Quantum Networking, where it is headed

Youssef Khristo
School of Information Technology and Computer Science
Nile University
Cairo, Egypt
y.khristo@nu.edu.eg

Bassem Asaad
School of Information Technology and Computer Science
Nile University
Cairo, Egypt
b.asaad@nu.edu.eg

Nashwa Abdelbaki
School of Information Technology and Computer Science
Nile University
Cairo, Egypt
nabdelbaki @nu.edu.eg

***Abstract*—It is an undeniable fact that computer science has gone a long way, from the invention of transistor-based electronic computers to the rise of artificial intelligence and quantum computing. Now that we are looking at the quantum horizon, the last piece that would complete the quantum revolution is quantum networking.**

Keywords—computer networks, quantum, quantum computing, quantum networking, classical computer, qubit, Quantum Key Distribution (QKD)

I. Introduction

For decades, classical computers dominated -and still are- the world; digital, transistor-based processors have been evolving to include more cores and threads and be more power efficient. With the ongoing studying of quantum mechanics, computer scientists found ways of using the quantum states of quantum particles (e.g. photons) to perform computations. For the past decade, tech giants such as IBM and Google have been investing billions in the development of quantum processors. As for governments, the European Commission dedicated a 1 billion Euro to a project having the goal of boosting the European quantum technology research [1]. The rise of quantum computing stemmed from the possibilities that quantum mechanics offer in the fields of computation and information theory, which includes -but not limited to- problems that classical computing cannot solve. The last piece in the puzzle is connecting quantum processers through quantum networks, allowing the transfer of quantum states in the form of what is now called qubits, since quantum processors perform the computations using quantum particles, classical channels will be redundant as it is more logical to send the quantum states directly, completely removing the classical communication layers.

II. Quantum Mechanics

Before discussing the insides of quantum networks and how they work, we first must review some important properties of quantum particles and the mechanics that governs them.

A. Quantum

In physics, a quantum is the minimum amount of physical entity involved in a physical interaction [3]. For a transistor-based computer, transistors are activated using electrical current made of electrons. In quantum computing however, quantum particles such as quarks and photons are used by measuring their state; a prominent application is measuring the polarization of photons.

B. Superposition

Unlike transistors which could only exist in a single state (either on or off), a quantum particle could exist in a superposition of multiple states at the same time. Let us take photons as an example, while n classical bits could exist in 2^n states, a superposed photon could exist in all 2^n states at the same time.

C. Quantum Measurment

The tricky part about quantum computing is the measurement of quantum particles states, as it could directly affect the quantum state of a given particle. Suppose that we would like to measure the quantum state of a photon in a laser beam at a given point in time, the simple act of measuring its state (let alone other external factors) would alter, in fact, alter it to another state, hence errors. To deal with this problem, quantum computers rely on the property of superconductivity, where quantum processors perform their measurements in a super cooled environment, reaching temperatures as low as 272.9 kelvins, as to inhibit external physical activity, hence preventing it from affecting the readings.

D. Qubit

In classical computers, a I or O state is referred to as a bit, where a byte consists of 8 bits that translates into electric circuits built from transistors, creating what is known as logical gates. In quantum computers, some quantum processors did build a 2-state model based on the classical one, where the bits are quantum bits, hence the qubit term was coined.

E. No-cloning Theorem

Unlike in classical systems where the cloning of information is important, physics disallow arbitrary transformations of quantum system through the act of cloning a qubit with an unknown state [4], a property that greatly affect the design of quantum networks [1].

F. Entaglement

As noted, before, a qubit could be in 1 or more states at the same time, independent from other quantum particles'

2020 16th International Computer Engineering Conference (ICENCO) | 978-1-7281-6392-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICENCO49778.2020.9357398

states. However, an important property called entanglement, where the state of a qubit cannot be measured individually, that is the state of a qubit is dependent on the state of one or more qubits.

Suppose that we have a group of quarks in a state of entanglement, if we measure the quark A, the state of quark B and C is changed instantaneously, regardless of the distance between them. This property baffled Einstein and his colleagues, since it directly contradicts with the theory of general relativity, making them pursue the creation of the EPR theorem.

G. Quantum Computing

A direct application of these physical phenomena is quantum computing, that is the use of quantum mechanical properties to perform calculations using what is called quantum processors. A quantum processor performs measurements on quantum particles states, feeding these readings to classical computers that are wrapping the quantum processor as their core.

III. Quantum Networks

A quantum network is a medium that facilitates the transmission of quantum information and quantum states between quantum processors, called end nodes. Since most quantum computers utilize photons as their quantum particles, the media through which these photons would be transmitted are based on either optical fiber or free space networks.

A. Components

- **End nodes**: the quantum nodes are simple quantum processors performing computation on qubits and yielding results, that is then transmitted through quantum channels.
- **Quantum Channel**: a quantum channel is the medium through which quantum information gets transmitted. An example of quantum information is the state of a qubit. Fiber optics channels are used just like in classical communication, whether in single-mode or multimode, where multimode allows for more precise communication [5]. Another example is free space networks, where quantum information transmission does not rely on fiber optics rather it depends on a direct line of site between photon transmitters. A perfect implementation is satellite to earth transmission, however, the longer the distance the more chances of environmental disturbances on the polarization of photons.
- **Quantum Repeaters**: a quantum repeater can store and transmit quantum states to other nodes/repeaters. Amplifiers are not used like the case with classical networks because qubits cannot be copied (no-cloning theorem).

B. Quantum Internet

Unlike classical internet, where bits are used to communicate between different nodes and classical computation is used, quantum communication relies on the quantum bits, explained earlier, to communicate between different nodes, using Quantum Key Distribution, explained in the coming section, that provides more secure communication utilizing quantum mechanics theories.

C. Quantum Key Distriution (QKD)

Quantum Key Distribution (QKD) is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics.

The research on quantum cryptography can be traced back to 1969 as a first thought of using the theory of quantum mechanics to protect information security. However, this idea was not achieved because of the short life of single quantum state. After that, the first QKD protocol (BB84 protocol) was introduced in 1984, then E91 protocol and B92 protocol [6]. After that, we moved to the practical application of the theory.

Different implementations were done in different areas like in 2014, where a remote quantum key distribution system withstanding hacker attacks, was implemented with extended transmission distance to 200 km. other schemes and protocols were introduced like Device independent QKD protocols.

The biggest advantage of device independent QKD is that even if the quantum mechanics is not established, it can still provide unconditional secure key distribution.

D. Quantum Secure Direct Communication (QSDC)

QSDC is a new communication form different from QKD. The differences between QKD and QSDC are that QSDC transmits secret information in quantum channel directly.

QSDC is one of the main research branches of quantum communication system. Its focus is on transmitting secure information directly without generating quantum key first. However, the research of QSDC is mainly focused on the design of QSDC protocol, and most protocols designed are in ideal environment. Obviously, the research of QSDC has a certain distance from the practice.

E. Quantum Teleportation (QT)

Quantum Teleportation refers to transmitting qubits without either the physical transfer of the particle storing the qubit or the violation of the quantum mechanics principles [1]. Indeed, with just local operations, referred to as Bell-State Measurement (BSM), and an EPR pair (maximally entangled qubits) shared between source and destination, quantum teleportation allows one to “transmit” an unknown quantum state between two remote quantum devices.

QT plays an important role in the field of quantum computation and quantum communication. Different QT schemes were proposed starting 1993. In 1998, for the first time, a research group in Austria successfully demonstrated the quantum teleportation experimentally [6].

In 2012, the hundred kilometers quantum teleportation and entanglement distribution in free space was achieved for the first time in the world, which laid technical foundation for launching the first quantum communication satellite [6].

In 2019 physicists just achieved the first-ever quantum teleportation between computer chips.

F. Reasearch on Quantum Communication Network

Compared to the classical communication, the quantum communication has additional physical resources, i.e., the superposition and entanglement, and the quantum concepts usually have a manifold characteristic.

Quantum communication network is aiming at reaching to more users with more secure and wide networks, utilizing the quantum mechanics and overcoming classical security networks issues. Reaching out to global wide area quantum communication network is still under research and experiments.

In 2002, the United States began to design DARPA quantum key distribution network and built a six-node quantum network by 2004 [6]. Passing by different researches and experiments, we reached out 2013, when quantum communication test network in Jinan (including 50 nodes and 90 users) put into operation, and in 2014, the Beijing-Shanghai route project went through the demonstration, which has been delivered in 2016, and an intercontinental quantum communication network linking Asia and Europe is planned to be built in 2020 [6]. A global quantum wide area network is to be built in 2030 as the structure diagram is shown in Figure 1 [1].

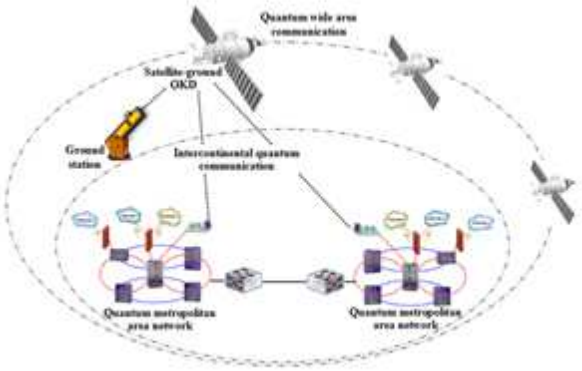

Figure 1. The structure diagram of quantum wide area network [1]

IV. Current Challenges

The field of quantum networking came a long way, we're not however close to a real-life deployment on a large scale; implementing quantum networks in current 5G technology for example as scientists are still to reach a consensus on many details.

A. Quantum Network Coding

The main idea of network coding is to improve the overall throughput and efficiency by combining multiple packets for transmission, providing maximum flow of information. The butterfly network is a perfect example of linear network coding.

It is preferable however in quantum computing to process quantum information locally, where transmitting quantum data could corrupt the quantum state of the system, which raise the question of whether it is possible to create a quantum network coding scheme altogether.

In a paper published in 2010, a quantum coding scheme based on classical network coding was proposed [8], suggesting a perfect scheme for quantum teleportation; that is the transmission of quantum information through classical networks and a previously shared quantum entanglement between the sending and receiving locations.

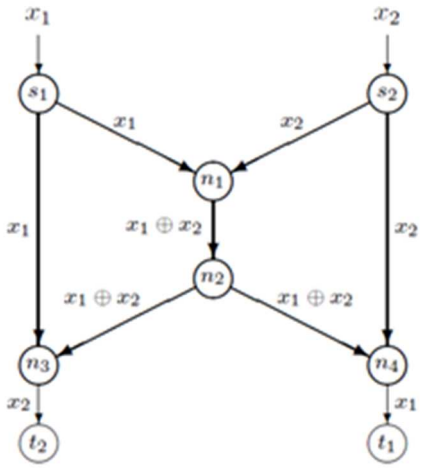

Figure 2. The butterfly network and a classical linear coding protocol [8]

B. Quantum Key Distribution Networks

For QKD to be successful, protocols must be put in place to govern the quantum information transmission for QKD networks, and for this there are 3:

1) *BB84 protocol (1984)*
2) *E91 protocol (1991)*
3) *B92 protocol (1992)*

Some examples of QKD networks are the DARPA Quantum Network, the Swiss Quantum Network, and the Chinese QKD Network later launched with the 2016 QUESS space mission.

C. Quantum Network Security

The most obvious and straight forward way of protecting quantum data and subsequently quantum networks is cryptography. One method of ensuring a network's security is by using cryptographic protocols with longer encryption keys (e.g. TLS), and the distribution of quantum cryptographic keys through QKDs. In theory, quantum key distribution is not hackable and is a single part of the whole security solution.

With the advancement of quantum processors, the need for algorithms based on quantum computing (post-quantum cryptography) was in place, as one of the main purposes of quantum computers is to break classical cryptographic algorithms, hence the need for "quantum" cryptographic algorithms.

The most prominent approaches for post-quantum cryptography are as follows [9]:

1) *Lattice-based cryptography*
2) *Multivariate cryptography*
3) *Hash-based cryptography*
4) *Code-based cryptography*

5) *Supersingular elliptic curve isogeny cryptography*
6) *Symmetric key quantum resistance*

D. Entanglement Distribution

In a network with nodes having no entanglement shared with distant nodes must communicate this entanglement through neighboring nodes. In this scenario, repeaters are used to receive the entangled states, store them, and then distribute them using a unitary operation called entanglement swapping through the rest of the quantum network.

The idea behind entanglement distribution is that in the case of quantum internet, especially when using photons in a medium of say optical fiber channels or free space networks, this data could get corrupted, rendering the quantum information useless. Instead, node A could share information with node B without sending any physical information, all while using entanglement between quantum particles.

E. Scalability and security

Scalability and security are crucial part of any computer network. In already proposed and existing multi-user quantum network implementations, the use of repeaters, quantum memories, and active switching. These networks use many resources, affecting scalability and increasing the difficulty of securing them. Figure 3 proposes a passive quantum network architecture that is an attempt to address the existing issues [10].

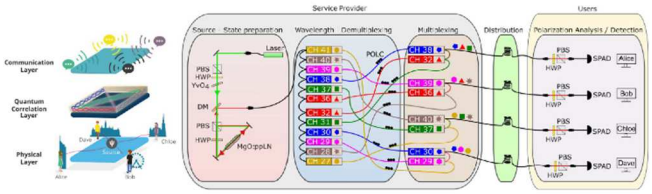

Figure 3. Passive quantum network

CONCLUSION

Quantum communication networking is a multidimensional discipline, that is moving forward to replace the classical communication networks. Overcoming the security threats and utilizing quantum mechanics to cope with the developing technologies and the increasing importance and dependability on information. In this paper, we provided a survey on quantum networks main concepts and pillars, shedding the light on the research history and open points and challenges that still need more research and experiments, in order to reach securely the expectations to have the global quantum wide area network.

REFERENCES

[1] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," in *IEEE Network*, vol. 34, no. 1, pp. 137-143, January/February 2020, doi: 10.1109/MNET.001.1900092.

[2] G. Shi, D. Dong, I. R. Petersen and K. H. Johansson, "Reaching a Quantum Consensus: Master Equations That Generate Symmetrization and Synchronization," in IEEE Transactions on Automatic Control, vol. 61, no. 2, pp. 374-387, Feb. 2016, doi: 10.1109/TAC.2015.2434034.

[3] Wiener, N. (1966). *Differential Space, Quantum Systems, and Prediction*. Cambridge: The Massachusetts Institute of Technology Press

[4] Park, James (1970). "The concept of transition in quantum mechanics". Foundations of Physics. **1** (1): 23–33.

[5] Van Meter, Rodney (2014). Quantum Networking. Hoboken: Wiley. pp. 127–196.

[6] Quantum Communication Networks and Trust Management: A Survey Shibin Zhang1, *, Yan Chang1, Lili Yan1, Zhiwei Sheng1, Fan Yang1, Guihua Han1, Yuanyuan Huang1 and Jinyue Xia2 *Van Meter, Rodney (2014). Quantum Networking. Hoboken: Wiley. pp. 127–196*

[7] Topics in Quantum Networking Fengyou Sun Department of Information Security and Communication Technology NTNU – Norwegian University of Science and Technology Trondheim, Norway. arXiv:1903.02910

[8] H. Kobayashi, F. Le Gall, H. Nishimura and M. Rötteler, "Perfect quantum network communication protocol based on classical network coding," 2010 IEEE International Symposium on Information Theory, Austin, TX, 2010, pp. 2686-2690, doi: 10.1109/ISIT.2010.5513644.

[9] Daniel J. Bernstein, Introduction To Post-Quantum Cryptography.

[10] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel and R. Ursin, "An Entanglement-Based Wavelength Multiplexed Quantum Communication Network," 2019 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany, 2019, pp. 1-1, doi: 10.1109/CLEOE-EQEC.2019.8872932.

[11] J. P. van Dijk, E. Charbon, and F. Sebastiano, "The electronic interface for quantum processors," Microprocessors and Microsystems, 2019.

[12] M. Dyakonov, "The case against quantum computing," IEEE Spectrum,vol. 56, no. 3, pp. 24–29, March 2019.

[13] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta,"Validating quantum computers using randomized model circuits," arXiv preprint arXiv:1811.12926, 2018