Master's Thesis (Academic Year 2023)

Link Management in Quantum Network

Keio University Graduate School of Media and Governance
Makoto Nakai

Abstract of master's Thesis - Academic Year 20xx

Link Management in Quantum Network

Quantum networking is the new paradigm of networking that allows to transfer quantum state and achieve various new applications. RuleSet-based communication protocol is known to be one of the practical communication protocols to establish a scalable quantum network. Ideally, multiplexing and real-time resource management should be realized in order to improve the performance and robustness of the network. However, the protocol to handle multiple connections and allocate of physical links has not been proposed. This thesis proposes the link management protocol for quantum network that involves negotiation to determine a set of RuleSets (which is called a link allocation policy) to execute and the timing of apply the new link allocation policy. It also discusses the implementation of communication setup and teardown based on the proposed protocol and validates the proposed approach by performing a set of network simulations.
Keywords :
1. Quantum Networking, 2. RuleSet-Based Communication Protocol, 3. Networking Protocol,

Keio University Graduate School of Media and Governance
Makoto Nakai

Contents

1 Introduction **1**
- 1.1 Background . . . 1
- 1.2 Research Contribution . . . 2
- 1.3 Thesis Structure . . . 2

2 Background **3**
- 2.1 Quantum Physics . . . 3
  - 2.1.1 Pure State . . . 3
  - 2.1.2 Mixed State . . . 5
  - 2.1.3 Fidelity . . . 6
- 2.2 Quantum Operations . . . 7
  - 2.2.1 I Gate . . . 7
  - 2.2.2 X Gate . . . 7
  - 2.2.3 Y Gate . . . 7
  - 2.2.4 Z Gate . . . 8
  - 2.2.5 H Gate . . . 8
  - 2.2.6 Rotation Gate . . . 8
  - 2.2.7 General One Qubit Gate . . . 8
  - 2.2.8 Controlled-NOT Gate . . . 8
  - 2.2.9 Measurement . . . 9
- 2.3 Quantum Circuit . . . 9
- 2.4 Quantum Entanglement . . . 10
  - 2.4.1 Bell Pair . . . 10
  - 2.4.2 Multipartite Entanglement . . . 10
  - 2.4.3 Bell State Measurement . . . 10
  - 2.4.4 Quantum Teleportation . . . 11
  - 2.4.5 Entanglement Swapping . . . 12
  - 2.4.6 Entanglement Purification . . . 12
- 2.5 Quantum Networking . . . 13
  - 2.5.1 Quantum Node . . . 13
  - 2.5.2 Quantum Link . . . 14

3 Related Works **15**
- 3.1 Protocol Stack For Quantum Network . . . 15
- 3.2 Physical Layer Protocols For Quantum Network . . . 16

3.3 Link Layer Protocols For Quantum Network . . . 17
3.4 RuleSet-Based Quantum Network . . . 19

4 Problem Definition **20**
4.1 Problem Definition . . . 20

5 Proposal: Link Management For Quantum Network **21**
5.1 Overview . . . 21
5.2 Assumptions . . . 21
5.3 Requirements . . . 21
5.3.1 Functional requirements . . . 21
5.3.2 Non functional requirements . . . 22
5.4 Link Allocation Policy . . . 22
5.5 Link Allocation Policy Negotiation Phase . . . 22
5.6 The Timing Negotiation Phase . . . 22
5.7 Resource Management . . . 22
5.8 Messages . . . 23
5.8.1 LinkAllocationUpdateMessage . . . 23
5.8.2 BarrierMessage . . . 23
5.9 Finite State Machine For Link Allocation Policy . . . 24
5.9.1 States . . . 24
5.9.2 Events . . . 25
5.9.3 Description of Finite State Machine . . . 26
5.10 Finite State Machine For Link Management . . . 26
5.10.1 States . . . 26
5.10.2 Events . . . 27
5.10.3 Description of Finite State Machine . . . 27

6 Evaluation **28**
6.1 Experiment . . . 28
6.1.1 Two Node Network With an MM Link . . . 28
6.1.2 Two Node Network With an MIM Link . . . 28
6.1.3 Two Node Network With an MSM Link . . . 28
6.1.4 Two Node Network With an MIM Link (Without Timing Negotiation) 28

7 Conclusion **29**
7.1 Conclusion . . . 29

A Appendix **30**
A.1 The Entire Calculation To Derive The Bell Pair After Purification . . . 30

Acknowledgement **32**

List of Figures

2.1 Bloch Sphere 4
2.2 A example of quantum circuit 9
2.3 Quantum circuit for Bell state measurement 11
2.4 Quantum circuit for quantum teleportation 11
2.5 Quantum circuit for entanglement swapping 12

3.1 Message sequences in the link layer protocol in [1] 17
3.2 Message sequences in the link layer protocol in [2] 18
3.3 Message sequences in the link layer protocol in [3] 18
3.4 Connection Setup in the RuleSet-based quantum network from [3] 19

5.1 The FSM for the negotiation phase 26
5.2 The FSM for the resource management phase 27

List of Tables

2.1 A table of correspondence between measurement result and Bell pair . . . 11

3.1 Protocol Stack for Quantum Network in [1] 15
3.2 Protocol Stack for Quantum Network in [2] 16

5.1 The Message Fields in a LinkAllocationUpdateMessage 23
5.2 The Message Fields in a BarrierMessage 23

A.1 A table of correspondence between Bell pairs before and after applying a CNOT gate 30

Chapter 1

Introduction

1.1 Background

The recent development of quantum technologies such as quantum computing, quantum networking and quantum sensing are expected to provide new capabilities. For example, quantum processors can theoretically simulate quantum systems whose size are intractable even for their classical equivalence [4]. Quantum network realizes the secure generation of an encryption key [5] [6]. Quantum sensing allows the detection of sensitive physical properties such as magnetic field.[7].

Also, various applications can be realized by connecting these technologies via quantum network, such as distributed quantum computing [8], blind quantum computing [9], a precise clock synchronization [10] and improvement of the resolution of telescopes [11]

However, there are two major problems for transmitting quantum data to a distance location. One is "non-cloning theorem" [12], which is the fact that quantum state cannot be copied. Unlike classical network, it is almost impossible to neither amplify a quantum state or send it forward because the quantum state will be heavily corrupted by the high probability of loss and high error rate. The other problem is that it is so difficult to establish a Bell pair between nodes separated by a long distance, again due to a photon will be spoiled by the physical noise and photon loss.

These two problems can be solved by using particular type of nodes called quantum repeaters [13]. Quantum repeaters perform entanglement swapping [14] and purification [15], each of which extends two neighboring Bell pairs to a single longer Bell pair, and improves the fidelity of the Bell pair, respectively. These operations end up with generating an end-to-end Bell pair that can be used by quantum teleportation [16], which is the protocol to send an arbitrary quantum state to a distant location.

Entanglement swapping and purification involve requires frequent message exchange with neighboring nodes in order to coordinate actions, such as entanglement swapping and purification, with neighboring nodes and those communication slow down the generation of an end-to-end Bell pair. However, a communication protocol [17] called RuleSet-based communication protocol solves this problem by distribute an object called RuleSet, which a sequence of operations execute to each node. This feature reduces the amount of unnecessary communication and improves the scalability of the entire network.

1.2 Research Contribution

Multiple connections should be established simultaneously in order to enhance the overall performance and robustness of the entire network and the same thing can be applied to quantum network. However, the previous work only proposes the method to allocate required physical Bell pairs and establish a single end-to-end Bell pair, in other word, an single connection by consuming those physical resources. This thesis proposes a protocol to realize three important tasks, which are the negotiation about what set of connections are going to be established, the one about when to switch from those in the previous round, and coordinated resource management between two nodes connected by each link. It also discusses the updated procedure of establishing a new connection and tearing down one of the existing connections while several connections are being established by applying the proposed protocol. The approach presented in this thesis is validated by the simulation of RuleSet-based quantum networks under several circumstances.

1.3 Thesis Structure

The structure of this thesis is as follows.

Chapter 2 provides the background knowledge to understand the key concepts readers would encounter throughout this thesis.

Chapter 3 explains the detail of RuleSet-based quantum networking.

Chapter 4 presents the problem that this thesis addresses.

Chapter 5 offers the overview of the link management protocol and the messages required for its negotiation process.

Chapter **??** provides how link management protocol proposed in this thesis will be triggered after the process of connection setup and teardown. It also includes the pseudocode of methods that the node software need to execute and messages outside of the link management protocol.

Chapter 6 presents several scenarios used to validate this protocol.

Chapter 7 offers the conclusion of this thesis and discusses future works.

Chapter 2

Background

2.1 Quantum Physics

This subsection provide the fundamental knowledge of quantum physics, which will make readers feel familiar with the concept and notations that they will encounter throughout this thesis.

2.1.1 Pure State

Pure state is the representation of quantum state of the whole system without the assumption of external noise.

Quantum Bit

A conventional computer uses a bit to represent a basic unit of information, which are 0 and 1. A basic unit of quantum information, on the other hand is called a quantum bit (or **qubit** in short) are $|0\rangle$ and $|1\rangle$, each of which can be described in the form of a vector.

For example

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

The state of a single qubit $|\psi\rangle$ can be described as follows.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \, (\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$$

. After the operation called measurement, the quantum state would be collapsed into either 0 or 1. The measurement probability of 0 is $|\alpha|^2$ and that of 1 is $|\beta|^2$. In other words, a single qubit can take both states probabilistically at the same time.

For instance, a qubit can be

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{1}$$

whose measurement probability of 0 and 1 is 50% and 50% respectively.

Bloch Sphere

Because $|\alpha|^2 + |\beta|^2 = 1$, the notation of a single qubit state can be represented like this.

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2} + e^{i\phi}\sin\frac{\theta}{2})(\gamma, \phi, \theta \in \mathbb{R}) \tag{2.1}$$

.

Because $e^{i\gamma}$ is just a global state, it can be ignored and the same state can be rewritten like this.

$$|\psi\rangle = \cos\frac{\theta}{2} + e^{i\phi}\sin\frac{\theta}{2}(\phi, \theta \in \mathbb{C}) \tag{2.2}$$

Because the equation above has two parameters, any pure single qubit state can be considered as a point on the surface and its geometric representation is called **Bloch sphere**.

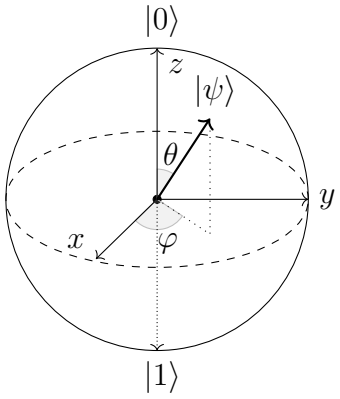

Figure 2.1: Bloch Sphere

Multi-Qubit State

The quantum state for multi-qubits is a **tensor product** of a state vector of each qubit. The general notation of two qubit state is

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \tag{2.3}$$
$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \tag{2.4}$$
$$(\alpha, \beta, \gamma, \delta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1) \tag{2.5}$$

.

For example, the state $|00\rangle$ is equal to

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{2.6}$$

.

However, some quantum states such as

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{2.7}$$

cannot be decomposed into quantum state of each qubit. These special quantum states are called **entangled** states.

2.1.2 Mixed State

Mixed state is another representation of quantum state in more general cases, such as the presense of physical error. Mixed state is described in the form of a matrix which is called density matrix. Assume quantum system takes one of their collections $\{|\psi_i\rangle\}$ (i is an index) with the probability of p_i.

Mixed State

The density matrix of this system ρ is described by

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{2.8}$$

Evolution

The quantum system after applying a unitary operator U is the following.

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger \tag{2.9}$$

Measurement

Suppose one performs measurement on a quantum state $|\psi_i\rangle$ using a measurement operator M_m.

Then, the measurement probability of m is

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = tr(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) \tag{2.10}$$

The measurement probability of m from the collection of state $\{|\psi_i\rangle\}$ is

$$\begin{aligned} p(m) &= \sum_i p_i p(m|i) \\ &= \sum_i p_i \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle \\ &= \sum_i p_i \,\mathrm{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) \\ &= \mathrm{tr}(M_m^\dagger M_m \rho) \end{aligned} \tag{2.11}$$

The quantum state after the measuring $|\psi_i\rangle$ is

$$|\psi_i^m\rangle = \frac{M_m|\psi_i^m\rangle}{\sqrt{\langle\psi_i^m|M_m^\dagger M_m|\psi_i^m\rangle}} \tag{2.12}$$

The corresponding density matrix is

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\sqrt{\langle\psi_i^m|M_m^\dagger M_m|\psi_i^m\rangle}} \tag{2.13}$$

$$\begin{aligned} p(i|m) &= \frac{p(m,i)}{p(m)} = \frac{p(m|i)p_i}{p(m)} \\ &= \frac{\mathrm{tr}(M_m^\dagger M_m\rho)p_i}{\mathrm{tr}(M_m^\dagger M_m\rho)} \\ &= p_i \end{aligned} \tag{2.14}$$

Therefore, the state can also be described by the equation

$$\begin{aligned} \rho_m &= \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m\rho)} \\ &= \frac{M_m\rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m\rho)} \end{aligned} \tag{2.15}$$

2.1.3 Fidelity

Fidelity is one of the distance between two quantum state. the fidelity of quantum state ρ and σ is

$$F(\rho,\sigma) = \mathrm{tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} \tag{2.16}$$

For instance, if they commute and diagonal in the same basis like the following,

$$\rho = \sum_i r_i|i\rangle\langle i|, \sigma = \sum_i s_i|i\rangle\langle i| \tag{2.17}$$

The fidelity between these two states would be

$$\begin{aligned} F(\rho,\sigma) &= \mathrm{tr}\sqrt{\sum_i r_i s_i|i\rangle\langle i|} \\ &= \mathrm{tr}(\sum_i \sqrt{r_i s_i}|i\rangle\langle i|) \\ &= \sum_i \sqrt{r_i s_i} \end{aligned} \tag{2.18}$$

The fidelity between a pure state $|\psi\rangle$ and a mixed state ρ is

$$\begin{aligned} F(\psi,\rho) &= \mathrm{tr}\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} \\ &= \sqrt{\langle\psi|\rho|\psi\rangle} \end{aligned} \tag{2.19}$$

2.2 Quantum Operations

2.2.1 I Gate

I gate is equal to the 2×2 identity matrix, which is

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.20}$$

.

For example,

$$I|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{2.21}$$

$$I|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{2.22}$$

.

2.2.2 X Gate

X gate

X gate flips the logical value of a qubit.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.23}$$

.

For example,

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{2.24}$$

$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{2.25}$$

.

2.2.3 Y Gate

Y gate flips the logical value of a qubit and add an imaginary number.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{2.26}$$

.

For example,

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle \tag{2.27}$$

$$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle \tag{2.28}$$

.

2.2.4 Z Gate

Z gate flips the phase of $|1\rangle$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.29}$$

.

For example,

$$Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \tag{2.30}$$

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle \tag{2.31}$$

.

2.2.5 H Gate

H gate creates superposition.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.32}$$

.

For example,

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.33}$$

$$H|1\rangle = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.34}$$

.

2.2.6 Rotation Gate

2.2.7 General One Qubit Gate

2.2.8 Controlled-NOT Gate

A CNOT gate involves two qubits, one is called **controlled qubit** and the other is called **target qubit**. If the controlled qubit is 1, the bit value of the target qubit is flipped.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.35}$$

.

For example,

$$CNOT_{0,1}|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \tag{2.36}$$

$$CNOT_{0,1}|11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \tag{2.37}$$

.

2.2.9 Measurement

Quantum measurement can be described by using a group of measurement operators $\{M_m\}$ (m is the measurement result that is expected to get). If the quantum state before measurement is $|\psi\rangle$, the measurement probability of value m is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

The quantum state after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I$$

Also, the sum of the measurement probability of each possible measurement outcome is equal to one.

$$\sum_m p(m) = \langle\psi| \sum_m M_m^\dagger M_m|\psi\rangle = 1$$

2.3 Quantum Circuit

Here is the example of a quantum circuit.

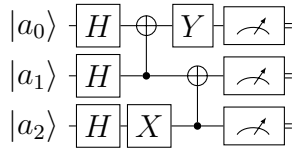

Figure 2.2: A example of quantum circuit

Each horizontal line represents each qubit and the square boxes that contain alphabets mean single quantum gates. The sign which involves a vertical line means a CNOT gate, and the box on the most right side indicates measurement.

2.4 Quantum Entanglement

Quantum entanglement is a special type of quantum state that cannot be described in the form of tensor product of the state of each particle.

2.4.1 Bell Pair

The entangled states between two qubits are called Bell pairs, and each of four states has a special notation.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.38}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.39}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.40}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.41}$$

.

2.4.2 Multipartite Entanglement

There are cases that more than two qubits are entangled and that state is called Greenberger–Horne–Zeilinger state or GHZ state.

Here is the braket notation of the GHZ state that involves three qubits.

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{2.42}$$

.

In the general case, the braket notation of the GHZ state of N qubits is the following.

$$|GHZ\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}} \tag{2.43}$$

.

2.4.3 Bell State Measurement

Bell state measurement is a special type of quantum measurement that determines which Bell pair the given two qubit entangled state is.

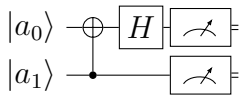

Figure 2.3: Quantum circuit for Bell state measurement

Measurement results	Bell state
00	$\|\Phi^+\rangle$
01	$\|\Phi^-\rangle$
10	$\|\Psi^+\rangle$
11	$\|\Psi^-\rangle$

Table 2.1: A table of correspondence between measurement result and Bell pair

2.4.4 Quantum Teleportation

Unlike classical communication, quantum states cannot be just copied and transmit to other nodes due to the no-cloning theorem, which forbids duplication of any quantum state. However, a method called quantum teleportation was proposed, which overcomes the restriction and allows sender to transmit single qubit state to a distant location.

This method requires both the single qubit state and a new Bell pair, and also the sender have to prepare two qubits and the receiver have to prepare one qubit. After applying a CNOT gate and an H gate in the figure above, the sender have to measure both qubits and send those measurement results over the classical network. After the receiver get those measurement results and apply some quantum gates if the measurement results of corresponding qubits on the sender's side are 1, in order to correct on the quantum state on the receiver's side.

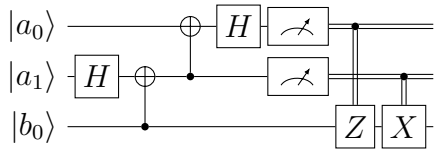

Figure 2.4: Quantum circuit for quantum teleportation

2.4.5 Entanglement Swapping

Entanglement swapping is the method to extend quantum entanglement by performing joint measurement on several quantum entanglement. For example, assume Alice has a single qubit, Bob has two qubits, and Charlie has one qubit. Then, there are Bell pairs between Alice's qubit and Bob's first qubit, and Bob's second qubit and Charlie's qubit, respectively. If Bob performs Bell state measurement on both of his qubits, Alice's qubit and Charlie's qubit are eventually entangled, even though they have not interacted with each other. This can be also seen as the teleporatation of a Bell pair by sending one of its particles. Here is the figure of quantum circuit to perform entanglement swapping.

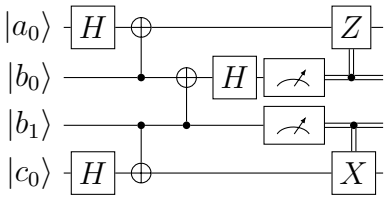

Figure 2.5: Quantum circuit for entanglement swapping

2.4.6 Entanglement Purification

Entanglement purification is a scheme to generate a set of quantum entanglements with higher fidelities from a larger set of imperfect quantum entanglements, local quantum operations, and classical communications. This procedure is also called entanglement distillation, or quantum concatenation. This section presents an example of entanglement purification that generates a single Bell pair with higher fidelity from two of those with less fidelity.

Assume Alice and Bob are supposed to share $|\Phi^+\rangle$, which is one of the Bell pairs. However, the state would be converted to the following mixed state due to the noisy nature of a quantum channel.

$$\rho_{AB} = P_{\Phi^+}|\Phi^+\rangle\langle\Phi^+| + P_{\Phi^-}|\Phi^-\rangle\langle\Phi^-| + P_{\Psi^+}|\Psi^+\rangle\langle\Psi^+| + P_{\Psi^-}|\Psi^-\rangle\langle\Psi^-|$$

$$\sum_{s\in\{\Phi^+,\Phi^-,\Psi^+,\Psi^-\}} P_s = 1$$

Any mixed state can be converted to Werner state by applying Pauli operations and $\frac{\pi}{2}$ operations, so Alice and Bob can obtain the following state.

$$\rho^{'}_{AB} = F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|)$$

Two noisy Bell pairs are required for entanglement purification. One of the Bell pair $\rho^{'}_{a_1b_1}$ is called source Bell pair, which may be purified, and the other one $\rho^{'}_{a_2b_2}$ is called target Bell pair, which is going to be measured. Then, Alice and Bob perform CNOT operations between a_1 and a_2, and b_1 and b_2, respectively. After that, they measure a_2 and

b_2 respectively, which is the qubit on the target Bell pair on their side and exchange the measurement results. If their measurement results match, the purification is successful, while they have to discard the source Bell pair and try again if those results do not match.

Here is the quantum state after measuring the target Bell pair.

$$\rho_{ab}^{'} = \frac{1}{N}\left[F^2+\frac{1}{9}\left(1-F\right)^2\right]|\Phi^+\rangle\langle\Phi^+|+\frac{2F(1-F)}{3N}|\Phi^-\rangle\langle\Phi^-|+\frac{2(1-F)^2}{9N}(|\Psi^+\rangle\langle\Psi^+|+|\Psi^-\rangle\langle\Psi^-|)$$
$$(N = F^2 + \frac{2F(1-F)}{3} + \frac{2(1-F)^2}{9})$$

The purification becomes successful if F $> \frac{1}{2}$. The readers can refer to more detailed calculation in the AppendixA.1

2.5 Quantum Networking

This section explains the important concepts of quantum networking.

2.5.1 Quantum Node

Quantum nodes are the nodes on a quantum network, which can be categorized into one of the following three categories, which was discussed in [18]

End nodes

MEAS measures the photons it receives. Although its functionality seems to be pretty limited, a pair of this node can perform quantum key distribution. In addition to that, the single node can be used as a terminal for blind quantum computation.

COMP represents quantum processor. This node also has the functionality of measuring qubits and also storing them in quantum memories.

SNS has sensing functionality by using quantum entanglement, which can be used for clock synchronization and a reference frame for interferometry.

Quantum repeaters and routers

REP1 plays a role of the 1st generation quantum repeater. It performs entanglement swapping and improves the fidelity of Bell pair by purification. The detail of each generation of quantum repeater network will be discussed in the later section.

REP2 plays a role of the 2nd generation quantum repeater. It performs entanglement swapping and perform quantum error correction on a logical qubits, which is composed of several physical qubits.

RTR behaves as the border between two different networks and also involves rewriting the given RuleSets into either 1st generation protocol and 2nd generation protocol based on what the network assumes.

Support nodes

EPPS, which stands for an entangled photon pair source, performs symmetric parametric down conversion. It creates pairs of entangled photons and send them to link end points. This node is used in terrestrial links or in satellite, which emits photons to telescopes on the ground.

BSA or Bell State Analyzer, generates a entangled state between two quantum memories by swapping two different entanglements between a single quantum memory and a single photon. The success probability of entanglement swapping with linear optics scheme does not exceed 50%.

RGSS generates multipartite photonic entangled state for memoryless quantum network. It sends each half of the generated repeater graph state to the neighboring nodes. The photons are measured at link end nodes.

ABSA performs both a single-photon measurement and two-photon measurements and their measurement basis changes based on previous measurement outcomes, logical encoding and the structure of repeater graph states.

OSW plays a role of optical switches and can exist independently or as a part of the type of nodes that are mentioned above. It switches photons from incoming links to outgoing ones.

2.5.2 Quantum Link

Quantum link is a physical Bell pair that is generated between two neighboring quantum nodes. This subsection introduces three link architectures discussed in [19].

MeetIntheMiddle

Meet-In-the-Middle, or MIM in short, collect photons from both end points of a physical link and create entanglements and send them back. Generation of these entanglements are performed in the Bell State Analyzer located in the middle.

SenderReceiver

Unlike MIM, the Bell State Analyzer is located in one of the endpoints of a physical link.

MidpointSource

EPPS in the middle performs generate entanglements and send them to the both endpoints of a physical link.

Chapter 3

Related Works

3.1 Protocol Stack For Quantum Network

This section discusses the protocol stack for quantum network. The protocol stack is a collection protocols that supports various levels of communication. Here is the comparison of the protocol stack for quantum network that are presented in the previous works.

Name	Functionality
Application	Run an application on an E2E connection
Purification Control	Perform purification to E2E connection
Entanglement Swapping Control Purification Control	Perform entanglement swapping to establish an E2E connection Perform purification to a physical bell pair
Entanglement Control	Provide robustness to the bell pair establishment
Physical Entanglement	Establish a physical bell pair

Table 3.1: Protocol Stack for Quantum Network in [1]

The work [1] is the first study that proposed the quantum protocol stack and its proposal assumes the quantum repeater protocol that manages error using entanglement purification for both a link between two neighboring nodes and an end-to-end connection between two end nodes. It has to be mentioned that this work assumes the number of hops for entanglement swapping and purification is assumed to be $N = 2^n$ (n is a positive integer) in a linear topology. Also, this work does not assume the routing functionality in any protocol layer.

Another work [2] proposes the different stack of quantum networking protocols that assumes the existence of transport layer that teleports a qubit using an end-to-end connection that is established by up to the network layer. Also, it mentions the future outlook that the functionalites of routing and entanglement management may be separated from the network layer.

Although several previous works present different protocol stacks in terms of those in the upper layer, those protocol stacks still have some common features, which are

- Establishment of an actual physical Bell pair

Name	Functionality
Application	Run an application on an E2E connection
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

Table 3.2: Protocol Stack for Quantum Network in [2]

- Robust entanglement generation
- Extension of physical bell pairs in order to establish an end-to-end Bell pair

These three elements will be the foundation of quantum network. This thesis will introduce specific protocols in the physical layer that is responsible for establishing the physical bell pair and link layer that adds robustness in the process of entanglement generation.

3.2 Physical Layer Protocols For Quantum Network

A previous work [2] proposes the communication protocol for the physical layer for two of the four different use cases of a quantum network that it defines. The protocol is called the midpoint heralding protocol (MHP) in short.

MHP for Create and Keep (CK)

Create and Keep is the use case when multiple entanglements should be stored simultaneously, such as quantum sensing [20], metrology [21] and distributed quantum computing [22]. The process of entanglement generation is triggered by the reception of the message from the link layer, which includes the following parameters.

- An ID for the entanglement generation attempt
- Generation parameters
- Qubits on the physical device which entanglements will be stored.
- The detail of microwave and laser pulse sequence

Then, the GEN message, which asks for the entanglement generation with the ID in the given message and the timestamp is sent to the support node in the middle. The support node uses the given timestamp to see if it receives the same IDs from the both side within a certain amount of time. Also, it sends a REPLY message which includes the result, which is either success or failure, the generated state, and a sequence of IDs of entangled qubits after the measurement. Then the end node performs an additional gate operation on the physical qubit depending on what state is generated, and redirected the received information to the link layer.

MHP for Measure Directly (MD)

Measure Directly is the usecase when multiple entanglements need to be created sequentially such as quantum key distribution [6] and secure identification [23]. The basic procedure is the same as the one above, but there are two main differences. One is the operations that the end nodes perform on qubits. Instead of performing additional state, it performs measurement on a specific basis. The othe one is the timing of measurement. These nodes perform these measurement only they receive successful responses.

3.3 Link Layer Protocols For Quantum Network

Communication protocols for link layer have been proposed in several previous studies [1, 2, 3]. The biggest difference between the communication protocol for the physical layer protocol and the one for the link layer is reliability. The former involves the process of actual entanglement generation and classical communication that triggers the process. On the other hand, the latter requires the additional classical communication that indicates the beginning and end of entanglement generation.

The first protocol [1] assumes that end nodes of a physical link are directly connected via an optical fiber. First of all, multiplexed optical pulses are sent to the receiver and they are demultiplexed and measured at the receiver. After several entanglements are generated, the ACK or NACK "keep" flags for each physical qubit are sent back to the sender.

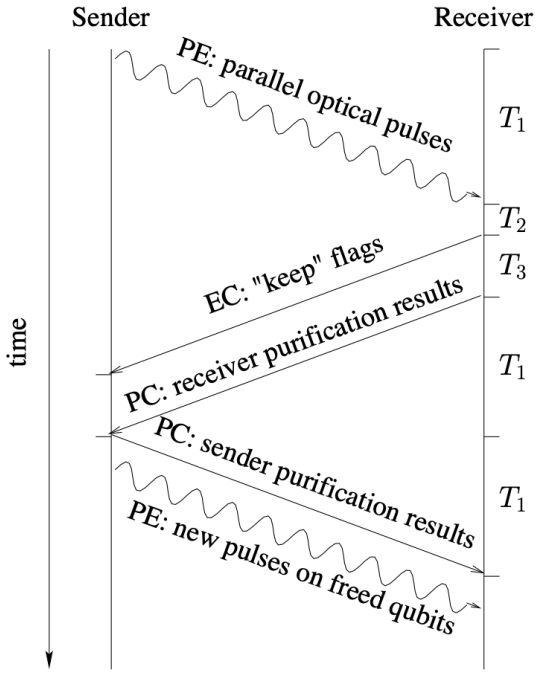

Figure 3.1: Message sequences in the link layer protocol in [1]

The next protocol [2] assumes several components, which are Distributed Queue to

store requests, Quantum Memory Management (QMM) to decide which physical qubits to use, Fidelity Estimation Unit (FEU) to estimate hardware capabilities, and Scheduler that schedules the timing of incoming requests. The link layer receives a CREATE operation from the upper networking layer with the number of entangled pairs it requires, the minimum required fidelity, and the amount of time it can wait. After that, the FEU estimates the hardware capabilities and the amount of time it would take to generate the entanglement pairs. It the request will be rejected if the estimated time exceeds the given amount of time. If it is accepted, the link layer send the "yes" response with the unique ID and the number of requested entanglement pairs.

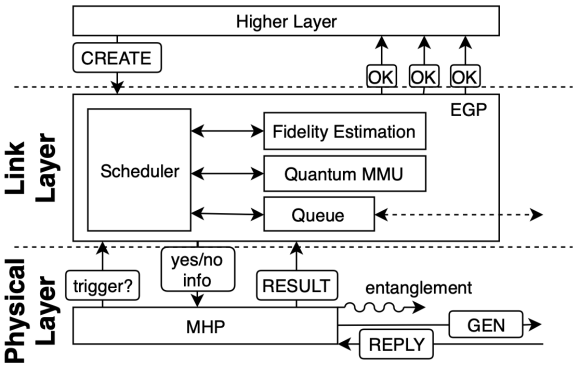

Figure 3.2: Message sequences in the link layer protocol in [2]

The last protocol [3] assumes either SendReceiver or MeetInTheMiddle for its link architecture. First of all, each end node sends Boot Up Notification to its neighboring BSA nodes. After these notifications are received, the BSA node in the middle calculates the emission timing and send it back to its neighboring end nodes. Then end nodes emit a bulk of photons and send the message to notify the end of photon emission. Lastly, the BSA node transmits the measurement results either sequentially or in batch and the message that includes the next emission timing.

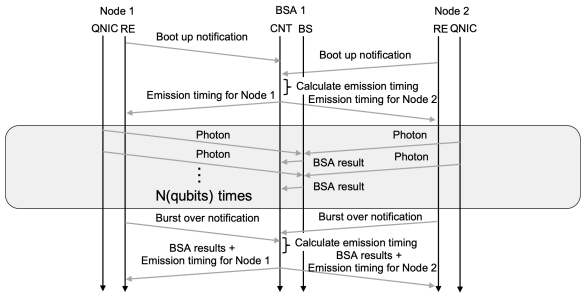

Figure 3.3: Message sequences in the link layer protocol in [3]

3.4 RuleSet-Based Quantum Network

This section explains the essential features of RuleSet-based quantum networking. Before the connection is established, the initiator sends the ConnectionSetupRequest and the information about each link along the path to the responder. After the responder receives the request, it sends the ConnectionSetupResponse and an object called RuleSet. RuleSet is a collection of Rule, which contains both one or more Condition clauses and Action clause. Condition clause is the condition to meet in order to perform a specific operation, and an Action clause is the operation itself, such as entanglement swapping and purification. Connection establishment is performed by executing the RuleSet in each node instead of performing synchronization with neighboring nodes for each operation, so that it can reduce the number of message exchange and eventually build a more scalable quantum network.

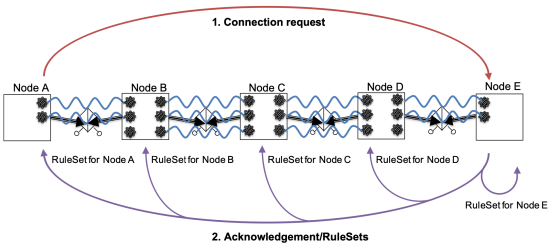

Figure 3.4: Connection Setup in the RuleSet-based quantum network from [3]

Chapter 4

Problem Definition

4.1 Problem Definition

In order to maximize the overall performance and the aggregative use of resource in the entire network, several connections are desired to be established in the real-time fashion. However, there are two major obstacles to overcome in the case of quantum network.

One is the absence of link management protocol for quantum network. There is a previous work [24] that proposes and compares the performance of various multiplexing strategies, but it does not mention any concrete methods to establish multiple connections and allocate the available physical links to each of these connections.

The other one is the lack of interaction between connection management and the subsequent resource management. The current RuleSet-based communication protocol [17] only proposes the scheme to establish a single connection and it does not explain the method to tear it down and free the allocated physical links after the end of RuleSet execution.

This thesis tackles the first problem by proposing the link management protocol the involves the negotiation about the set of connections to establish and the one about when to start the establishment. It also discuss the messages and their properties that are required to run this protocol.

Additionally, this thesis explains how the link management scheme is going to be triggered when a new connection is established and the old one is torn down. This explanation includes the methods to implement in the relevant software components when RuleSet-based quantum network is simulated or deployed in the real world.

Chapter 5

Proposal: Link Management For Quantum Network

5.1 Overview

This chapter proposes the protocol for the management of the physical Bell pairs that are available on each quantum link.

This protocol has two separated phases. The first phase is the negotiation about the set of RuleSets that are going to be established in the next round. The second phase is the negotiation about when to apply the next set of RuleSets. These negotiations will take place between the two end point of each link.

5.2 Assumptions

This protocol is proposed based on the following assumptions.

- Existence of both a classical link and quantum link between two neighboring nodes.
- No delay in transmitting messages
- No failures in nodes and links
- Transmission of classical messages each of which includes a sequence number (an incremental identifier) from a support node every time a new Bell pair is generated.

5.3 Requirements

This protocol has several requirements as follows.

5.3.1 Functional requirements

- The two end nodes of each link must coordinate what set of RuleSets and their order to execute in the next round

- The two end nodes of each link must coordinate the timing of when to execute these RuleSets

5.3.2 Non functional requirements

- This protocol must be independent from the underlying link architecture of a quantum link.

5.4 Link Allocation Policy

In order to establish multiple connections over a single link, the both end nodes of the link need to make the coordinated decisions about what connections need to be established. This set of connections, to be more specific, the set of RuleSets, would be called **Link Allocation Policy** in the rest of this thesis.

5.5 Link Allocation Policy Negotiation Phase

After the node receives a message that notifies the establishment of a new connection, or the termination of one of the existing connections, both nodes between a single link need to agree with the link allocation policy that are going to be executed in the next round. Therefore, this protocol involves the transmission of messages that include the information of the next link allocation policy in each node. It has to be mentioned that the order of arrival of RuleSets in the next policy might be different, so the protocol also requires the mechanism to determine which policy needs to be prioritized. This can be achieved by inserting a random integer to the message and adopt the order with the larger value.

5.6 The Timing Negotiation Phase

The end nodes of a physical link also need to align the timing of updating the link policy in order to assign the same Bell pair to the connection. Otherwise,they might allocate the physical qubits of two different Bell pairs, which might end up with the failure of the entire connection.

5.7 Resource Management

The actual resource allocation process needs to take place before or during the execution of the RuleSets that were determined in the previous steps. On the contrary to that, the release of physical resources that were allocated to the terminated RuleSets need to be executed after the notification of connection teardown, which the node receives from the networking layer.

5.8 Messages

This protocol involves the exchange of two kinds of messages, which are **LinkAllocationUpdateMessage** and **BarrierMessage**. This section proposes the required fields and their types in each message.

5.8.1 LinkAllocationUpdateMessage

This message contains the following fields.

Field Name	Type	Explanation
srcAddress	integer	The source address
destAddress	integer	The destination address
activeLinkAllocations	RuleSet[]	The current link allocation policy
nextLinkAllocations	RuleSet[]	The upcoming link allocation policy
randomValue	integer	A random value

Table 5.1: The Message Fields in a LinkAllocationUpdateMessage

5.8.2 BarrierMessage

This message contains the following fields.

Field Name	Type	Explanation
srcAddress	integer	The source address
destAddress	integer	The destination address
sequenceNumber	integer	A sequence number of the first available physical Bell Pair

Table 5.2: The Message Fields in a BarrierMessage

5.9 Finite State Machine For Link Allocation Policy

Finite state machine (FSM) is commonly provides a simple and clear description about the behavior of the communication protocol [25]. Each state in the finite state machine represents the condition of a communication node, its events represents the change such as transmission and reception of messages, and the action represents the reaction to the event based on the previous condition. This section explains the behavior of one of the end nodes of a link during the negotiation phase.

5.9.1 States

Init

This is the initial state that each node starts with. In this state, neither the negotiation about the upcoming link allocation policy or the one about when to update the policy are happening. The FSM transits into either LAUSnd state or LAURecv state by sending an LinkAllocationUpdateMessage or receiving the one from its neighboring nodes.

LAUSnd

This is the state when a node sends a LinkAllocationUpdateMessage to its neighboring node. In this state, a node is waiting for the incoming LinkAllocationUpdateMessage from those nodes in return, so that the FSM can move to LAUSync state by coordinating the new link allocation policy.

LAURecv

This is the state when a node receives a LinkAllocationUpdateMessage from its neighboring node. In this state, a node is about to send LinkAllocationUpdateMessages back to those nodes, so that the FSM can move to LAUSync state by coordinating the new link allocation policy.

LAUSync

This is the state when both end nodes coordinated the next link allocation policy. The FSM transits into either BarrierSnd state or BarrierRecv state if the negotiation goes successfully, otherwise it transits back to Init if they fail.

BrSnd

This is the state when a node sends a BarrierMessage to its neighboring node. In this state, a node is waiting for the incoming BarrierMessage from that node in return, so that the FSM can move to BarrierMessage state by coordinating from which Bell Pair the new link allocation policy should be applied.

BrRecv

This is the state when a node receives a BarrierMessage from its neighboring node. In this state, a node is about to send BarrierMessage back to that node, so that the FSM can move to BarrierSync state by coordinating from which Bell Pair the new link allocation policy should be applied.

BrSync

This is the state when both end nodes of a link successfully coordinated from which Bell Pair the new link allocation policy should be applied. The FSM transits to the Init state until the next negotiation about the link allocation policy becomes triggered from the networking layer.

5.9.2 Events

+LAU

This event indicates the reception of a LinkAllocationUpdateMessage.

-LAU

This event indicates the transmission of a LinkAllocationUpdateMessage.

+Br

This event indicates the reception of a BarrierMessage.

-Br

This event indicates the transmission of a BarrierMessage.

LAUSuccess

This event indicates the success in the coordination of the next link allocation policy.

LAUFail

This event indicates the failure in the coordination of the next link allocation policy.

5.9.3 Description of Finite State Machine

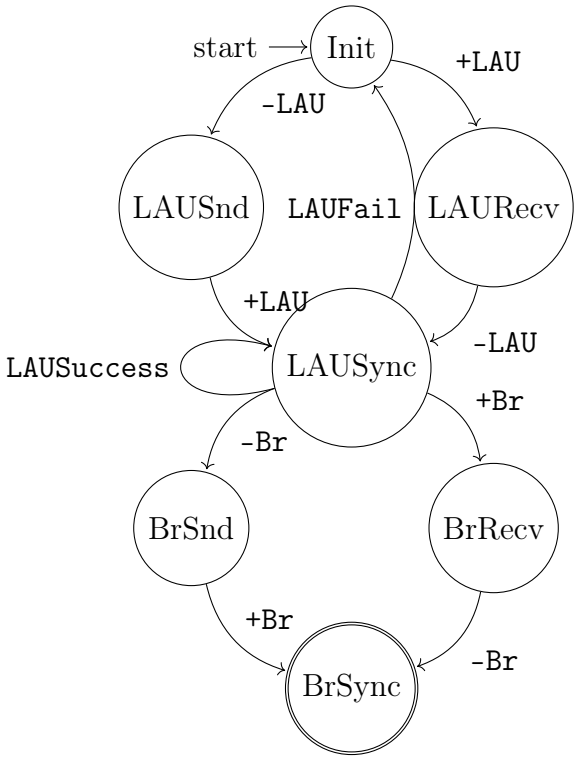

Figure 5.1: The FSM for the negotiation phase

5.10 Finite State Machine For Link Management

This section provides the different finite state machine for the link management phase. It focuses on the behavior of a single quantum link for simplicity.

5.10.1 States

Up

This is the state when a quantum link is established between its two end nodes. In this state, it is not allocated to any specific RuleSet. The FSM transits to Allocated if the link becomes allocated to one of the RuleSets in the active link allocation policy.

Down

This is the state when a quantum link is not established between its two end nodes. In this state, it can be no Bell pair between two existing quantum memories in the case of a quantum repeaters with those memories, or the situation when incoming photons have not arrived to memoryless quantum repeaters. The FSM transits to Up if a Bell pair is established.

Allocated

This is the state when a quantum link is allocated to one of the RuleSets in the active link allocation policy. The FSM transits to Up if the link becomes released after the connection that this link used to be allocated is terminated. It can also transits to Down if the physical qubits on the link are measured during execution of the RuleSet that this link is allocated to.

5.10.2 Events

BellPairGen

This event indicates the generation of a Bell pair

Allocate

This event indicates the allocation of a given Bell pair to RuleSet.

Free

This event indicates the release of an available Bell pair from that RuleSet that it is used to be allocated to.

Measure

This event indicates the measurement of two physical qubits of the given Bell pair while the RuleSet is being executed.

5.10.3 Description of Finite State Machine

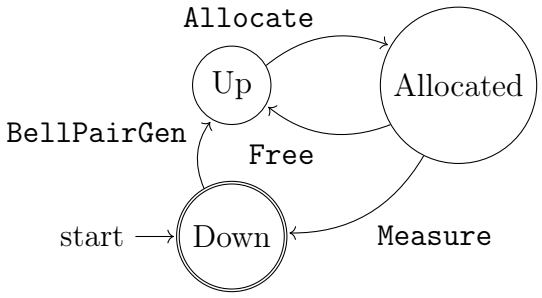

Figure 5.2: The FSM for the resource management phase

Chapter 6

Evaluation

6.1 Experiment

The author performed several experiments using QuISP (Quantum Internet Simulation Package) and demonstration of the proposed protocol in several circumstances.

6.1.1 Two Node Network With an MM Link

Both nodes coordinated both the upcoming link allocation policy and the sequence number of the first available physical entanglement pair.

6.1.2 Two Node Network With an MIM Link

Both nodes coordinated both the upcoming link allocation policy and the sequence number of the first available physical entanglement pair.

6.1.3 Two Node Network With an MSM Link

6.1.4 Two Node Network With an MIM Link (Without Timing Negotiation)

Chapter 7

Conclusion

7.1 Conclusion

This thesis proposed the link management protocol for quantum network, which provides coordinated decision about two aspects. One is the upcoming link allocation policy, which are the list of RuleSets, or operations each node needs to execute in order to establish an end-to-end connection. The other one is the particular Bell pair that the next link allocation policy should be applied to. Also, the author validated the approach by performing several simulation for a RuleSet-based quantum network.

Appendix A

Appendix

A.1 The Entire Calculation To Derive The Bell Pair After Purification

Before applying a CNOT gate	After a applying CNOT gate
$\|\Phi^+\rangle\|\Phi^+\rangle$	$\|\Phi^+\rangle\|\Phi^+\rangle$
$\|\Phi^+\rangle\|\Phi^-\rangle$	$\|\Phi^-\rangle\|\Phi^-\rangle$
$\|\Phi^+\rangle\|\Psi^+\rangle$	$\|\Phi^+\rangle\|\Psi^+\rangle$
$\|\Phi^+\rangle\|\Psi^-\rangle$	$\|\Phi^-\rangle\|\Psi^-\rangle$
$\|\Phi^-\rangle\|\Phi^+\rangle$	$\|\Phi^-\rangle\|\Phi^+\rangle$
$\|\Phi^-\rangle\|\Psi^-\rangle$	$\|\Phi^+\rangle\|\Phi^-\rangle$
$\|\Phi^-\rangle\|\Psi^+\rangle$	$\|\Phi^-\rangle\|\Psi^+\rangle$
$\|\Phi^-\rangle\|\Psi^-\rangle$	$\|\Phi^+\rangle\|\Psi^-\rangle$
$\|\Psi^+\rangle\|\Phi^+\rangle$	$\|\Psi^+\rangle\|\Psi^+\rangle$
$\|\Psi^+\rangle\|\Phi^-\rangle$	$\|\Psi^+\rangle\|\Psi^-\rangle$
$\|\Psi^+\rangle\|\Psi^+\rangle$	$\|\Psi^+\rangle\|\Phi^+\rangle$
$\|\Psi^+\rangle\|\Psi^-\rangle$	$\|\Psi^+\rangle\|\Phi^-\rangle$
$\|\Psi^-\rangle\|\Phi^+\rangle$	$\|\Psi^-\rangle\|\Psi^+\rangle$
$\|\Psi^-\rangle\|\Phi^-\rangle$	$\|\Psi^-\rangle\|\Psi^-\rangle$
$\|\Psi^-\rangle\|\Psi^+\rangle$	$\|\Psi^-\rangle\|\Phi^+\rangle$
$\|\Psi^-\rangle\|\Psi^-\rangle$	$\|\Psi^-\rangle\|\Phi^-\rangle$

Table A.1: A table of correspondence between Bell pairs before and after applying a CNOT gate

Two noisy Bell pairs are required for entanglement purification, so assume the quantum

state of the entire system can be described as follows.

$$\begin{aligned}
\rho^{'}_{a_1b_1} \otimes \rho^{'}_{a_2b_2} &= F^2|\Phi^+\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Phi^+| \\
&+ \frac{F(1-F)}{3}(|\Phi^+\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Phi^+| + |\Phi^+\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Phi^+| + |\Phi^+\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Phi^+| \\
&\quad + |\Phi^-\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Phi^-| + |\Psi^+\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Psi^+| + |\Psi^-\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Psi^-|) \\
&+ \frac{(1-F)^2}{9}(|\Phi^-\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Phi^-| + |\Phi^-\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Phi^-| + |\Phi^-\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Phi^-| \\
&\quad + |\Psi^+\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Psi^+| + |\Psi^+\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Psi^+| + |\Psi^+\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Psi^+| \\
&\quad\quad + |\Psi^-\rangle|\Phi^-\rangle\langle\Psi^-|\langle\Phi^-| + |\Psi^-\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Psi^-| + |\Psi^-\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Psi^-|)
\end{aligned}$$

One of the Bell pair $\rho^{'}_{a_1b_1}$ is called source Bell pair, which may be purified, and the other one $\rho^{'}_{a_2b_2}$ is called target Bell pair, which is going to be measured. Then, Alice and Bob perform CNOT operations between a_1 and a_2, and b_1 and b_2, respectively. The entire quantum state on this point would be as follows.

$$\begin{aligned}
\rho^{'}_{a_1b_1} \otimes \rho^{'}_{a_2b_2} &= F^2|\Phi^+\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Phi^+| \\
&+ \frac{F(1-F)}{3}(|\Phi^-\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Phi^-| + |\Phi^+\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Phi^+| + |\Phi^-\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Phi^-| \\
&\quad + |\Phi^-\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Phi^-| + |\Psi^+\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Psi^+| + |\Psi^-\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Psi^-|) \\
&+ \frac{(1-F)^2}{9}(|\Phi^+\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Phi^+| + |\Phi^-\rangle|\Psi^+\rangle\langle\Psi^+|\langle\Phi^-| + |\Phi^+\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Phi^+| \\
&\quad + |\Psi^+\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Psi^+| + |\Psi^-\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Psi^+| + |\Psi^+\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Psi^+| \\
&\quad\quad + |\Psi^-\rangle|\Psi^-\rangle\langle\Psi^-|\langle\Psi^-| + |\Psi^-\rangle|\Phi^+\rangle\langle\Phi^+|\langle\Psi^-| + |\Psi^-\rangle|\Phi^-\rangle\langle\Phi^-|\langle\Psi^-|)
\end{aligned}$$

Because getting the quantum state after measuring the last two qubits is equivalent to taking the partial trace of the target Bell pair, here is the description of the source Bell pair after measurement.

$$\rho^{'}_{ab} = \frac{1}{N}\left[F^2+\frac{1}{9}\left(1-F\right)^2\right]|\Phi^+\rangle\langle\Phi^+| + \frac{2F(1-F)}{3N}|\Phi^-\rangle\langle\Phi^-| + \frac{2(1-F)^2}{9N}(|\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|)$$

$$(N = F^2 + \frac{2F(1-F)}{3} + \frac{2(1-F)^2}{9})$$

The purification becomes successful if F $> \frac{1}{2}$

Acknowledgement

Reference

[1] R. Van Meter, T.D. Ladd, W.J. Munro, and K. Nemoto. System design for a long-line quantum repeater. *IEEE/ACM Transactions on Networking*, 17(3):1002–1013, JUN 2009.

[2] Axel Dahlberg, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpędek, Matteo Pompili, Arian Stolk, Przemysław Pawełczak, Robert Knegjens, Julio de Oliveira Filho, Ronald Hanson, and Stephanie Wehner. A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication*, SIGCOMM '19. ACM, AUG 2019.

[3] Takaaki Matsuo. Simulation of a dynamic, ruleset-based quantum network, 2019.

[4] Richard P Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6/7):467–488, 1982.

[5] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, Dec 2014.

[6] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[7] I K Kominis, T W Kornack, J C Allred, and M V Romalis. A subfemtotesla multichannel atomic magnetometer. *Nature*, 422(6932):596–9, Apr 2003.

[8] Rodney Van Meter and Simon J. Devitt. The path to scalable distributed quantum computing. *Computer*, 49:31–42, 2016.

[9] Pablo Arrighi and Louis Salvail. Blind quantum computation. *International Journal of Quantum Information*, 4(05):883–898, 2006.

[10] Richard Jozsa, Daniel S Abrams, Jonathan P Dowling, and Colin P Williams. Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9):2010, 2000.

[11] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin. Optical interferometry with quantum networks. *Phys. Rev. Lett.*, 123:070504, Aug 2019.

[12] A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

[14] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, Dec 1993.

[15] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996.

[16] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[17] Takaaki Matsuo, Clément Durand, and Rodney Van Meter. Quantum link bootstrapping using a ruleset-based communication protocol. *Physical Review A*, 100(5):052320, 2019.

[18] Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdušek, Takahiko Satoh, Shota Nagayama, and Shigeya Suzuki. A quantum internet architecture. In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 341–352. IEEE, 2022.

[19] Cody Jones, Danny Kim, Matthew T Rakher, Paul G Kwiat, and Thaddeus D Ladd. Design and analysis of communication protocols for quantum repeater networks. *New Journal of Physics*, 18(8):083015, 2016.

[20] Daniel Gottesman, Thomas Jennewein, and Sarah Croke. Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.*, 109:070503, Aug 2012.

[21] Peter Komar, Eric M Kessler, Michael Bishof, Liang Jiang, Anders S Sørensen, Jun Ye, and Mikhail D Lukin. A quantum network of clocks. *Nature Physics*, 10(8):582–587, 2014.

[22] Michael Ben-Or and Avinatan Hassidim. Fast quantum byzantine agreement. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 481–485, New York, NY, USA, 2005. Association for Computing Machinery.

[23] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and qkd in the bounded-quantum-storage model. In *Advances in Cryptology-CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings 27*, pages 342–359. Springer, 2007.

[24] Luciano Aparicio and Rodney Van Meter. Multiplexing schemes for quantum repeater networks. In *Quantum Communications and Quantum Imaging IX*, volume 8163, pages 59–70. SPIE, 2011.

[25] Gregor V. Bochmann. Finite state description of communication protocols. *Computer Networks (1976)*, 2(4):361–372, 1978.

[26] Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, et al. Quisp: a quantum internet simulation package. In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 353–364. IEEE, 2022.

[27] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, Brussels, BEL, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).