Overview of Technology Research in Quantum Communication System

Yixuan Chen

Physics, University of California - San Diego, San Diego, California, 92093, USA

yic070@ucsd.edu

Abstract. As the established communication networks no longer meet people's need in the speed and the security in transferring information, quantum communication draws people's attention. Taking advantage of the basic quantum properties, quantum communication guarantees the message being delivered promptly and safely. This paper first introduces a general background quantum communication. After that, we introduced the history of the development of quantum communication and Quantum Key Distribution (QKD) as well as the general flow of quantum communication. Based on that, we evaluated a scheme of quantum communication network based on QKD, proposing different methods to improve the security and efficiency of the transmission of information. We encapsulated the history of the development of QKD. We conclude that the improvement of quantum communication depends on the algorithms. While various algorithms are proposed, we discussed a potentially possible way to combine the advantages of the algorithms. However, the actual effectiveness of our method still needs to be testified in future researches.

Keywords: Quantum communication, Communication network, Quantum key distribution.

1. Introduction

While the establishment of quantum mechanics erects a monument in the development of human race, it reveals to people in a staggering way that the rules human witness in classical physics could trace their origins in quantum mechanics – the world is essentially quantized. As human attains more knowledge in quantum studies, the subject of quantum information also draws more attentions and becomes the hotspot in the international studies in quantum mechanics and informatics.

1.1. Quantum Mechanics

Being regarded as one of the two pillars in modern physics, quantum mechanics differs from classical physics in the way it describes energies: energies are not continuous; rather, they are quantized, meaning that they are restricted to discrete values. The word "quantum" derives from "quantus" in Latin, meaning "how much". In quantum mechanics, "quantum" refers to the smallest particles that could not be divided into smaller parts. In quantum communication, a single photon is presented to simulate a quantum, hence a photon is also called "light quantum". Several special characters of quantum involve the superposition of quantum state, quantum coherence, quantum entanglement, and quantum non-cloning theorem [1].

1.2. Quantum Informatics

Quantum informatics is a forefront subject that studies how signals and information could be generated, encoded, transferred, and received by applying the theories in quantum mechanics. Quantum informatics include quantum communication, quantum cryptography, and quantum computation.

1.2.1 Quantum Communication

The information transferred in quantum communication is carried by particles like single photon, atom, or spinning electron. The main fields in quantum communication include Quantum Private Communication (QPC), Quantum Teleportation (QT), and Quantum Dense Coding (QDC). Quantum Key Distribution (QKD) guarantees the security of the piece of information not being monitored and

deciphered by the third party, and is realized by the non-cloning principle and the uncertainty principle [2].

1.2.2 Quantum Cryptography

One of the most important examples of quantum cryptography is QKD. QKD is a method that produces a shared random secret key during the communication of two parties. The key is known exclusively by the sender and the receiver, and could be used to encode and decode messages. The first protocol of QKD is BB84. In 1984, BB84 is put forward by Charles H. Bennett and Gills Brassard, in which the message is conveyed by using photon polarization states. Both the sender (Alice) and the receiver (Bob) are connected to a quantum communication channel, and in the case of photons it's an optical fiber or free space [2, 3]. Soon in 1991 E91 protocol was devised, in which Artur Ekert simplified BB84 and used entangled pairs of photons. In the past three decades, the quantum communication is not only realized, but has also witnessed a series of advances. In 1989, IBM is the first laboratory to have successfully realized quantum information transfer. In the year of 2000, the Los Alamos team of U.S. accomplished QKD experiment in the free space, reaching new milestone in quantum engineering. In 2016, China launched satellite Micius, the first time entanglement-based quantum-key distribution has been demonstrated using a satellite. However, still in today, the development of quantum communication is still limited by the distance, efficiency, and the size of the data [4, 5].

1.2.3 Quantum Computation

Quantum computing was proposed in 1980s, and its model is designed by using quantum mechanics to explain the Turing machine. Compared to conventional computers, quantum computers are substantially faster, due to the presence of the superposition in quantum mechanics. Potential applications of quantum computation involve cryptography, machine learning, computational biology, etc.

1.3. Introduction to the Main Work

This paper consists of three sections. The first section is a general introduction to the basic knowledge in quantum mechanics, quantum informatics, quantum communication, and quantum cryptography. In the second section, the key technologies are explained, including quantum communication network, two-way quantum teleportation, multi-user info-sharing and multicast routing schemes in quantum networks. In the third section, these quantum communication technologies are analyzed and compared.

2. Methodology

In 1935, Einstein, postdoctoral Rosen and researcher Podolski cooperated at Princeton Institute of higher studies to complete the paper "can the quantum mechanical description of physical reality be considered complete?" and published this paper in the Physical Review in May. This is the first paper to explore the counterintuitive prediction of quantum mechanics theory for strongly correlated systems. In this paper, they describe the EPR paradox in detail and try to discuss the incomplete properties of quantum mechanics through an ideological experiment. They did not further study the properties of quantum entanglement.

After reading the EPR paper, Schrodinger had many thoughts. He wrote a letter to Einstein in German. In this letter, he first used the term verschränkung (which he translated as "entanglement"), which is to describe the relationship between two temporarily coupled particles in the EPR thought experiment. Soon after, Schrodinger published an important paper to define the term "quantum entanglement" and explore related concepts. Schrodinger realized the importance of this concept. He showed that quantum entanglement is not only an interesting property of quantum mechanics, but also a characteristic property of quantum mechanics; Quantum entanglement makes a complete cut between quantum mechanics and classical ideas. Like Einstein, Schrodinger was not satisfied with

the concept of quantum entanglement, because quantum entanglement seemed to violate the speed limit set for information transmission in relativity. Later, Einstein ridiculed quantum entanglement as a ghostly over distance effect.

EPR paper obviously aroused the interest of many physicists and inspired them to explore the basic theory of quantum mechanics. However, in addition to this aspect, physicists believe that this topic has nothing to do with modern quantum mechanics. For a long time, the physics academic community did not pay special attention to this topic, and did not find any major defects in the EPR paper. EPR paper attempts to establish localized implicit variable theory to replace quantum mechanics theory. In 1964, John Bell put forward a paper that showed that the prediction of quantum mechanics for EPR thought experiment was obviously different from the localized implicit variable theory. Generally speaking, if we measure the spin of two particles along different axes, the statistical correlation result obtained by quantum mechanics is much stronger than the localized implicit variable theory. Bell inequality qualitatively gives this difference, and experiments should be able to detect this difference. Therefore, physicists have done many experiments to test Bell inequality.

In 1972, John crowzer and Stuart Freedman first completed this test experiment. In 1982, Alan asper's doctoral thesis was entitled "this kind of test experiment". The experimental results obtained by them accord with the prediction of quantum mechanics and do not accord with the prediction of localized implicit variable theory, so it is confirmed that localized implicit variable theory is not tenable. However, there are loopholes in each relevant experiment, which makes the correctness of the experiment questioned. Before making a summary, more accurate experiments need to be completed.

Over the years, many research results have contributed to the possibility of using these super correlations to transmit information, which has led to the successful development of quantum cryptography. The most famous are the BB84 protocol invented by Charles Bennett and Gilles brassard and the E91 protocol invented by Artur Eckert.

On June 16, 2017, the quantum science experiment satellite Mozi was first successfully realized. After two quantum entangled photons were distributed at a distance of more than 1200 km, they can still maintain their quantum entanglement state.

On April 25, 2018, the experimental team led by Mika Sillanpää, a professor at the University of Alto, Finland, successfully entangled two independently vibrating eardrums. Each eardrum is only 15 microns wide, about the width of hair, and is made of 10 metal aluminum atoms. Through the superconducting microwave circuit, the interaction between the two tympanic membranes lasted about 30 minutes at near absolute zero (-273.15℃). This experiment demonstrates macroscopic quantum entanglement [6, 7].

As quantum communication constantly progresses, one-to-one quantum communication has gradually become unable to cater to people’s demand. In order to maximize the resource to serve more users at one time, quantum communication network is being studied. Different systems are designed based on various mediums and principles to find multi-user quantum communication. Here, we introduce two different systems, and discuss the possible schemes to improve.

In 2014, Jianmin Wang proposed a model of quantum communication network based on QKD [8]. In the model, Wang divides the quantum transmission network into classical and quantum parts. The duty of the quantum part involves encrypting the information with the key acquired from the QKD process. The quantum part will then select the transmission route, converting segments of information into quantum state. To finish it off it will transmit the negligible information. As the keys that decrypt the information are transferred through the quantum route, the classical part transfers the encrypted data to the receiver.

One problem in QKD is that since the data are transmitted through the classical route, it faces a considerably significant chance of being attacked and captured by the hackers. Then, it’s highly possible for them to decipher the key and consequently decrypt the data transferred. In actual quantum communications, the signals have to be modulated with random number in order to satisfy the requirement for quantum communication. In this process, random numbers directly determines the

security of the quantum communication [9]. Wu Zhu in 2016 proposed a more secured hybrid random number generator. This generator has various schemes to merge low-efficiency random number sources in order to improve its efficiency. Additionally, the scheme utilizes the time interval between dark count, the noise in the single-photon detector, and single photon to generate random number arrays. This method is of high efficiency, practical, and could easily be conducted [10].

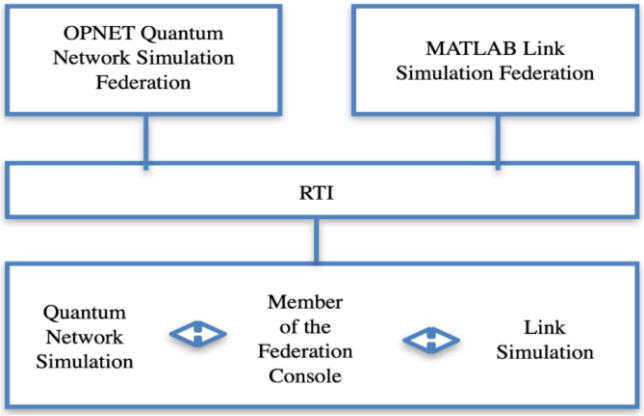

Figure 1. The Construction Graph of Quantum Communication Network based on HLA

The member of OPNET network simulation federation is constructed based on the topology of quantum communication network. It's primary duty is to simulate the communicative properties of quantum communication network. The distribution of HLA proxy node is shown in figure 2 [11]:

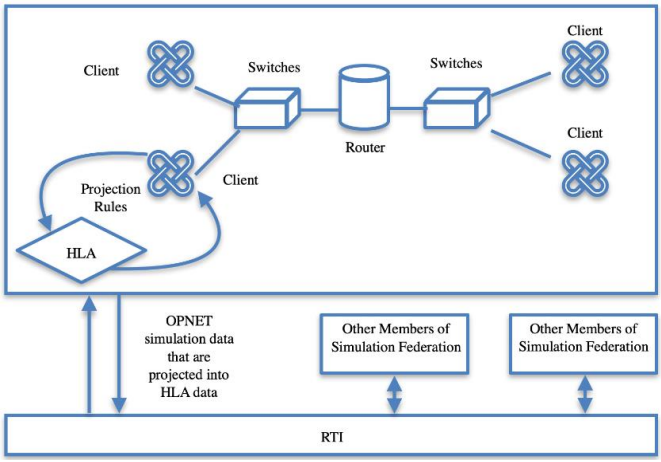

Figure 2. The distribution of HLA proxy node

The following graph illustrates how data is processed in a HLA proxy node.

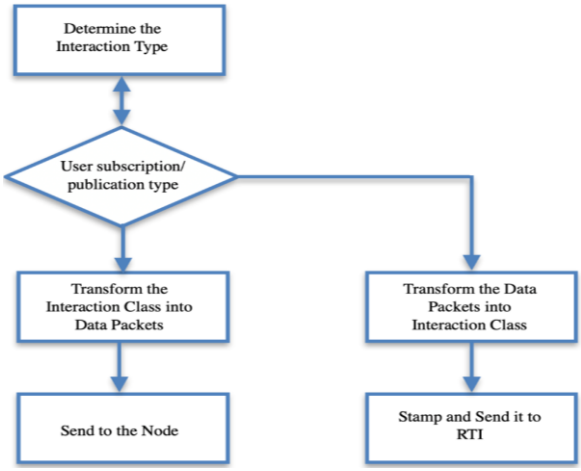

Figure 3. The Flow Chart of How Data is Processed in a HLA Proxy Node

3. Conclusion & Discussion

The methods above the quantum imaging based on are composed of two elements: quantum computing and image processing. These methods save the storage capacity by extracting the edge information from the images. The quantum imaging methods are developed and widely applied in medical and biological fields. For instance, the illness cause could be detected by observing the shape of the red cells.

As the methods mentioned above, different methods apply different algorithms to achieve the derivative effect of the initial images. Compared with traditional optical differentiation methods, The instrumental setups for quantum imaging have the advantages of convenience and could be tied to optical path of microscopes. The development of technology pushes the image processing algorithms to achieve the higher contrasts and detailed detections.

Take some quantum imaging methods for instance, researchers used the algorithms of quantum generative adversarial learning to achieve the spatial differentiation. Or the quantum imaging expansion and Grover search algorithm could corporate to achieve the ideal effects. In addition, quantum image systems are aimed to compress the capacity of images. The quantum electrons have different number of spin states. The more spin states the electron has, the less space the algorithm needs to operate the differentiation process. Compressing the process of quantum calculation is essential for large scale image detections.

In conclusion, the improvement of the quantum imaging methods is the improvement of the algorithms. The diversity of the algorithms provides more possibility for the quantum imaging development. How to combine the advantages of the algorithm with the characters of quantum itself is a research topic in this.

References

[1] An L. Research on multicast transmission in quantum communication networks. 2019.

[2] Bennett C H and Brassard G. Quantum cryptography: public key distribution and coin tossing [C], in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Gangalore, India (IEEE, New York). 1984, 175-179.

[3] Liu W. Research on parameters estimation and the non-markovianity of quantum channel. 2018.

[4] Ye H. Research of data acquisition system in quantum communication system. 2014.

[5] Li W L, Li C F, and Guo G C. Probabilistic teleportation and entanglement matching [J]. Physical Review A, 2000, 61(3): 034301.

[6] D. Bouwmeeser, Pan J W, K Mattle. Experimental quantum teleportation Nature (London). 1997, 390: 575-579.

[7] Kong L. Research on quantum communication protocols in quantum communication. 2015.

[8] Wang J. Research on quantum communication network architecture and distributed simulation. 2014.

[9] Gottesman D, Lo H K, Lutkenhaus N and Preskill J. Security of quantum key distribution with imperfect devices [J]. Quant. Inf. Comput. 2004, 5: 325-360.

[10] Zhu W. Research on quantum communication control system. 2016.

[11] Peev M, Pacher C, Alleaume R, et al. The SECOQC quantum key distribution network in Vienna [J]. New Journal of Physics, 2009, 11(7): 075001.