Notice that the order of recovery steps in conventional quantum teleportation and our protocol is different. Nevertheless, switching the order of X and Z does not affect the result since

$$XZ = -ZX. \tag{8}$$

Switching the order of these two operations only generates a global phase shift, which has no effect on the transmitted information.

5 Protocol for Determining a Malicious Node

We have so far suggested a scheme that conceals information from intermediate nodes. However, malicious nodes can modify data received from a predecessor and forward it to the successor. In this case, although malicious node obtains no information from the data bit, it can sabotage the end-to-end information transmission by modification on the data bit. To avoid sabotage, we now propose the protocol for determining a malicious node.

The protocol comprises two procedures such that a source can, with a certain possibility, (1) detect if unauthorized modification occurs and (2) determine which node is the malicious node in the route once modification occurs. The two procedures are presented as below.

5.1 Procedure I: Detection of unauthorized modification

This scheme detects whether unauthorized modification occurs. In our scheme, the source sends some check bits in addition to data bit to check the malicious node. The check qubits are not sent along with the data bits. The presence of a malicious node is detected only when the source invokes Procedure-I. Notice that a regular transmission attempt, in which source is sending quantum data, is still vulnerable to malicious modifications - unlike two-party quantum teleportation. However, the source can enhance the frequency of sending check bit to enhance the probability of detecting malicious modification.

5.1.1 The scheme of the Procedure I

The steps of the proposed scheme are as follows. We will explain and analyze the protocol in section 5.1.2.

1) The source mixes the transmitted data sequence with check bits in random positions. Each check bit randomly has one of the following four states: $|A_+\rangle$, $|A_-\rangle$, $|B_+\rangle$ or $|B_-\rangle$. $|A_+\rangle$ and $|A_-\rangle$ corresponds to measurement **A**. $|B_+\rangle$ and $|B_-\rangle$ corresponds to measurement **B**. $|A_\pm\rangle$ and $|B_\pm\rangle$ are nonorthogonal with respect to each other. We will discuss more properties of $|A_+\rangle$, $|A_-\rangle$, $|B_+\rangle$ or $|B_-\rangle$ in section 5.1.2. Note that $\langle A_+|A_-\rangle = \langle B_+|B_-\rangle = 0$.
2) The source records (1) which bits are check bits and (2) the states of each check bit. The source then forwards the mixed data sequence to the first intermediate node and starts the data transport.
3) While the destination receives a certain number of qubits, the source informs receiver that which check bits are in the transmitted qubits and whether they correspond to measurement **A** or measurement **B**.
4) The destination performs the measurement **A** on a check bit if the check bit is $|A_+\rangle$ or $|A_-\rangle$ or measurement **B** if the check bit is $|B_+\rangle$ or $|B_-\rangle$. It then sends the measurement result to the source.
5) If the measurement results for the check bits from the destination differ from the record held by the source, the source knows that a malicious node has modified data qubit.
6) If a malicious node exists and modifies the data, the source turns to Procedure II–determination of the malicious node. Otherwise, the source can return to step 1 if it wants to continue the detection.

5.1.2 Analysis of Procedure I

We now analyze the detection protocol presented above.

We first explain why using two different bases, **A** and **B**. If we use only one base, say **A**, the malicious node can always perform the **A** measurement as a type of modifications on the transmitted data. In this case, although the data bits are modified, the check bits are not modified because they are eigenstates of **A**, and hence the unauthorized modification cannot be detected. A similar situation occurs if only **B** is used. Hence, we use **A** and **B** randomly.

In the following, we discuss the condition that maximizes the successful detection probability for this protocol. We assume that the malicious node modifies the data bit by measurement **A** or **B** only. This is a reasonable assumption, because the probability of a successful detection when a malicious node modifies data by **A** or **B** is less than that when modifies by any other operators. We also assume the malicious node uses **A** or **B** with equal probability. The source sends the check bits with probability P_c. This means that if the source sends N qubits, there are NP_c check bits. Each check bit is randomly one of $|A_+\rangle$, $|A_-\rangle$, $|B_+\rangle$ or $|B_-\rangle$ with equal probability.

Define P_j as the conditional probability that a modified check bit is detected as a modified bit by measurement **A** or **B** and the record kept at the source, under the condition that a malicious node modifies the transmitted data. This means that the measurement result at the destination differs from the record kept at the source. Maximizing P_j will help us achieve greater efficiency in detecting whether malicious nodes exist. P_j depends on the relation between **A** and **B**. The condition for maximizing P_j is

$$\langle A_+|B_+\rangle = \langle A_+|B_-\rangle = \langle A_-|B_+\rangle = \langle A_-|B_-\rangle = \pm\frac{1}{\sqrt{2}}. \quad (9)$$

The proof for Eq. 9 is in the Appendix B.

5.2 Procedure II : Imperceptible determination of a malicious node

In Procedure I, only the source knows of the existence of the malicious node, while the other nodes do not. The purpose of the following scheme is to determine the malicious node imperceptibly; that is, we do not want the malicious node to be aware that we already know of its existence before we identify it. The main concept of the proposed determination method is as follow.

The source is denoted as $node_0$. Assuming $node_i$ is not a malicious node, by the presented protocol, it has the ability to secretely determine whether $node_{i+1}$ is a malicious node. The determination process is imperceptible, which means that all the $node_k, k > i$, do not know the fact that the determining procedure is being executed. Once $node_i$ recognizes that $node_{i+1}$ is not the malicious node, $node_i$ asks $node_{i+1}$ to perform the same procedure to determine if $node_{i+2}$ is the malicious node. Because we assume the source is not a malicious node, we can find the malicious node in the route recursively and imperceptibly using this protocol.

To achieve this goal, we modify the teleportation process before starting the transmission. The detail of this protocol is in the following section.

5.2.1 Scheme for Procedure II

First, Bell states $|\beta_{00}\rangle$ (as a communication channel) between $node_{i+1}$ and $node_{i+2}$ are offered by $node_i$ ($\forall i \geq 0$,) irrespective of whether there is a malicious node. $Node_i$ offers Bell states mixed with some special pair (non-Bell states) as faked channels for $node_{i+1}$ and $node_{i+2}$. Each offered pair, including Bell pair and non-Bell pair, has its own specific serial number. $Node_i$ keeps a serial table, as illustrated in Table 2. A serial table denotes which pair is the Bell state and which is not, and does not let all $node_k(k > i)$ know the content of the table. Whenever $node_{i+1}$ wants to transmit a data bit to $node_{i+2}$, $node_{i+1}$ must query $node_i$ as to which pair for transmission. $Node_i$ will indicates $node_{i+1}$ which pair $node_{i+1}$ should use by indicating the serial number of the pair in the serial table. The details and steps are described as follows and illustrated in Fig. 6.

1) $Node_i$ produces three-qubit states $|P\rangle|Q\rangle|R\rangle = |\beta_{jk}\rangle|1\rangle$. In which $|Q\rangle|R\rangle$ is the special, non-Bell state mentioned above. The index jk is randomly chosen and recorded in a table with a corresponding serial number, as shown in Table 2.
2) $Node_i$ randomly mixes $|Q\rangle|R\rangle$ to the Bell states $|\beta_{00}\rangle$ for $node_{i+1}$ and $node_{i+2}$ as channels. Note that $node_i$ records the index (jk) of $|Q\rangle|R\rangle$ in a local serial table. These mixed states are nonentangled for $node_{i+1}$ and $node_{i+2}$. $Node_i$ should know which pairs are special to determine the malicious node.
3) If the system is not in the detection or determination mode (i.e., no malicious node was found in Procedure I), $node_i$ forwards the data qubit to $node_{i+1}$ and informs $node_{i+1}$ to use the Bell state $|\beta_{00}\rangle$ for transmission once it has received the query from $node_{i+1}$.
4) If the system is in the determination mode, $node_i$ transmits the state $|P\rangle$ instead of the data bit by conventional quantum teleportation, and indicates $node_{i+1}$ to use the state $|Q\rangle|R\rangle$ for transmission. Note that $node_{i+1}$ does not know that the channel it is using is not the Bell state $|\beta_{00}\rangle$.
5) $Node_i$ receives the measurement result from $node_{i+1}$ after $node_{i+1}$ sends the measurement result jk in conventional quantum teleportation. If the result jk is in accordance with the corresponding index record in the serial table that $node_i$ maintains, $node_i$ judges $node_{i+1}$ as nonmalicious node. Then $node_i$ requests $node_{i+1}$ to implement Procedure II to determine whether $node_{i+2}$ is the malicious node. If the result is not jk, then $node_i$ judges $node_{i+1}$ to be the malicious node. Thus, the malicious node is determined.
6) If $node_{i+1}$ is verified as being a normal node, then $node_{i+1}$ sends $|P\rangle$ to $node_{i+2}$ through the Bell state indicated by $node_i$ since $node_{i+1}$ has been verified as not being the malicious node. Then $node_{i+1}$ requests $node_{i+2}$ to forward the data to $node_{i+3}$ through pair $|Q\rangle|R\rangle$, which is nonentangled and denoted in the serial table of $node_{i+1}$.
7) If the source finds that no node is determined as being malicious after all nodes have been checked by their respective predecessors, the source restarts Procedure II.
8) After all detection and determination processes are complete, the source tells the destination to drop the invalid bits.

The algorithm for each node is illustrated in Fig. 5.

5.2.2 Analysis of Procedure II

We now analyze the validity, cost, and features of Procedure II.

First, we consider steps 4 and 5 in Procedure II. $Node_i$ sends state $|P\rangle$ instead of the data bit to $node_{i+1}$. The pair (channel) between $node_{i+1}$ and $node_{i+2}$ is in a nonentangled state $|Q\rangle|R\rangle$. The most important key in this protocol is that, the operation to forward $|P\rangle$ from

Determination algorithm for $node_i$
1. // check-message $\triangleq$ the order to check the successor.
2. **If** not received check-message
3. **then** forward data.
4. **Else**
5. Select a non-Bell state with serial number s.
6. Send $|P_s\rangle$ to the next node.
7. Indicate $node_{i+1}$ using $|Q_s\rangle|R_s\rangle$ to forward $P_s\rangle$.
8 **If** measured result $\neq$ index of s
9. **then** $node_{i+1}$ is the malicious node.
10. **Else**
11. send check-message to $node_{i+1}$.

Fig. 5. Algorithm for each node in the determination mode.

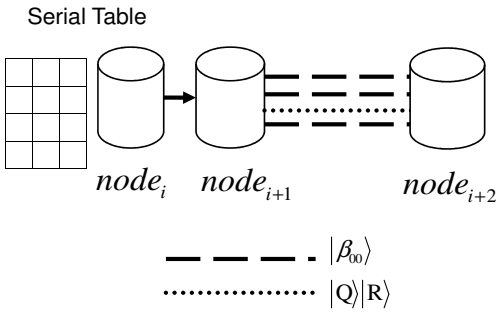

Fig. 6. Protocol for determining the malicious node.

$node_{i+1}$ to $node_{i+2}$ now is equivalent to state measurement on $|P\rangle|Q\rangle$. Because $|P\rangle|Q\rangle = |\beta_{jk}\rangle$, the measurement result (due to teleportation between $node_{i+1}$ and $node_{i+2}$) published by $node_{i+1}$ must be (j, k). Otherwise, $node_{i+1}$ definitely modifies the received qubit or publishes the incorrect result, which means that $node_{i+1}$ is the malicious node. Note that jk is known uniquely by $node_i$.

The time taken to implement Procedure II is proportional to the total number of intermediate nodes N in the worst case, which occurs when the malicious node is the last intermediate node in the route. Hence, we would use at most N bits of bandwidth for determination of the malicious node. The average bandwidth consumption is $N/2$ bits.

TABLE 2
Example of a serial table maintained by each node

Serial number	Type of channel	Index (jk)
10091	...	...
10092	Bell state	n/a
10093	non-Bell state	10
10094	non-Bell state	11
10095	Bell state	n/a
10096	...	...

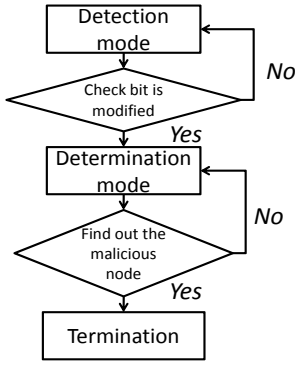

Fig. 7. The flow chart of the malicious node determination protocol.

A feature of this protocol is that the malicious node never knows that Procedure II has been implemented until the malicious node is caught by its predecessor, a nonmalicious node. While $node_i$ is checking if $node_{i+1}$ is the malicious node, $node_k (k > i)$ is not perturbed and is thus not aware of what is happening.

The publication of a fake measurement result is also prevented by this protocol, since the publication of a fake measurement result is a type of modification and sabotage. The probability of a successful determination P_s is dependent on the level of modification. The malicious node is at a relatively high risk of being identified if it modifies the transmission excessively.

The complete procedures of the determination protocol are covered in sections 5.1 and 5.2, and are illustrated by a flow chart in Fig .7. We analyze the performance for the whole protocol in Appendix C.

6 Discussion

We proposed two schemes for implementing quantum state end-to-end secure data transport. The first scheme prevents an intermediate node from obtaining information carried by a qubit, which means that an illegal node can only sabotage the transmission. The second scheme offers a certain probability of determining which node is the malicious node imperceptibly. The probability of successful detection depends on the relation between **A** and **B** and the frequency of sending check bits.

We should have considered the imperfection in the transmission, including quantum noise, imperfect gate operation and measurement. These cases would cause confusion regarding whether a malicious node exists and whether a successor is the malicious node. The miscarriage for whether a malicious node exists result in Procedure II being implemented in error. In this case, the cost is N bits bandwidth if there are N nodes. However, if the miscarriage occurs during the implementation of Procedure II, a nonmalicious node is determined as a malicious node, and the real malicious node would

realize that Procedure II has been implemented. The malicious node would stop the sabotage of the transmission to cheat the determination process. This is a more serious problem.

One solution to alleviate the quantum noise problem is applying quantum error correction code, at the cost of the bandwidth consumption. To analyze the effect of imperfect gate operation and measurement, we can apply a probabilistic model. Given the success rate of each operation and measurement, we can calculate the success rate of the protocol with a probabilitic model.

Another interesting issue is the collusion attack that two or more malicious nodes work together to attack the system. For example, there may be two malicious nodes A and B. Malicious node A is nearer the source and simply does what a normal node does . Malicious node B is further away from the source and sabotages the transmission. When Procedure II is activated, node A can always be certified as a normal node. However, node A will tell node B that Procedure II has been activated and instructs node B to stop the sabotage. Thus node B can also escape from the determination procedure. We cannot determine the malicious node in this situation using our protocol. This is due to the restriction that our determination procedure always starts at the source. A security mechanism that is resistant to collusion attack is still an open problem.

The cost of bandwidth in the determination procedure is proportional to the total number of intermediate nodes N. The total bandwidth cost would be high if the number of intermediate nodes were to increase. We will try to solve this situation in our future work.

To determine the malicious node imperceptibly, the channel of the Bell state is offered by the predecessor. This is inconvenient if all the nodes are in a line. The node offering the channel needs to transport the qubit to the next two nodes. A slightly better solution is that $node_i$, which offers the pair, teleports the channel pair to $node_{i+1}$. Then, $node_{i+1}$ teleports half of the pair to $node_{i+2}$. However this costs an extra Bell state pair.

7 Conclusion

We propose a protocol for end-to-end transportation of the quantum state, via more than one intermediate node. The proposed protocol comprises two schemes, which are described in sections 4 and 5. The first scheme avoids the leakage of information to the intermediate nodes. The second scheme determines a malicious node that tries to sabotage the transmission by modifying the transmitted qubit and forwarding it to the successor. Our performance and bandwidth cost might not be optimal, but we can achieve the above goals imperceptibly. These protocols could be used in a quantum computer network or distributed quantum computation.

Appendix A
Proof for intermediate nodes

Here we show the transmission from one node to another using one-qubit teleportation, even when the first qubit is held by the source, and prove Eq. 7, We denote the source as S, the k^{th} intermediate node as N_k. The intermediate node immediately after the source is denoted as N_1. The state shared by the S and N_k is $|\chi_k\rangle$. Before the first teleportation, the initial state shared by S and N_1 is $|\chi_1\rangle$. After the first teleportation, the state shared by S and N_2 is $|\chi_2\rangle$. To prove the extension is valid, we first prove $|\chi_2\rangle$ = $|\chi_1\rangle$.

We verify this by considering conventional teleportation described in section 3.1 and the initial state $|\chi_1\rangle$ in Eq. 7. Here we consider the $i = 0$ case in Eq. 7.The state before the first teleportation is as follows.

$$|\chi_1\rangle \otimes \beta_{00}\rangle = \left(\frac{1}{\sqrt{2}}\alpha(|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}}\beta(|10\rangle + |01\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) \quad (10)$$

$$= \frac{1}{2}\alpha\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) + \frac{1}{2}\beta\left(|1000\rangle + |0100\rangle + |1011\rangle + |0111\rangle\right) \quad (11)$$

Notice that the first bit is held in S. The second and the third bit are held in the N_1. The fourth bit is held in the N_2. Now, we will rearrange the order of the bits in the following mathematical calculation. We change the second bit into the third position, the third bit into the fourth position, and the fourth bit into the second one. The sole purpose of this rearrangement is to make the proof clearer and readable. The rearrangement has no physical effect on the state. The representation of the rearrangement is marked by a dagger.

$$(origin)|abcd\rangle^{\dagger} = |adbc\rangle(rearrangement) \quad (12)$$

The Bell state measurement now operates on the third and fourth bit. Notice that after rearrangement, the first bit is still held by the source, the second bit is held by the N_2, the third and the fourth bit are held by the N_1.

$$\begin{aligned}(|\chi_1\rangle \otimes \beta_{00}\rangle)^{\dagger} = &\frac{1}{2\sqrt{2}}\left(\alpha(|00\rangle + |11\rangle) + \beta(|01\rangle + |10\rangle)\right)|\beta_{00}\rangle \\ &+\frac{1}{2\sqrt{2}}\left(\alpha(|01\rangle + |10\rangle) + \beta(|00\rangle + |11\rangle)\right)|\beta_{01}\rangle \\ &+\frac{1}{2\sqrt{2}}\left(\alpha(|00\rangle - |11\rangle) + \beta(|10\rangle - |01\rangle)\right)|\beta_{10}\rangle \\ &+\frac{1}{2\sqrt{2}}\left(\alpha(|01\rangle - |10\rangle) + \beta(|11\rangle - |00\rangle)\right)|\beta_{11}\rangle\end{aligned}$$

$$= \sum_{i,j=0}^{i,j=1} X_2^j Z_2^i \left(\frac{1}{2\sqrt{2}}\left(\alpha(|00\rangle + |11\rangle) + \beta(|01\rangle + |10\rangle)\right)|\beta_{ij}\rangle\right)$$

With the Bell state measurement on the third and fourth bits, and the recovery procedure on the third bit, we have following result.

$$|\chi_2\rangle = \frac{1}{\sqrt{2}}\left(\alpha(|00\rangle + |11\rangle) + \beta(|01\rangle + |10\rangle)\right) = |\chi_1\rangle$$

The state of the first and second bit is back to state $|\chi_1\rangle$. Because teleportation between nodes N_k and N_{k+1} are identical, we have $|\chi_2\rangle = |\chi_3\rangle = ... = |\chi_k\rangle = |\chi_{k+1}\rangle = ...$ for all k. Hence, $|\chi_k\rangle = |\chi_1\rangle$ for all k. Readers can prove the case $i = 1$ by following the similar procedure.

APPENDIX B
PROOF FOR OPTIMAL CONDITION

Equation 9 is proved as follows. We assume that the original state of the check bit (at the source; one of $|A_+\rangle$, $|A_-\rangle$, $|B_+\rangle$ or $|B_-\rangle$) is $|\phi_i\rangle$, and the state after modification is $|\phi_f\rangle$ (owing to modification by either measurement **A** or **B**). Each combination of $|\phi_i\rangle$ and $|\phi_f\rangle$ is a situation. We then have

$$P_j = \sum_{\text{all situation } i} P(i)P(d = 1 \mid i), \tag{13}$$

where $P(i)$ is the probability that situation i occurs. $d = 1$ means the modified bit is detected as modified, which means the measurement result of the modified bit at the destination differs from the record at the source. $P(d = 1 \mid i)$ is the conditional probability that the modified bit is detected under the condition that situation i occurs. $P(i)$ and $P(d = 1 \mid i)$ for each situation are listed in Tables 3 and 4, respectively. In these two tables, the first row is the original state of the check bit at the source, $|\phi_i\rangle$, and the first column is the state after modification by the malicious node, $|\phi_f\rangle$.

We now explain Table 3. We denote $|A_+\rangle$, $|A_-\rangle$, $|B_+\rangle$ and $|B_-\rangle$ as $|A_\pm\rangle|B_\pm\rangle$. We assume that the source chooses check bits from one of $|A_\pm\rangle|B_\pm\rangle$ with equal probabilities of $\frac{1}{4}$. Therefore, the probability that a certain situation occurs is $\frac{1}{4} \times \frac{1}{2} \times |\langle\phi_i|\phi_f\rangle|^2$. The factor $\frac{1}{4}$ comes from the fact that the source mixes $|A_\pm\rangle|B_\pm\rangle$ with equal probability . The factor $\frac{1}{2}$ comes from the fact that the malicious node performs measurement **A** or **B** with equal probability. For example, the probability of the situation that the state of a check bit is originally $|A_+\rangle$ and the malicious node modifies it to $|B_+\rangle$ is $\frac{1}{8}|\langle A_+|B_+\rangle|^2$. Similar probabilities are deduced for all the other cases.

Table 4 is more simple. For example, if $|A_+\rangle$ is modified to $|A_-\rangle$, then the probability of successful detection is 1 because the measurement result definitely differ from the record at the source. Note that the measurement depends on the original state of the check bit.

For $\forall|X\rangle$ and $|\phi_+\rangle|\phi_-\rangle$ such that $\langle\phi_+|\phi_-\rangle = 0$, there is a relation in quantum mechanics that is expressed as

$$\langle\psi|\phi_+\rangle^2 = 1 - \langle\psi|\phi_-\rangle^2 \tag{14}$$

TABLE 3
$P(i)$, the probability that a situation occurs under the condition that a malicious node modifies the transmitted data. The first row is the original state of the check bit at the source (before modification). The first column is the state after modification by the malicious node.

	A_+	A_-	B_+	B_-
A_+	1/8	0	$\frac{1}{8}\|\langle B_+\|A_+\|\rangle^2$	$\frac{1}{8}\|\langle B_-\|A_+\rangle\|^2$
A_-	0	1/8	$\frac{1}{8}\|\langle B_+\|A_-\rangle\|^2$	$\frac{1}{8}\|\langle B_-\|A_-\rangle\|^2$
B_+	$\frac{1}{8}\|\langle A_+\|B_+\rangle\|^2$	$\frac{1}{8}\|\langle A_-\|B_+\rangle\|^2$	1/8	0
B_-	$\frac{1}{8}\|\langle A_+\|B_-\rangle\|^2$	$\frac{1}{8}\|\langle A_-\|B_-\rangle\|^2$	0	1/8

TABLE 4
$P(d = 1 \mid i)$, the probability of successful detection in each situation under the condition that a malicious node modifies the transmitted data. The first row is the original state of the check bit at the source (before modification). The first column is the state after modification by the malicious node.

	A_+	A_-	B_+	B_-
A_+	0	1	$\|\langle B_-\|A_+\rangle\|^2$	$\|\langle B_+\|A_+\rangle\|^2$
A_-	1	0	$\|\langle B_-\|A_-\rangle\|^2$	$\|\langle B_+\|A_-\rangle\|^2$
B_+	$\|\langle A_-\|B_+\rangle\|^2$	$\|\langle A_+\|B_+\rangle\|^2$	0	1
B_-	$\|\langle A_-\|B_-\rangle\|^2$	$\|\langle A_+\|B_-\rangle\|^2$	1	0

From Tables 3 and 4 and Eqs. 13 and 14, we have

$$P_j = 8 \times \frac{1}{8}\langle A_+|B_+\rangle^2(1 - \langle A_+|B_+\rangle^2) \tag{15}$$

From Eq. 15, the condition for maximizing $P_j$is

$$\langle A_+|B_+\rangle^2 = \frac{1}{2} \tag{16}$$

By Eqs. 14 and 16, we have the Eq. 9. Note that in the optimal case, $P_{j,max} = \frac{1}{4}$.

APPENDIX C
PERFORMANCE OF THE MALICIOUS NODE DETERMINATION PROTOCOL

We now analyze the performance of the complete protocol, which comprise Procedure I and Procedure II. We focus on the bandwidth consumption of this protocol. The notations are defined as follows.

- P_m: the probability that the malicious node modifies each data qubit.
- P_c: the probability that the source sends the check bit.
- P_j: given a modified bit is detected, the conditional probability that the check bit is a modified bit, as described section 5.1.2.
- P_s: the conditional probability that the malicious node is determined, given that Procedure II is applied.

- $P_d(i)$: the probability that the source detects a modification event until the destination receives the i^{th} bit. Notice that the source only knows a malicious node in the route, but does not know which node is malicious.
- $P_a(i)$: the probability that a malicious node is caught until the destination receives the i^{th} bit. The number of bits is counted from the beginning of Procedure II
- $S(d,a)$ the joint probability that the destination exactly receives d^{th} bits (including both data bits and check bits) in Procedure I and a bits in Procedure II.
- $M(x,N)$: the number of maliciously modified bits that are received by the destination, in the scenario where N nodes are in the route and the malicious node is the x^{th} node.
- $C(x,N)$: the total bandwidth cost, in the scenario where N nodes are in the route and the malicious node is the x^{th} node. We consider all the non-data bits as the cost (i.e., the sum of check bits in Procedure I and the bits used for determination in Procedure II).
- $\overline{M(N)} \equiv \frac{1}{N}\sum_{x=1}^{x=N} M(x,N)$: Expected value of $M(x,N)$ on x.
- $\overline{C(N)} \equiv \frac{1}{N}\sum_{x=1}^{x=N} C(x,N)$: Expected value of $C(x,N)$ on x.

The goal of performance evaluation is to find out the effectiveness and the efficiency of the protocol. The expected number of bits that are modified maliciously $\overline{M(N)}$ indicates how fast the protocol could stop the malicious operation. The expected cost $\overline{C(N)}$ indicates how efficient the efficient the protocol operates. From the definition of the joint probability for independent variables, we have

$$S(d,a) = P_d(d)P_a(a) \tag{17}$$

From the definition, the probability of a bit being detected as a modified bit is $P_mP_cP_j$ in Procedure I. The malicious node randomly modifies a data qubit with probability P_m. This could be modeled as a Bernoulli process. From definition, we have

$$P_d(i) = (1-P_mP_cP_j)^{i-1}P_mP_cP_j \tag{18}$$

The case is similar for Procedure II. But once a malicious node is safe from checking by its predecessor (with the probability $1-P_s$), it costs at least totally N bits to check the other nodes because the check process will go through the entire route. Hence,

$$P_a(i) = \begin{cases} (1-P_s)^{\frac{i-x}{N}}P_s & \text{if } \frac{i-x}{N} \in \text{integer} \\ 0 & \text{else} \end{cases} \tag{19}$$

From the definitions of $M(x,N)$ and $C(x,N)$, we sum up all the terms in all scenarios

$$M(x,N) = \sum_{d=1}^{d=\infty}\sum_{a=1}^{a=\infty} S(d,a)P_m(d+a) \tag{20}$$

and

$$C(x,N) = \sum_{d=1}^{d=\infty}\sum_{a=1}^{a=\infty} S(d,a)(P_cd+a) \tag{21}$$

Notice that the source cannot transport data bits during Procedure II because there is a malicious node in the route. Hence, all the bandwidth used in Procedure II should be considered as bandwidth cost.

Let $u = \frac{a-x}{N}$. From Eqs. 17, 18, 19, and 20, we have

$$\Rightarrow M(x,N) = P_m^2P_cP_jP_s\sum_{d=1}^{d=\infty}\sum_{u=1}^{u=\infty}(1-P_mP_cP_j)^{d-1} (1-P_s)^{u-1}(d+uN+x) \tag{22}$$

Since $\overline{x} = \frac{N}{2}$, from the definition of $\overline{M(N)}$, we compute the expected value

$$\Rightarrow \overline{M(N)} = P_m^2P_cP_jP_s\sum_{d=1}^{d=\infty}\sum_{u=1}^{u=\infty}(1-P_mP_cP_j)^{d-1} (1-P_s)^{u-1}(d+(u+\frac{1}{2})N) \tag{23}$$

Expand the last parenthesis in the last term. Then, sum over u in the first term and v in the second term. We have

$$\Rightarrow \overline{M(N)} = P_m^2P_cP_jP_s\left[\sum_{d=1}^{\infty}(1-P_mP_cP_j)^{d-1}\frac{d}{P_s}+ \sum_{u=1}^{\infty}(1-P_s)^{u-1}\frac{uN}{P_mP_cP_j}+\frac{N}{2P_mP_cP_jP_s}\right] \tag{24}$$

$$\Rightarrow \overline{M(N)} = P_m^2P_cP_jP_s\left[\sum_{d=1}^{\infty}\frac{-\partial}{P_s\partial(P_mP_cP_j)}(1-P_mP_cP_j)^{d}+ \sum_{u=1}^{\infty}\frac{-N}{P_mP_cP_j}\frac{\partial}{\partial P_s}(1-P_s)^{u}+\frac{N}{2P_mP_cP_jP_s}\right] \tag{25}$$

Reordering the partial derivative and summation operations in Eq.25, we have

$$\Rightarrow \overline{M(N)} = \frac{1}{P_cP_j}+\frac{NP_m}{P_s}+\frac{NP_m}{2} \tag{26}$$

Going through the similar calculation, we have

$$\overline{C(N)} = \frac{1}{P_mP_j}+\frac{N}{P_s}+\frac{N}{2} \tag{27}$$

In summary, the number of modified bits transported to the destination depends on the behavior of the source. The bandwidth cost depends on the behavior of the malicious node. Both of these quantities are proportional to the size of the network.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: Discrete log and factoring," *Proc. 35th Symp. Foundations of Computer Science*, pp. 124–134.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J.SCI.STATIST.COMPUT.*, vol. 26, p. 1484.

[4] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE Unternational Conference on Computers, System, and Signal.*, pp. 175–179, 1984.

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[6] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov 1992.

[7] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, no. 18, p. 187902, Oct. 2002.

[8] A. Wójcik, "Eavesdropping on the ıping-pong quantum communication protocol," *Phys. Rev. Lett.*, vol. 90, no. 15, p. 157901, Apr 2003.

[9] I.-M. Tsai and S.-Y. Kuo, "Digital switching in the quantum domain," *IEEE Transactions on Nanotechnology*, vol. 1, no. 3, pp. 154–164, Sep. 2002.

[10] R. Ratan, M. Shukla, and A. Oruc, "On random routing and its application to quantum interconnection networks," *2006 40th Annual Conference on Information Sciences and Systems*, pp. 1744–1749, Mar. 2006.

[11] Y. Shi and E. Soljanin, "On multicast in quantum networks," *40th Annual Conference on Information Sciences and Systems*, pp. 871–876, Mar. 2006.

[12] K. Van Meter, R. andNemoto and W. Munro, "Communication links for distributed quantum computation," *IEEE Transactions on Computers*, vol. 56, no. 12, pp. 1643–1653, Dec. 2007.

[13] S.-T. Cheng, C.-Y. Wang, and M.-H. Tao, "Quantum communication for wireless wide-area networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 7, pp. 1424–1432, Jul. 2005.

[14] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block," *Phys. Rev. A*, vol. 68, no. 4, p. 042317, Oct 2003.

[15] D. Leung, J. Oppenheim, and A. Winter, "Quantum network communication–the butterfly and beyond," *Arxiv preprint quant-ph/0608223*, 2006.

[16] C. Elliott, "Building the quantum network," *New Journal of Physics*, vol. 4, p. 46, 2002.

[17] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *Arxiv preprint quant-ph/0503058*, 2005.

[18] M. Dianati, R. Alléaume, M. Gagnaire, and X. Shen, "Architecture and protocols of the future European quantum key distribution network," *Security and Communication Networks*, vol. 1, no. 1, 2008.

[19] S. Olmschenk, D. Matsukevich, P. Maunz, D. Hayes, L. Duan, and C. Monroe, "Quantum teleportation between distant matter qubits," *Science*, vol. 323, no. 5913, p. 486, 2009.

[20] I. Marcikic, H. De Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Long-distance teleportation of qubits at telecommunication wavelengths," *Nature*, vol. 421, no. 6922, pp. 509–513, 2003.

[21] L.-M. Duan, M. Lukin, I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, p. 413, 2001. [Online]. Available: doi:10.1038/35106500

[22] D. K. L. Oi, S. J. Devitt, and L. C. L. Hollenberg, "Scalable error correction in distributed ion trap computers," *Physical Review A*, vol. 74, p. 052313.

[23] L. Jiang, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, "Scalable quantum networks based on few-qubit registers," 2007. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0703029

[24] A. M. Steane and D. M. Lucas, "Quantum computing with trapped ions, atoms and light," 2000. [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0004053

[25] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, "Distributed quantum computation over noisy channels," *Phys. Rev. A*, vol. 59, no. 6, pp. 4249–4254, Jun 1999.